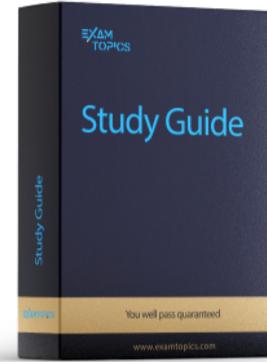




- Expert Verified, Online, **Free**.

Prepare for your AWS Certified Solutions Architect - Professional SAP-C02 exam with additional products



Study Guide

1066 PDF Pages

[Download Now](#)



Video Course

192 Lectures

\$19.99

[Buy Now](#)

[Custom View Settings](#)

Topic 1 - Exam A

Question #1

Topic 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.

 **robertohyena** Highly Voted 9 months, 2 weeks 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 33 times

 **zhangyu20000** Highly Voted 9 months, 2 weeks ago

A because it requires all VPC can resolve the example.com. All VPCs must be associated with private hosted zone

upvoted 6 times

 **task_7** Most Recent 2 weeks ago

Selected Answer: D

D provides the best balance between performance, simplicity, and security, making it the most suitable choice for the given requirements. By using a Route 53 inbound resolver within the shared services VPC, you reduce the latency and complexity associated with forwarding DNS queries to other VPCs or EC2 instances.

upvoted 2 times

 **Soweetadad** 2 weeks, 6 days ago

Selected Answer: A

Answer is A. In the link that someone posted, it says "When a Route 53 private hosted zone needs to be resolved in multiple VPCs and AWS accounts as described earlier, the most reliable pattern is to share the private hosted zone between accounts and associate it to each VPC that needs it." <https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/>

upvoted 1 times

 **career360guru** 3 weeks, 1 day ago

Correct Answer is A. D does not meet the requirement of all VPC able to resolve example.com.

upvoted 1 times

 **dimitry_khan_arc** 1 month ago

Selected Answer: D

D is more suitable

upvoted 2 times

 **vn_thanhung** 3 weeks, 5 days ago

<https://aws.amazon.com/vi/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/#:~:text=Although%20it%20is%20possible%20to%20use%20forwarding%20rules%20to%20resolve%20private%20hosted%20zones%20in%20other%20VPCs%2C%20we%20do%20not%20recommend%20that.%20The%20most%20reliable%2C%20performant%20and%20low%2Dcost%20approach%20is%20to%20share%20and%20associate%20private%20hosted%20zones%20directly%20to%20all%20VPCs%20that%20need%20them>

Answer is A not D

upvoted 1 times

 **weequan** 1 month ago

Selected Answer: D

<https://aws.amazon.com/blogs/security/simplify-dns-management-in-a-multiaccount-environment-with-route-53-resolver/>

upvoted 1 times

 **autobahn** 1 month, 3 weeks ago

So which the correct answer? A or D? When most people have voted for A, should I take that as the correct answer?

upvoted 1 times

 **chico2023** 2 months ago

Selected Answer: A

Requirement 2: All VPCs should be able to resolve cloud.example.com.

upvoted 1 times

 **Magoose** 2 months, 2 weeks ago

Selected Answer: A

Option D is incorrect because it associates the private hosted zone only with the shared services VPC, rather than all the VPCs. This does not meet the requirement of ensuring that all VPCs can resolve cloud.example.com

upvoted 2 times

 **NikkyDicky** 3 months ago

Selected Answer: A

it's a

upvoted 1 times

 **Jonalb** 3 months, 1 week ago

Selected Answer: A

Its A

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html>

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

upvoted 2 times

 **antonvigs** 3 months, 1 week ago

Selected Answer: A

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

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

upvoted 1 times

 **antonvigs** 3 months, 1 week ago

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

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

upvoted 1 times

 **tromyunpak** 3 months, 2 weeks ago

all the vpc needs to reach the inbound resolver in the shared services vpc and so tgw attachments are needed. so IMO answer is A

upvoted 1 times

 **Roontha** 3 months, 4 weeks ago

Answer : A

<https://medium.com/tuimm/resolve-aws-private-hosted-zones-from-on-premise-with-route-53-inbound-resolver-ba683b371522>

upvoted 1 times

 **Roontha** 3 months, 3 weeks ago

I go with D. AWS has given the info on this exact use case with Architecture diagram.

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

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

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

upvoted 1 times

 **rtguru** 4 months ago

I go with D

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.

 **robertohyena** Highly Voted 9 months, 2 weeks ago

C.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/dns-failover.html>

upvoted 12 times

 **leehjworking** 5 months ago

Step1 - set up resources - Route 53 failover DNS records for the domain names

upvoted 1 times

 **c73bf38** Highly Voted 7 months, 1 week ago

The best solution to give the API the ability to fail over to a different AWS Region would be option 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.

This solution involves deploying a new API Gateway API and Lambda functions in another region. The company should also convert the DynamoDB tables to global tables to enable cross-region replication of the data. Then, the company should change the Route 53 DNS record to a failover record and enable target health monitoring to automatically route traffic to the new region in the event of a failure or outage in the primary region.

upvoted 6 times

 **Simon523** Most Recent 3 weeks, 6 days 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** 1 month ago

Selected Answer: C

C is my choice

upvoted 1 times

 **whenthan** 1 month, 2 weeks 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** 1 month, 4 weeks ago

C is correct.

upvoted 1 times

 **NikkyDicky** 3 months ago

Selected Answer: C

It's C

upvoted 1 times

 **cheese929** 3 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

✉ **RunkieMax** 4 months, 2 weeks ago

Selected Answer: C

C fit the best the question

upvoted 1 times

✉ **braveheart22** 4 months, 3 weeks ago

c73bf38, I totally agree with the explanation.

upvoted 1 times

✉ **Sarutobi** 5 months, 2 weeks ago

Selected Answer: C

I also agree with C. But not sure why not B, B is actually pretty good option. No, that I have experience in this specific case; what I normally see is Active/Standby. But option B sounds good because, in theory, we need to have both regions running the current code (Lambda) and if an outage happens we are sure both work, and we don't have stale config/code in the failover region. Sometimes multi-answer does not return the best endpoint for the use case, so that could be something against this solution.

upvoted 2 times

✉ **mfsec** 6 months ago

Selected Answer: C

C is good here

upvoted 1 times

✉ **kiran15789** 6 months, 3 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/apigateway/latest/developerguide/dns-failover.html>

upvoted 1 times

✉ **dev112233xx** 7 months ago

Selected Answer: C

Easy one :)

upvoted 1 times

✉ **Sarutobi** 7 months, 2 weeks ago

Selected Answer: C

C is correct.

upvoted 1 times

✉ **masetromain** 8 months, 2 weeks ago

Selected Answer: C

The solution that will meet these requirements is option 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.

This solution will allow the API to failover to a different region, by using Route 53 failover record. The failover record will direct traffic to the primary API endpoint (the one in the primary region) as long as it is healthy. If the primary endpoint becomes unavailable, traffic will be directed to the secondary endpoint (the one in the secondary region). Additionally, by converting the DynamoDB tables to global tables, the data will be available in both regions, which is required for the failover scenario. Target health monitoring can be used to monitor the health of the API Gateway, and when it is determined that the primary endpoint is unavailable, the traffic will be directed to the secondary endpoint.

upvoted 3 times

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

Selected Answer: C

I agree with answer C. this is the correct use case of road 53 DNS failover record

upvoted 4 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.

 **Snip** Highly Voted  9 months, 2 weeks 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 29 times

 **robertohyena** Highly Voted  9 months, 2 weeks ago

Answer: D.

Not A: too much overhead and maintenance.

Not B: SCP at Root will still deny Config to the temporary OU.

Not C: Too much overhead to create allow list.

upvoted 14 times

 **dimitry_khan_arc** Most Recent  1 month ago

Selected Answer: D

Chosen D.

B is not correct because root having explicit deny will override any explicit allow in its child OU even if allowance is given. Unless I keep Onboarding account under a parent where there is not explicit deny for Config service, Onboarding account can not configure. So, need to move the explicit deny from root account to production account and then keep onboarding account under root.

upvoted 1 times

 **autobahn** 1 month ago

So which is the correct answer B or D? Why is the portal saying it as "B" though many of them think it is D?

upvoted 2 times

 **technosavvy** 1 month, 1 week ago

Option D: This option would allow administrators to make changes to AWS Config rules for the new account, but it would also move the SCPs that limit access to other restricted services to the Production OU. This could create security risks for the other accounts in the organization.

upvoted 1 times

 **Karamen** 1 month, 3 weeks ago

The right answer is D

upvoted 1 times

 **autobahn** 1 month, 3 weeks ago

I'm thinking it is B because in D, it says move the organization's SCP to Production OU.. First of all why is this extra step needed? After configuring the Onboarding Account, all that needs to happen is to move that account under Production OU. Production Account's SCP should stay as is. That's my opinion. SO, B seems to be more straightforward solution.

upvoted 1 times

 **sebnzogang** 1 month, 4 weeks ago

Selected Answer: B

D: is not correct, because removing the root SCPs on the production OU means removing all the security rules on the services preventing changes, including changes to the AWS Config rules. and depending on the scenario this will be a security hole for production.

Don't forget that the aim is to introduce the new AWS account into the Production OU with the same configurations and restrictions as the accounts that are already there.

So thanks to the temporary OU on which we have an SCP that authorises actions on AWS Config, we just need to modify the configuration of the new account so that it matches the production requirements. Once the configuration requirements have been met, we move the new account into the production OU.

upvoted 3 times

victorHugo 3 weeks, 5 days ago

" All accounts are members of the Production OU", therefore we don't need the SCP in root.

upvoted 1 times

chico2023 2 months ago

Selected Answer: D

D is the only one that has: "Move the organization's root SCP to the Production OU"

An SCP at a lower level can't add a permission after it is blocked by an SCP at a higher level.

upvoted 1 times

NikkyDicky 3 months ago

Selected Answer: D

it's D

upvoted 1 times

Jonalb 3 months, 1 week ago

Selected Answer: D

Explanation:

By creating a temporary OU named Onboarding for the new account, the company can isolate the new account and make the necessary adjustments without affecting the existing accounts.

Applying an SCP to the Onboarding OU that allows AWS Config actions will grant the administrators of the new business unit the required permissions to update existing AWS Config rules.

Moving the organization's root SCP to the Production OU ensures that the existing policies and restrictions are still enforced for the rest of the accounts within the organization.

Once the adjustments to AWS Config are complete and the new account is aligned with the company's policies, the new account can be moved to the Production OU, integrating it into the existing account structure and applying the same policies.

upvoted 2 times

bhanus 3 months, 2 weeks ago

The question NOWHERE talks about shared services VPC. Not sure if its missing here. D is the answer. A is also correct but its time taking as association of R53 zone for all the VPCs is time consuming. Imagine in future VPCs grow in number and you need to make sure R53 zone is associated with all VPCs which is time consuming. D makes it easy by associating to shared services VPC's once

upvoted 1 times

RunkieMax 4 months, 2 weeks ago

Selected Answer: D

root scp should to be move to production to let the onboarding OU the time to enforce the security

upvoted 1 times

Limlimwdwd 4 months, 2 weeks ago

Selected Answer: D

Root account deny control will supersede all the allow in the OU.. only way to workaround is move it to prod to keep the control measure

upvoted 1 times

Anonymous9999 5 months, 1 week ago

Selected Answer: D

From <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#subnets>:

Any account has only those permissions permitted by every parent above it. If a permission is blocked at any level above the account, either implicitly (by not being included in an Allow policy statement) or explicitly (by being included in a Deny policy statement), a user or role in the affected account can't use that permission

Thus it cannot be B

upvoted 1 times

mfsec 6 months ago

Selected Answer: D

D is correct

upvoted 1 times

dev112233xx 6 months ago

Selected Answer: D

D is the correct answer. Explicit Deny on root can't be bypassed by just adding "allow" in the OU SCP

upvoted 2 times

Question #4

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.

 **robertohyena** Highly Voted  9 months, 2 weeks ago

- C.
- Aurora writers is a distractor.
 - Single master mode only has read replica - with Aurora replicas.
 - Multi master mode, not in the options
 - NLB does not support round robin and least outstanding algorithm

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Integrating.AutoScale.html>
upvoted 18 times

 **c73bf38** Highly Voted  7 months, 1 week ago

Selected Answer: C

The best solution to provide a consistent user experience that will allow the application and database tiers to scale would be option C:

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

This solution involves enabling Aurora Auto Scaling for Aurora Replicas to automatically add and remove read replicas to match the application's workload. The solution also uses an Application Load Balancer to distribute traffic to the application layer, with the round robin routing algorithm to balance the traffic evenly across multiple instances. Sticky sessions should be enabled to maintain session affinity for each user, allowing for a consistent user experience.

upvoted 11 times

 **rsn** Most Recent  2 weeks, 4 days 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** 2 weeks, 2 days 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 2 times

 **dimitry_khan_arc** 1 month ago

Selected Answer: C

write replica is distractor. NLB does not support round robin

upvoted 1 times

 **NikkyDicky** 3 months ago

Selected Answer: C

it's C

upvoted 1 times

 **ptpho** 3 months, 3 weeks ago

It's C

No idea about NLB.

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

upvoted 1 times

 **Limlimwdwd** 4 months, 2 weeks ago

Selected Answer: C

Aurora Replicas and ALB will meet the purpose

upvoted 1 times

 **EthicalBond** 5 months ago

Selected Answer: C

Read Replicas

ALB with sticky sessions (due to stateful application)

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: C

Aurora replicas + ALB

upvoted 1 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html#Aurora.Replication.Replicas>

upvoted 1 times

 **gameoflove** 6 months, 4 weeks ago

C.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html#Aurora.Replication.Replicas>

upvoted 1 times

 **masetromain** 8 months, 2 weeks ago

Selected Answer: C

C is correct. This solution will provide a consistent user experience by using an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled. This allows the application and database tiers to scale by using Aurora Auto Scaling for Aurora Replicas. This will ensure that the application is able to handle the increased user base while maintaining a consistent user experience. The use of an Application Load Balancer also allows for better routing of traffic to the available Aurora Replicas.

upvoted 2 times

 **ThaiNT** 9 months ago

Using Amazon Aurora Auto Scaling with Aurora replicas

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Integrating.AutoScale.html>

upvoted 2 times

 **masssa** 9 months, 1 week ago

C is correct

upvoted 2 times

 **Arun_Bala** 9 months, 1 week ago

Selected Answer: C

Correct ans is c

upvoted 2 times

 **nez15** 9 months, 2 weeks ago

SAP-C01 Question.

<https://www.examtopics.com/discussions/amazon/view/36075-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 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.

 **EricZhang** Highly Voted 9 months, 2 weeks 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 38 times

 **vn_thanh tung** 1 month 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 1 times

 **masetromain** Highly Voted 9 months, 2 weeks ago

I think this is answer D: Lambda@Edge can modify headers

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html>

upvoted 21 times

 **vn_thanh tung** 1 month ago

Agree D

upvoted 2 times

 **vestersly** Most Recent 1 week, 2 days ago

Selected Answer: B

The answer is certainly B ,We must consider the serverless requirement in the new design.

upvoted 4 times

 **cheese929** 2 weeks, 2 days ago

Selected Answer: A

Both CloudFront function and Lambda@Edge can do the job. but CloudFront function can do it at approximately 1/6th the price of Lambda@Edge. Thus I go for A.

upvoted 1 times

 **Melampos** 2 weeks, 6 days ago

Selected Answer: B

ALB in answer cannot fit with requirement (serverless).

upvoted 2 times

 **awsent** 3 weeks, 1 day ago

Answer: D

Due to service is being used by devices, using CloudFront. API Gateway is a regional service and request could experience latency. CloudFront Functions are executed prior to request to Edge Cache, this scenario requires changes to the response header, hence Lambda@Edge.

upvoted 1 times

 **dimitry_khan_arc** 1 month ago

Selected Answer: B

Cloudfront could have been a choice but as soon as it talks about ALB the requirement to keep serverless is compromised. So, B is the answer.
upvoted 1 times

 **autobahn** 1 month ago

It has to be B since ALB is not a serverless service. The company prefers a serverless architecture. Also, the requirement doesn't talk about Caching or reducing Latency. So, A & D cannot be the right choice.

upvoted 1 times

 **chico2023** 1 month, 3 weeks ago

Selected Answer: A

Interestingly, the link shared by Karamen (<https://aws.amazon.com/blogs/aws/introducing-cloudfront-functions-run-your-code-at-the-edge-with-low-latency-at-any-scale/>) points to answer A.

CloudFront functions include: "HTTP header manipulation: View, add, modify, or delete any of the request/response headers." This helps giving weight to answer A as the correct one.

upvoted 2 times

 **Karamen** 2 months ago

the correct answer is D.

<https://aws.amazon.com/blogs/aws/introducing-cloudfront-functions-run-your-code-at-the-edge-with-low-latency-at-any-scale/>

upvoted 1 times

 **RotterDam** 1 month, 1 week ago

Why not (A)? They both can do the same thing - only CF Functions can do it much earlier at the Edge Location much closer to the user BEFORE it hits Regional Cache (Lambda@Edge work at the Regional Cache)

upvoted 1 times

 **Russ99** 2 months ago

Selected Answer: D

As to A, Amazon CloudFront does not provide built-in capabilities to directly remove or modify HTTP headers

upvoted 1 times

 **RotterDam** 1 month, 1 week ago

Says who? CF functions do this very well as announced in their Blogs

The second category of use cases are simple HTTP(s) request/response manipulations that can be executed by very short-lived functions. For these use cases, you need a flexible programming experience with the performance, scale, and cost-effectiveness that enable you to execute them on every request.

To help you with this second category of use cases, I am happy to announce the availability of CloudFront Functions, a new serverless scripting platform that allows you to run lightweight JavaScript code at the 218+ CloudFront edge locations at approximately 1/6th the price of Lambda@Edge.

<https://aws.amazon.com/blogs/aws/introducing-cloudfront-functions-run-your-code-at-the-edge-with-low-latency-at-any-scale/>

upvoted 2 times

 **allen_devops** 2 months, 1 week ago

Option A is correct. For option B and C, they doesn't support mapping based on headers. It only concern payload, context and stage. For Option D, it should be associate with viewer request. It should be viewer response.

upvoted 1 times

 **allen_devops** 2 months, 1 week ago

To correct myself, Data Mapping is only available for REST API, not HTTP so C is wrong. For option B, default gateway response is used to responded with an error.

upvoted 1 times

 **Jonalb** 2 months, 2 weeks ago

Selected Answer: A

<https://trackit.io/cloudfront-functions-vs-lambdaedge-which-one-should-you-choose/>

upvoted 3 times

 **Magoose** 2 months, 2 weeks ago

Selected Answer: D

Option A is incorrect because using a CloudFront function to remove headers is not possible. CloudFront functions do not have the capability to modify headers in response to viewer requests.

upvoted 1 times

 **davidcc8g** 2 months, 2 weeks ago

just wonder if in real exam will be such case? the answer is wrong, but we selected correct one

upvoted 1 times

 **RotterDam** 1 month, 1 week ago

I believe this is an actual exam question mate...

upvoted 1 times

 **Mom305** 2 months, 3 weeks ago

A you can configure a lambda@Edge but now you can now set headers with CloudFront Functions

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: A

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

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/*"
  ]
}
```

  robertohyena  9 months, 2 weeks 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 18 times

  higashikumi  6 months, 3 weeks 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 10 times

 **career360guru** Most Recent 3 weeks, 1 day ago

A & C are the right answer

upvoted 2 times

 **[Removed]** 2 months, 1 week 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 1 times

 **NikkyDicky** 3 months ago

C&D. can only vote for one? lol

upvoted 1 times

 **BasselBuzz** 3 months, 1 week ago

Selected Answer: D

C and D for sure

upvoted 1 times

 **SkyZeroZx** 3 months, 2 weeks ago

Selected Answer: D

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 1 times

 **rbm2023** 4 months ago

Selected Answer: C

C AND D

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/*"

These steps allow the IAM user User_DataProcessor from Account B to access the S3 bucket in Account A by granting the appropriate permissions.

upvoted 1 times

 **rtguru** 4 months ago

C&D is the correct answer

upvoted 1 times

 **AmitB** 4 months, 2 weeks ago

Answer is C& D

Ref

<https://repost.aws/knowledge-center/cross-account-access-s3>

upvoted 1 times

 **iamunstopable** 5 months ago

Answer: C & D are correct

upvoted 1 times

 **EthicalBond** 5 months ago

Selected Answer: C

Doesn't make sense for account B to control access to resources in account A. So D is NOT the answer.

Account A owns the bucket and sets the bucket policy to allow access to a principal/user in Account B

upvoted 2 times

 **momo3321** 5 months ago

Nope, this is the multiple answers question and in this case, it's required the performing from both way (Account A & Account B), doesn't work if only Account B open the policy to the bucket which belong to Account A

upvoted 1 times

 **Don2021** 5 months, 1 week ago

C & D - 100%

upvoted 2 times

 **elad18** 5 months, 3 weeks ago

Selected Answer: C

C & D.

But the ListBucket action won't work as you need to mention the arn of the bucket itself as well (without the /*)

upvoted 2 times

 **OCHT** 5 months, 3 weeks ago

Selected Answer: C

C & D.

upvoted 1 times

 **hpipit** 6 months ago

Selected Answer: C

C and D, 100%

upvoted 1 times

 **dev112233xx** 6 months ago

Selected Answer: C

C+D no doubts

upvoted 1 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 15 times

 **zhangyu20000** Highly Voted 9 months, 2 weeks ago

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

upvoted 12 times

 **chikorita** 4 months ago

you surely dont have any industry experience or else you wouldn't recommend to run Microservice architecture on LAMBDA functions

upvoted 4 times

 **btx** 3 months, 1 week ago

Not trivial to move containers to lambda functions. Not impossible though. They have containers. A serverless way of directly hosting those containers is ECS fargate.

upvoted 1 times

 **anita_student** 7 months, 1 week ago

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

upvoted 4 times

 **MansaMunsa** 6 months, 1 week ago

A) is not correct. AWS documentation says you can package and deploy Lambda functions AS container images. A) says Deploy Container images as lambda functions, the opposite.

upvoted 5 times

 **task_7** Most Recent 1 week, 6 days ago

Selected Answer: D

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

upvoted 2 times

 **cheese929** 2 weeks, 2 days ago

Selected Answer: B

B is correct.

upvoted 1 times

 **career360guru** 3 weeks, 1 day 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 re-

factors 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 1 month ago

Selected Answer: B

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

upvoted 1 times

asim_rasheed 1 month, 1 week 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 2 times

Shijokingo 1 month, 4 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 1 times

aviathor 3 weeks, 6 days ago

You can indeed use FarGate with EKS...

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

upvoted 1 times

stevegod0 1 month, 4 weeks ago

Seems option A provides the most cost-effective solution with minimal operational complexity by leveraging AWS Lambda and API Gateway for the serverless architecture of the microservices.

upvoted 1 times

hirenshah005 2 months ago

Selected Answer: B

The key points from Q. you can get is solution have to be minimum operation overhead and most cost effective.

The amount of steps needed to work with Lambda are high as beyond what they mentioned in A we have to have API Gateway as well to make it work properly. Also Lambda with high concurrency is expensive compared to Fargate.

On the other hand B makes it super simple ECS and fargate makes it cheaper.

upvoted 2 times

NikkyDicky 3 months ago

Selected Answer: B

it's B

upvoted 1 times

Jonalb 3 months, 1 week ago

Selected Answer: B

Explanation:

Amazon ECS with Fargate: By uploading the container images to Amazon ECR and using Amazon ECS with the Fargate launch type, you can run the microservices in containers without having to manage the underlying infrastructure. Fargate automatically scales the containers based on the load.

Separate Production and Testing Environments: With two separate auto-scaled Amazon ECS clusters, you can have dedicated environments for production and testing, ensuring isolation and allowing for separate deployments and configurations.

Application Load Balancers (ALB): Configuring two separate ALBs allows you to direct traffic to the appropriate ECS clusters. This ensures proper routing of requests between the production and testing environments.

Option B provides a cost-effective solution by utilizing the serverless nature of Fargate, which eliminates the need to provision and manage EC2 instances explicitly. It also allows for separate environments, easy scalability, and traffic routing using ALBs, providing flexibility and minimizing operational complexity.

upvoted 2 times

SkyZeroZx 3 months, 1 week ago

Selected Answer: B

EKS is more costly than only use fargate

then B

upvoted 2 times

Jonalb 3 months, 3 weeks ago

Selected Answer: B

I would vote for B!

But the segmentation with namespace in k8s cluster is a reality for economy reasons. Although it is not a good practice.

upvoted 1 times

rtguru 4 months ago

B seems to be the most cost effective compared to A&C

upvoted 1 times

👤 **EthicalBond** 5 months ago

Selected Answer: B

A is great but takes time and too many integrations

B is serverless and easy to achieve.

C is not serverless

D not applicable

upvoted 1 times

👤 **2aldous** 5 months, 1 week ago

A.

Before the discussion, check this: <https://docs.aws.amazon.com/lambda/latest/dg/gettingstarted-images.html>

Also, manage two load balancers are not cost effective.

upvoted 1 times

👤 **2aldous** 4 months, 2 weeks ago

Change to "B", because A says "upload image to AWS Lambda" that's actually not possible, you should upload the image to ECR also for Lambda container.

upvoted 2 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.

 **masetromain** Highly Voted  9 months, 2 weeks ago

Selected Answer: B

I go with B

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

upvoted 15 times

 **masetromain** 8 months, 2 weeks 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 9 times

 **dimitry_khan_arc** Most Recent  1 month ago

Selected Answer: B

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

upvoted 1 times

 **NikkyDicky** 3 months ago

it's a B again

upvoted 1 times

 **Parimal1983** 3 months 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** 3 months, 2 weeks ago

Selected Answer: B

SNS + Health check

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B

SNS + Health check
upvoted 1 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>
upvoted 1 times

 **higashikumi** 6 months, 3 weeks 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** 7 months, 2 weeks 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** 5 months, 3 weeks 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** 5 months, 1 week 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** 5 days, 18 hours 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

 **aws0909** 7 months, 3 weeks ago

I will go with option B as it reduces the RTO

upvoted 1 times

 **Yihong** 7 months, 3 weeks ago

Selected Answer: B

A: no health check
C: active active
D: Equal weight?
upvoted 2 times

 **Untamables** 9 months ago

Selected Answer: B

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

Option A, C and D are wrong. The latency-based routing and endpoint weights should be used for active/active strategy.

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

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoints-endpoint-weights.html>

upvoted 4 times

 **ptpho** 9 months, 1 week ago

I go with B

5xx is incorrectly method to cover the case of the main site completely down
Its not act-act loading so R53 should not load traffic between 2 ALBs

upvoted 3 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.

 **masetromain** Highly Voted  9 months, 2 weeks ago

Selected Answer: ADF

I go with ADF

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

upvoted 11 times

 **masetromain** 8 months, 2 weeks 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 7 times

 **spencer_sharp** 9 months, 1 week ago

Why C is wrong?

upvoted 2 times

 **Karamen** 1 month, 2 weeks ago

let suppose in case one of used AZ is failed?

upvoted 1 times

 **dtha1002** 4 months 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** 8 months, 2 weeks 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** 7 months, 2 weeks ago

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

upvoted 5 times

 **NikkyDicky** Most Recent  3 months ago

Selected Answer: ADF

it's of course ADF

upvoted 1 times

 **Parimal1983** 3 months 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** 4 months ago

ADF will meet the described provisions

upvoted 1 times

 **RunkieMax** 4 months, 2 weeks ago

Selected Answer: ADF

Fit the best the question

upvoted 1 times

 **Maja1** 5 months 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 3 times

 **dev112233xx** 6 months ago

Selected Answer: ADF

ADF the correct answers 

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: ADF

ADF is the best fit.

upvoted 1 times

 **gameoflove** 6 months, 2 weeks 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** 6 months, 3 weeks ago

Selected Answer: ADF

adf correct

upvoted 1 times

 **spd** 6 months, 3 weeks 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** 6 months, 3 weeks 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

 **frfavoredo** 5 months, 3 weeks 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

 **higashikumi** 6 months, 3 weeks ago

A, D, E are the correct options to meet the requirements.

Option A is correct because an Auto Scaling group with a minimum capacity of two instances and an Elastic Load Balancer distributing traffic across them can provide high availability and automatic recovery from failure.

Option D is correct because a Multi-AZ deployment for the RDS instance will ensure that there is a synchronized standby copy of the database in

a separate Availability Zone that can be used for automatic failover.

Option E is correct because configuring an Auto Scaling group for the ElastiCache for Redis cluster will ensure that there is at least one available node at all times, and automatic recovery can be achieved by launching new instances to replace any failed nodes.

upvoted 1 times

✉ **Ajani** 6 months, 3 weeks ago

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

upvoted 1 times

✉ **gameoflove** 6 months, 4 weeks ago

Selected Answer: ADF

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

upvoted 1 times

✉ **spd** 7 months ago

Why F and Not E ? ElastiCache for Redis natively supports automatic Multi-AZ failover.

upvoted 2 times

✉ **Ajani** 6 months, 3 weeks ago

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

upvoted 1 times

✉ **spd** 6 months, 3 weeks ago

This does not answer why not E

upvoted 1 times

✉ **Musk** 7 months, 2 weeks ago

I don't dislike C

upvoted 1 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.

 **Raj40** Highly Voted  9 months, 2 weeks ago

A & E

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

upvoted 22 times

 **bur4an** Most Recent  3 weeks, 6 days ago

Selected Answer: AE

Agree with Raj40

upvoted 2 times

 **dimitry_khan_arc** 1 month 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 1 times

 **cattle_rei** 2 months, 1 week ago

Selected Answer: AE

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

upvoted 2 times

 **NikkyDicky** 3 months ago

Selected Answer: AE

AE is right

upvoted 1 times

 **Parimal1983** 3 months 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** 4 months ago

Correct answer is A&E

upvoted 2 times

 **Sarutobi** 5 months, 1 week 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 3 times

 **mfsec** 6 months ago

Selected Answer: AE

AE - easy

upvoted 1 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: AE

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

upvoted 1 times

 **higashikumi** 6 months, 3 weeks 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** 7 months ago

Selected Answer: AE

A&E are the correct answers imo

upvoted 1 times

 **Pratap** 7 months, 1 week ago

A and E as per <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GeneratingCustomErrorResponses.html#custom-error-pages-procedure>

upvoted 1 times

 **God_Is_Love** 7 months, 2 weeks ago

A is incorrect because, Cloud front already handles OAI and its easy to build up error page with it. DNS records apply is pretty quick, So C,E are correct.

upvoted 2 times

 **vsk12** 8 months ago

A & C as S3 can be used to host the static website and Route 53 can be configured for health checks and fail-over routing.

Refer AWS documentation -

Route 53 Fail Over S3

(<https://aws.amazon.com/premiumsupport/knowledge-center/fail-over-s3-r53/>)

Option E is wrong as CloudFront would return the error response for failure and does not provide a page that Route 53 can point to.

upvoted 2 times

 **MRL110** 2 months ago

Option E says: "Modify DNS records to point to a publicly accessible web page" which should mean Route53 here I guess.

upvoted 1 times

 **masetromain** 8 months, 2 weeks ago

Selected Answer: AE

Option A: Creating an S3 bucket and uploading custom error pages to it will allow you to provide a custom error page to visitors when the ALB returns a 502 error.

Option E: By configuring CloudFront custom error pages, visitors will be redirected to a publicly accessible web page when a 502 error occurs. DNS records can be modified to point to a publicly accessible web page, which will be displayed when the error occurs.

Option B and D are not a best practice since they would change the behavior of the load balancer and it's not the best way to display custom error pages.

Option C is not related to custom error pages and not the best way to handle the problem.

upvoted 3 times

 **excoRt** 9 months ago

Selected Answer: AE

A & E - Classic Cloudfront error page mechanism

upvoted 2 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.

 **masetromain** Highly Voted 9 months, 2 weeks ago

Selected Answer: BD

I go with BD

upvoted 16 times

 **masetromain** 8 months, 2 weeks 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 8 times

 **razguru** Highly Voted 9 months, 1 week 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

 **sreed77** Most Recent 1 week, 5 days 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 1 times

 **dimitry_khan_arc** 4 weeks, 1 day ago

Selected Answer: BD

B & D are most relevant

upvoted 1 times

 **whenthan** 1 month, 1 week 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 1 times

 **cattle_rei** 2 months ago

Selected Answer: BD

BD is the most correct, the rest are distractors

upvoted 1 times

 **cattle_rei** 2 months ago

BD seems the most correct
upvoted 1 times

 **NikkyDicky** 3 months ago

Selected Answer: BD
it's BD
upvoted 1 times

 **Parimal1983** 3 months ago

Selected Answer: BE

Using prefix list we can simplify routing tables instead of sharing individual subnet of the VPCs. Need to enable resource sharing at organization.
upvoted 2 times

 **Ixrdrm** 2 months, 4 weeks ago

When you go into RAM and create a resource share, you can only select a subnet to share.
upvoted 1 times

 **Brightalw** 1 month, 3 weeks ago

Prefix lists

ec2:PrefixList

Create and manage prefix lists centrally, and share them with other AWS accounts or your organization. This lets multiple AWS accounts reference prefix lists in their resources, such as VPC security groups and subnet route tables. For more information, see Working with shared prefix lists in the Amazon VPC User Guide.

upvoted 2 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: BD

The correct answers are D and B.

D will allow the infrastructure team to create a resource share in AWS Resource Access Manager in the infrastructure account. This will allow them to share the VPC with the other accounts in the organization.

B will enable resource sharing from the AWS Organizations management account. This is required to allow the resource share to be created.

C is not necessary, as the resource share will allow the other accounts to create resources in the shared VPC.

A is not necessary, as the resource share will allow the other accounts to connect to the shared VPC through the transit gateway.

E is not necessary, as the resource share will allow the other accounts to create resources in the shared VPC without the need for prefix lists.
upvoted 1 times

 **Amir70** 3 months, 2 weeks ago

A. By creating a transit gateway in the infrastructure account, you establish a centralized hub for network connectivity. The transit gateway acts as a transit point for traffic between VPCs and accounts.

C. Create VPCs in each individual AWS account within the organization and configure them to share the same CIDR range and subnets as the VPC in the infrastructure account. Then, peer the VPCs in each individual account with the VPC in the infrastructure account. This allows resources in the individual accounts to communicate over the shared network managed by the infrastructure team.

By following these steps, the infrastructure team can maintain control over the network in the dedicated infrastructure account, while individual accounts can create resources within subnets and utilize the shared network. The transit gateway provides the connectivity between the VPCs in different accounts, enabling seamless communication and resource access.

upvoted 1 times

 **rtguru** 4 months ago

I go with A&D
upvoted 1 times

 **karma4moksha** 4 months, 2 weeks ago

BD, agreed. A is wrong because if you share the network , there are no multiple networks and hence no gateway needed.
upvoted 1 times

 **Maja1** 5 months ago

Selected Answer: BD

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-sharing.html>

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: BD

BD is correct

upvoted 3 times

✉  **mKrishna** 6 months, 3 weeks ago

ANS: A & C.

Option B is not required because AWS Organizations is already being used to manage the accounts. Resource sharing needs to be enabled, but this can be done by creating a resource share.

Option D and E both involve creating a resource share in AWS Resource Access Manager (RAM), but they are not the correct solution for this scenario. Option D is specific to subnets, option E is specific to prefix lists, which are used for IP address ranges. Since VPCs are being used in this scenario, options D and E are not applicable.

upvoted 1 times

✉  **newtrojan** 4 months, 4 weeks ago

AWS orgs doesn't allow sharing by default <https://docs.aws.amazon.com/ram/latest/userguide/security-disable-sharing-with-orgs.html>

upvoted 2 times

✉  **kiran15789** 6 months, 3 weeks ago

wouldnt "Select each prefix list to associate with the resource share." will be use to do then go with selecting each subnet

upvoted 2 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.

 **Raj40** Highly Voted  9 months, 2 weeks ago

Selected Answer: A

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

upvoted 13 times

 **masetromain** Highly Voted  9 months, 2 weeks ago

Selected Answer: A

I go with A

upvoted 7 times

 **masetromain** 8 months, 2 weeks 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 7 times

 **task_7** Most Recent  1 week, 6 days 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 1 times

 **whenthan** 1 month, 1 week 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** 2 months 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** 3 months ago

Selected Answer: A

it s a

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: A

Create an AWS PrivateLink interface VPC endpoint.

upvoted 1 times

 **2aldous** 5 months, 1 week ago

Selected Answer: A
Access SaaS products through AWS PrivateLink is the answer.
upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A
Create an AWS PrivateLink interface VPC endpoint.
upvoted 1 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: A
<https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-access-saas.html>
upvoted 1 times

 **ptpho** 9 months, 1 week ago

It's A .clearly
upvoted 4 times

 **spencer_sharp** 9 months, 1 week ago

Selected Answer: A
<https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-access-saas.html>
upvoted 4 times

 **robertohyena** 9 months, 2 weeks ago

A is correct.
<https://docs.aws.amazon.com/vpc/latest/privatelink/create-endpoint-service.html#share-endpoint-service>
upvoted 5 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.

 **masetromain** Highly Voted  9 months, 2 weeks ago

Selected Answer: A

A is good

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

upvoted 9 times

 **masetromain** 8 months, 2 weeks 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 7 times

 **whenthan** Most Recent  1 month, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

 **stevegod0** 1 month, 4 weeks ago

A is correct:

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

upvoted 1 times

 **cattle_rei** 2 months 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** 3 months ago

Selected Answer: A

yep - A

upvoted 1 times

 **EricZhang** 4 months 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** 4 months, 3 weeks ago

Selected Answer: A

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

upvoted 2 times

 **2aldous** 5 months, 1 week ago

Selected Answer: A

Easy question :)

A is the answer.

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

Use AWS Systems Manager to manage patches

upvoted 1 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: A

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

upvoted 1 times

 **gameoflove** 6 months, 4 weeks ago

Selected Answer: A

AWS System Manager support On-premise and EC2 instance patching

upvoted 2 times

 **dev112233xx** 7 months ago

Selected Answer: A

A is correct ofc.. easy one)

upvoted 1 times

 **spencer_sharp** 9 months, 1 week ago

Selected Answer: A

AS THE SAME WITH SAP-C01 QUESTION 782

upvoted 2 times

 **Raj40** 9 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html>

upvoted 3 times

 **zhangyu20000** 9 months, 2 weeks ago

A is correct

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.

 **masetromain** Highly Voted  8 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. 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 9 times

 **rtgfdv3** Highly Voted  9 months, 2 weeks ago

Selected Answer: B

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

 **cattle_rei** Most Recent  4 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** 4 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** 1 month, 1 week ago

Selected Answer: B

d is wrong, shouldn't be "ABANDON"

upvoted 1 times

 **NikkyDicky** 3 months ago

Selected Answer: B

it's a B

upvoted 1 times

 **gameoflove** 4 months, 3 weeks 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** 4 months, 3 weeks 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 1 times

✉ **2aldous** 5 months, 1 week ago

Selected Answer: B

B.

Smart solution :)

upvoted 3 times

✉ **mfsec** 6 months ago

Selected Answer: B

Systems manager + eventbridge

upvoted 3 times

✉ **kiran15789** 6 months, 3 weeks 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** 9 months ago

Selected Answer: B

B

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

upvoted 4 times

✉ **masetromain** 9 months, 2 weeks 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** 9 months, 2 weeks 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

✉ **zhangyu20000** 9 months, 2 weeks ago

B is correct

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

upvoted 2 times

✉ **Raj40** 9 months, 2 weeks ago

Selected Answer: B

Correct answer B

upvoted 4 times

Question #15

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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 22 times

 **kiran15789** Highly Voted  6 months, 3 weeks ago

Selected Answer: CE

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

upvoted 7 times

 **whenthan** Most Recent  1 month 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** 3 months ago

Selected Answer: CE

it's CE

upvoted 1 times

 **Jonalb** 3 months, 1 week ago

Selected Answer: CE

cccccccccccccceeeeeeeeeeee

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: CE

C & E as Issue is associated with authorization

upvoted 1 times

 **SkyZeroZx** 3 months, 2 weeks ago

Selected Answer: CE

C & E as Issue is associated with authorization

upvoted 1 times

 **AWS_Sam** 4 months, 2 weeks ago

C + E are correct

upvoted 1 times

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

Selected Answer: CE

C & E as Issue is associated with authorization

upvoted 1 times

✉ **Maria2023** 5 months, 1 week ago

Selected Answer: CE

C and E are correct

upvoted 2 times

✉ **mfsec** 6 months ago

Selected Answer: CE

CE seems like the best choice

upvoted 2 times

✉ **mKrishna** 6 months, 3 weeks 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

✉ **Musk** 7 months, 2 weeks ago

Selected Answer: CE

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

upvoted 4 times

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

Selected Answer: CE

C and E.

In order to resolve the issue, the solutions architect should create an authorization to associate the private hosted zone in Account A with the new VPC in Account B (Option C). This will allow the new VPC in Account B to access the DNS records stored in the private hosted zone in Account A.

In addition, the solutions architect should associate the new VPC in Account B with the hosted zone in Account A (Option E) and delete the association authorization in Account A. This will ensure that the new VPC in Account B is properly configured to use the private hosted zone in Account A and resolve the db.example.com CNAME record set correctly.

upvoted 4 times

✉ **razguru** 9 months, 1 week ago

C & E are correct options.

upvoted 1 times

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

Selected Answer: CE

With comments and links the answer is C and E. (Ty robertohyène and JosuéXu)

C = 6. Run the following command to create the association between Account A's private hosted zone and Account B's VPC. Use the hosted zone's ID from step 3. B account.

E = 7. It is recommended to remove the association permission after the association is created. This will prevent you from recreating the same association later.

<https://aws.amazon.com/premiumsupport/knowledge-center/route53-private-hosted-zone/>

upvoted 4 times

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

<https://www.examtopics.com/discussions/amazon/view/36113-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

✉ **Raj40** 9 months, 2 weeks ago

Selected Answer: CE

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

upvoted 4 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 18 times

 **spencer_sharp** Highly Voted  9 months, 1 week ago

Selected Answer: C

No brainer

upvoted 9 times

 **cattle_rei** Most Recent  3 weeks, 4 days 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** 2 months, 2 weeks 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

 **totopopo** 2 months 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** 3 months ago

C more cost efficient

upvoted 1 times

 **karim_arous** 3 months, 1 week ago

Selected Answer: C

C without a doubt

upvoted 1 times

 **gameoflove** 4 months, 3 weeks ago

Selected Answer: C

C is only option which meet their requirement

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

Configure an Amazon CloudFront distribution.

upvoted 2 times

✉  **kiran15789** 6 months, 3 weeks ago

Selected Answer: C

y 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** 7 months ago

Selected Answer: C

C ofc.. i hope i will get such easy question in the real exam

upvoted 3 times

✉  **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

C is the correct

upvoted 2 times

✉  **komorebi** 9 months, 2 weeks ago

CCCCCCCCCC

upvoted 3 times

✉  **zhangyu20000** 9 months, 2 weeks ago

C is correct. Do works but not as cheaper as C

upvoted 3 times

✉  **God_Is_Love** 7 months ago

Agree that C is correct, why do you think D is not cheaper ?

upvoted 3 times

✉  **btx** 3 months, 1 week ago

Price per GB-month is cheaper in S3

upvoted 2 times

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

Selected Answer: C

answer C makes sense

upvoted 4 times

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

<https://www.examtopics.com/discussions/amazon/view/6008-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

Question #17

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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 14 times

 **masetromain** 8 months, 2 weeks 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 7 times

 **Sarutobi** 7 months 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 1 times

 **Sarutobi** 7 months ago

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

upvoted 1 times

 **anita_student** 7 months, 1 week ago

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

upvoted 5 times

 **AMohanty** 1 week, 4 days ago

Transit GW - connects both over Private VIF and Transit VIF

upvoted 1 times

 **zozza2023** Highly Voted 7 months, 4 weeks ago

Selected Answer: A

A is the correct solution and the best

upvoted 5 times

 **AMohanty** Most Recent 1 week, 4 days 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** 1 month ago

Selected Answer: A

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

upvoted 1 times

 **NikkyDicky** 3 months ago

Selected Answer: A

It's A.

D is not supported

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: A

A

keyword === Direct Connect gateway

upvoted 1 times

 **gameoflove** 4 months, 3 weeks 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** 6 months ago

Selected Answer: A

Provision a Direct Connect gateway.

upvoted 2 times

 **God_Is_Love** 7 months 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** 9 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

 **spencer_sharp** 9 months, 1 week ago

Selected Answer: A

transit gateway does not support cross-region

upvoted 4 times

 **Mahakali** 7 months, 1 week ago

<https://aws.amazon.com/about-aws/whats-new/2019/12/aws-transit-gateway-supports-inter-region-peering/>

But Still answer is A

upvoted 1 times

 **zhangyu20000** 9 months, 2 weeks ago

A is correct because direct connect gateway supports multi region

upvoted 2 times

 **masetromain** 9 months, 2 weeks ago

Selected Answer: A

I go with A

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

<https://jayendrapatil.com/aws-direct-connect-gateway/>

upvoted 2 times

 **masetromain** 9 months, 2 weeks ago

<https://www.examtopics.com/discussions/amazon/view/69343-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 14 times

 **RaghavendraPrakash** Highly Voted  5 months, 3 weeks 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

 **Arnaud92** 3 weeks, 5 days ago

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

upvoted 1 times

 **Boops** 2 weeks, 5 days ago

"The website contains static content"

Contains do not means that all the website is just static

upvoted 1 times

 **Six_Fingered_Jose** 2 weeks, 3 days ago

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

upvoted 2 times

 **alexua** Most Recent  2 days, 12 hours 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** 3 weeks, 1 day 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** 1 month 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** 1 month, 3 weeks 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 3 times

 **Arnaud92** 3 weeks, 5 days 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 1 times

 **Russ99** 2 months 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

 **giancarloooooo** 2 months, 3 weeks ago

Selected Answer: D

The answer is D because the question says "re-architect" so you don't want to intervene on the software, but only on the management. If the question said "re-factoring" then it would have been C

upvoted 2 times

 **chiajy** 1 month, 4 weeks ago

I support answer D but re-arc & re-fac mean the same thing. [Ref: <https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/>]

upvoted 1 times

 **Mom305** 2 months, 3 weeks ago

Selected Answer: C

Lambda to cover the serverless approach, S3 is way better than EFS, and SQS processes the events from S3

upvoted 1 times

 **NikkyDicky** 3 months ago

Selected Answer: C

C most fitting

upvoted 1 times

 **Jonalb** 3 months, 1 week ago

Selected Answer: C

Static content! guyssssss

upvoted 2 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: C

C is more serverless solutions

upvoted 1 times

 **easystoo** 3 months, 2 weeks ago

C-C-C-C-C-C-C-C-C

upvoted 1 times

 **muurilopes** 3 months, 3 weeks ago

Selected Answer: D

The application needs a backend to process video uploads

upvoted 1 times

 **dev112233xx** 4 months, 1 week ago

Selected Answer: D

How is it possible to host a website in S3???. the website has a STATIC "content" but website itself is NOT STATIC

upvoted 6 times

 **Arnaud92** 3 weeks, 5 days ago

why would they mention that the website has just some static content ? it makes no sense here.

upvoted 1 times

 **BATSIE** 3 months ago

Yes, you can host videos on Amazon S3. Amazon S3 is an object storage service that can store and retrieve any amount of data, including videos, images, and other media files.

While Amazon S3 can be used to host static websites, it is not limited to just that use case. You can use Amazon S3 to store and serve any type of file, including videos. You can also use Amazon S3 in combination with other AWS services such as Amazon CloudFront to deliver video content to users with low latency and high transfer speed

upvoted 1 times

 **nexus2020** 5 months, 2 weeks ago

Selected Answer: C

This solution eliminates the need for managing and scaling EC2 instances for the web application and the worker environment for processing the SQS queue.

upvoted 7 times

 **mfsec** 6 months ago

Selected Answer: C

Host the web application in Amazon S3

upvoted 3 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 16 times

 **whenthan** Most Recent  1 month ago

Selected Answer: B

requirmeents :

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

upvoted 1 times

 **NikkyDicky** 3 months ago

Selected Answer: B

B no dooubt

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: B

100% B

upvoted 1 times

 **gameoflove** 4 months, 3 weeks ago

Selected Answer: B

B solve the problem which is causing in the current scenario

upvoted 1 times

 **2aldous** 5 months, 1 week 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** 6 months ago

Selected Answer: B

Use AWS SAM and built-in AWS CodeDeploy

upvoted 1 times

✉️  **5up3rm4n** 6 months, 1 week 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 1 times

✉️  **kiran15789** 6 months, 3 weeks ago

Selected Answer: B

AWS Serverless Application Model (SAM)

upvoted 1 times

✉️  **spencer_sharp** 9 months, 1 week ago

Selected Answer: B

sam typical use case

upvoted 3 times

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

Selected Answer: B

AWS CodeDeploy is intended for this kind of use

<https://aws.amazon.com/fr/codedeploy/>

upvoted 2 times

✉️  **masetromain** 9 months, 2 weeks 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.

 **tman22** Highly Voted 9 months, 1 week ago

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

upvoted 27 times

 **tman22** 9 months, 1 week 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 9 times

 **zhangyu20000** Highly Voted 9 months, 2 weeks 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 15 times

 **career360guru** Most Recent 3 weeks, 1 day ago

Option A is the only cost effective solution.

Deep Archive can't be used for Web-Hosting. Anyone who thinks that is possible should try it once before selecting that option.

upvoted 3 times

 **bur4an** 3 weeks, 6 days ago

Selected Answer: A

Given the requirements and the need for the lowest cost solution, the best option would be:

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.

Options B and C involve launching EC2 instances which would add unnecessary complexity and cost since the company's priority is to minimize costs. Additionally, option D involves using the S3 Glacier Deep Archive storage class which is intended for long-term archival data and has longer retrieval times, making it less suitable for the given requirements.

upvoted 2 times

 **dkcloudguru** 1 month ago

Option D:

This option involves creating an Amazon S3 bucket and configuring it to use the S3 Glacier Deep Archive storage class as default. This storage class is designed for long-term storage of data that is rarely accessed and can be restored within several hours, offering the lowest cost storage for different access patterns. The S3 bucket is configured for website hosting and an S3 interface endpoint is created

upvoted 1 times

 **whenthan** 1 month ago

Selected Answer: A

large documents storage - s3 and availability and speed of retrieval are no concerns and lowest cost...

upvoted 2 times

 **Simon523** 1 month ago

Selected Answer: D

I think the key words are "Availability and speed of retrieval are not concerns" & "LOWEST cost". Of course user cannot directly access the file, for it require 12 hours to retrieval files, but cause the time is not concern, so I select "D".
upvoted 2 times

b3llman 1 month, 2 weeks ago

A - Glacier Deep Archive will take too long and it will hit the request timeout limit for S3.

upvoted 1 times

chico2023 1 month, 3 weeks ago

Selected Answer: A

This is so tricky, but I would also go with A.

The only reason I go with A is that answer D has "Configure the S3 bucket for website hosting". This part doesn't make sense (unless they were storing other types of static content) as objects archived in Glacier DA have to be restored first. Seriously. If it wasn't that, I would go D.

upvoted 1 times

MRL110 2 months ago

Since there is cost associated with One Zone-IA retrieval as well as interface endpoints, this should be B considering EFS One Zone-IA is cheaper than EBS SC1.

upvoted 2 times

Greyeye 1 month, 1 week ago

us-east-1

EFS - One Zone-Infrequent Access Storage (GB-Month) \$0.0133

EBS sc1 - \$0.015 per GB-month of provisioned storage

that pricing is very close...

upvoted 1 times

MRL110 2 months ago

Also, website access is not possible with interface-endpoints.

(<https://repost.aws/questions/QUu19UpXsTRnaPcg5biU54RA/s3-interface-endpoint>)

upvoted 1 times

Russ99 2 months ago

Selected Answer: A

As to D, S3 Glacier Deep Archive storage should not be used as the default storage for any daily usage. It is designed for long-term archiving of data that is rarely accessed. The default retrieval time for S3 Glacier Deep Archive items is 12 hours, which is too slow for most daily usage.

upvoted 1 times

khksoma 2 months, 1 week ago

It is A.

<https://tutorialsdojo.com/amazon-s3-vs-glacier/>

upvoted 1 times

Magoose 2 months, 2 weeks ago

Selected Answer: D

i dont see anything saying you cant use web hosting with Deep archive. I believe the web hosting is seperate from the storage class.

upvoted 1 times

hirenshah005 2 months ago

You are wrong Sir, Deep Archive can not make public objects even they are in Intranet

upvoted 1 times

Mom305 2 months, 3 weeks ago

Selected Answer: D

About enabling Website hosting in a S3 Bucket, remember that retrieving objects from Glacier Deep Archive will temporarily make the objects available into a Standard S3 bucket (which you can enable with Website hosting)

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects.html>

upvoted 2 times

NikkyDicky 3 months ago

Selected Answer: A

A

D is not usable

upvoted 1 times

dkx 3 months ago

S3 can be used to host static web content, while Glacier cannot. In S3, users create buckets. In Glacier, users create archives and vaults.

<https://tutorialsdojo.com/amazon-s3-vs-glacier/>

upvoted 2 times

Jonalb 3 months ago

Selected Answer: D

DDDDDDDDDDDDDDDD sorry guys

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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 20 times

 **masetromain** 8 months, 2 weeks 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 8 months, 1 week ago

Selected Answer: A

A 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 9 times

 **whenthan** Most Recent 3 weeks, 4 days ago

Selected Answer: C

More comprehensive approach

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

upvoted 1 times

 **whenthan** 3 weeks, 4 days ago

C provides more comprehensive approach

upvoted 1 times

 **bur4an** 3 weeks, 6 days 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

 **venvig** 1 month, 1 week ago

Option C is NOT correct because of the following reasons

While IAM can use a SAML 2.0 identity provider for federation, managing cross-account IAM users introduces complexity and can be challenging.

Provisioning IAM users mapped to federated users is a manual, cumbersome process.

Managing user identities across multiple AWS accounts rather than a single location doesn't align well with the company's requirement.

It may not easily provide the granular, conditional access based on user groups and roles in the Active Directory, especially across multiple accounts.

So, Answer A is correct

AWS Single Sign-On (SSO) is designed to integrate with identity sources, including on-premises Active Directory, via SAML 2.0.

AWS SSO supports automatic provisioning with SCIM.

With AWS SSO, you can grant access to AWS accounts using attribute-based access controls (ABACs), which provides the conditional access based on user groups and roles.

It meets the requirement of managing user identities in a single location.

upvoted 1 times

 **chico2023** 1 month, 3 weeks ago

Selected Answer: A

Answer: A

"The company's security policy requires conditional access to the accounts based on **user groups and roles**"

C would require an IdP to work.

upvoted 1 times

 **awsrd2023** 2 months, 3 weeks ago

Selected Answer: A

Perfectly matches the requirement

upvoted 1 times

 **NikkyDicky** 2 months, 4 weeks ago

Selected Answer: A

it's A

upvoted 1 times

 **javitech83** 3 months ago

Selected Answer: B

B is perfectly possible, we use it in my organization. AD could be possible but A is easier to implement and fully covers the requirement. It uses same authentication service, users are only managed in the active directory, and permissions are assigned based on the Active Directory groups that the user belongs to, and that are synchronized with AWS SSO using SSO and permission sets.

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: A

Here's how this solution satisfies the requirements:

Connect to Active Directory: AWS IAM Identity Center (AWS Single Sign-On) can be configured to integrate with Active Directory using SAML 2.0. This allows for the synchronization of user identities and authentication with the on-premises Active Directory service.

Automatic provisioning: By enabling automatic provisioning using the SCIM v2.0 protocol, user identities can be automatically provisioned and deprovisioned based on changes in the Active Directory. This ensures that user management remains centralized in a single location.

Attribute-based access controls (ABACs): AWS IAM Identity Center supports ABACs, which allow for conditional access to AWS accounts based on user groups and roles. This enables fine-grained control over access to the AWS resources based on attributes associated with the user identities in the Active Directory.

upvoted 1 times

 **Maria2023** 3 months, 1 week ago

Selected Answer: A

Initially I went for B, because I use permissionsets to assign policies in AD-to-AWS integrations. But that part - "Configure AWS IAM Identity Center (AWS Single Sign-On) by using IAM Identity Center as an identity source" means to abandon SAML and SCIM. Think the question is trick by nature and neither answer is completely right. You don't definitely need to use attributes - standard scenario is to provision users and groups and assign groups to accounts and permissionsets.

upvoted 1 times

 **geo1551** 3 months, 2 weeks ago

B

<https://docs.aws.amazon.com/singlesignon/latest/userguide/permissionsetsconcept.html>

upvoted 2 times

 **johnballs221** 3 months, 2 weeks ago

Selected Answer: D

I think A is wrong because ABAC refers to utilizing tags for access control, in this case we are required to use access control based on roles and groups, which is RBAC.

upvoted 1 times

 **chathur** 3 months, 4 weeks ago

Selected Answer: A

The fill guide is here.

<https://aws.amazon.com/blogs/security/configure-aws-sso-abac-for-ec2-instances-and-systems-manager-session-manager/>

upvoted 1 times

 **emiliocb4** 4 months ago

Selected Answer: B

B because AWS IAM Identity Center (AWS Single Sign-On) and to manage in a single point the user permission with the permission set. I'm using the same in my organization.

upvoted 4 times

 **rtguru** 4 months ago

I go with C

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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 26 times

 **masetromain** 8 months, 2 weeks 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 8 times

 **zhangyu20000** Highly Voted  9 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

 **whenthan** Most Recent  3 weeks, 4 days 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** 3 weeks, 6 days 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 1 times

 **CloudHandsOn** 1 month, 1 week 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** 1 month, 1 week ago

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

upvoted 1 times

 **chico2023** 1 month, 3 weeks 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** 1 month, 3 weeks ago

Selected Answer: B

code 429 means "Too many requests"

upvoted 1 times

 **aviathor** 2 months, 3 weeks ago

Selected Answer: A

There is no indication in the problem statement that the errors are caused by the API being overwhelmed with requests. It also states that the errors being displayed to the user are damaging to the application's reputation. Therefore the priority should be to avoid the errors being reported to the users, hence A.

upvoted 1 times

 **NikkyDicky** 2 months, 4 weeks ago

Selected Answer: B

B - because of the issue with large number of requests from small number of clients

upvoted 1 times

 **nqg54118** 3 months, 2 weeks ago

Selected Answer: A

exponential backoff

https://docs.aws.amazon.com/ja_jp/sdkref/latest/guide/feature-retry-behavior.html

upvoted 1 times

 **dev112233xx** 4 months, 1 week ago

Selected Answer: A

A makes more sense

upvoted 1 times

 **chikorita** 4 months ago

no bro

upvoted 1 times

 **aviathor** 2 months, 3 weeks ago

Not helpful... :)

upvoted 1 times

 **liangcw305** 4 months, 2 weeks ago

Selected Answer: B

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

upvoted 1 times

 **OnePunchExam** 5 months, 3 weeks ago

Selected Answer: A

- B is incorrect. We use throttling for APIs to help protect them from being overwhelmed by too many requests (which is not the issue here!). Also the question did not say error 429 is going to be returned.
- With retry, there is a chance the API will work thus resulting in successful response.
- Also if all else fails, return descriptive error messages is more elegant than throwing unhandled exceptions.

upvoted 5 times

 **aviathor** 2 months, 3 weeks ago

That was my thought too. It is not possible to conclude from the problem statement that the errors are caused by lack of capacity on the API side.

upvoted 1 times

 **Asagumo** 5 months, 3 weeks ago

Selected Answer: D

The answer is D, but the SLA numbers do not matter.

This existing system normally runs with 12 machines in a redundant configuration, so in the event of a failure, the system will run with 6 machines

and process scheduled jobs at 100% occupancy, giving priority to SLAs. In other words, even after migrating to EC2 instances, it is only necessary to be able to run 6 instances for scheduled jobs.

upvoted 1 times

 **Asagumo** 5 months, 3 weeks ago

Selected Answer: A

The problem statement "clients can tolerate retries of unsuccessful calls" can be interpreted as allowing end users to wait indefinitely. On the other hand, the problem statement "the errors are displayed to customers and are causing damage" can be interpreted to mean that the error page should be made to not appear.

If these are satisfied, it is A.

upvoted 5 times

 **mfsec** 6 months ago

Selected Answer: B

B is correct

upvoted 1 times

 **God_Is_Love** 7 months ago

Logical answer : While catching errors and showing nice error message is good for customers, it still does damage to API as clients think API is not working/responding well.

Retry and showing nice error will still invoke frustration to clients and damage to API :-)

As the api is being bombarded with small number of clients (note they are successfully

authenticated already trying to update resources with PUT) so assuming they are just bombarding with 429 too many requests.

So API throttling helps. Caching may give stale data (C is not apt here) Reserved concurrency when lambda is overloaded (D is not a fit either). B should be correct

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.

 **sambb** Highly Voted  7 months 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 is you can install a gateway in AWS, but Amazon would never advise this
 upvoted 9 times

 **Tofu13** 1 day, 8 hours ago

<https://aws.amazon.com/blogs/storage/new-enhancements-for-moving-data-between-amazon-fsx-for-lustre-and-amazon-s3/>
 upvoted 1 times

 **dqwswwwvtgxwkvgcvc** 1 month, 1 week ago

There is one S3 file gateway

<https://aws.amazon.com/storagegateway/file/s3/>
 upvoted 1 times

 **b3llman** 1 month, 2 weeks 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

 **bur4an** Most Recent  3 weeks, 6 days 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

 **dqwswwwvtgxwkvgcvc** 1 month, 1 week 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

 **chico2023** 1 month, 3 weeks 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 4 times

 **chiajy** 1 month, 4 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** 2 months 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 1 times

 **Asamara** 2 months, 3 weeks 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** 2 months, 3 weeks 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** 2 months, 4 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

 **Jonalb** 3 months, 1 week ago

Selected Answer: A

S3 Intelligent-Tiering !!!! ITS A
upvoted 1 times

 **hitesh24** 3 months, 3 weeks ago

By migrating the data to an S3 bucket with the S3 Intelligent-Tiering storage class, you can take advantage of cost optimization. S3 Intelligent-Tiering automatically moves data between two access tiers: frequent access and infrequent access, based on usage patterns. This ensures that data is stored cost-effectively while providing high performance when needed.

Using Amazon FSx for Lustre to create a new file system with the data from Amazon S3 using lazy loading allows for efficient access to the required subset of files during the monthly job. The file system is created on-demand and the data is loaded only when accessed, which helps reduce costs as you only pay for the storage and compute resources used during the job.

Deleting the file system when the job is complete ensures that you are not incurring any additional costs for the shared storage when it is not needed.

Therefore, option A provides the largest overall cost reduction while still meeting the performance requirements for the monthly job.

upvoted 4 times

 **gameoflove** 4 months, 3 weeks ago

Selected Answer: D

D is the most logical answer
upvoted 2 times

 **jj22222** 5 months, 3 weeks ago

Selected Answer: A

S3 intelligent tiering
upvoted 3 times

 **mfsec** 6 months ago

Selected Answer: A

A is the best choice

upvoted 1 times

 **cudbyanc** 6 months, 1 week ago

Selected Answer: A

definitely A

upvoted 2 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: A

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

upvoted 1 times

 **hobokabobo** 7 months ago

Selected Answer: A

A: provides High performance Access

B: EBS is by far more expensive than s3.

C: Lustre with Lazy Loading(A) is Cheaper than Batch loading

D: might be cheaper than A but does not provide High performance Access.

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.

 **God_Is_Love** Highly Voted  7 months 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 5 times

 **Simon523** Most Recent  3 weeks, 1 day ago

Selected Answer: C

Other option haven't mention multi AZ

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: C

Static IP-> NLB

upvoted 1 times

 **NikkyDicky** 2 months, 4 weeks ago

Selected Answer: C

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

upvoted 1 times

 **GilbertJorge** 3 months, 1 week 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** 3 months, 1 week ago

Selected Answer: C

Create one Elastic IP address for each Availability Zone.

upvoted 1 times

 **AWS_Sam** 4 months, 2 weeks ago

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

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

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

upvoted 2 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: C

IP address using NLB

upvoted 1 times

 **saurabh1805** 7 months ago

Selected Answer: C

C looks correct.

upvoted 2 times

 **zozza2023** 7 months, 4 weeks 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** 8 months ago

Selected Answer: C

C looks correct. I did not read the rest.

upvoted 1 times

 **masetromain** 8 months, 2 weeks 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 4 times

 **masetromain** 9 months, 2 weeks ago

Selected Answer: C

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

upvoted 2 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.

 **_lasco_** Highly Voted  7 months 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 14 times

 **joefromnc** Most Recent  4 weeks, 1 day ago

Can not be C because Savings Plans require long term commitment.

upvoted 2 times

 **Russ99** 1 month, 2 weeks ago

Selected Answer: D

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

upvoted 1 times

 **ggrodsckiy** 1 month, 3 weeks 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 3 times

 **joefromnc** 4 weeks, 1 day ago

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

upvoted 1 times

 **awsr2023** 2 months, 3 weeks 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 affect tight SLA - is actually 35/65 instead of 65/35).
- C. Savings Plan (Against no long term commitments requirement).

upvoted 3 times

 **NikkyDicky** 2 months, 4 weeks ago

Selected Answer: D

D

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

upvoted 1 times

 **aca1** 4 months 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** 4 months, 2 weeks 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** 5 months, 1 week 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** 5 months, 1 week 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** 5 months, 2 weeks ago

Option C as per ChatGPT

upvoted 2 times

 **rxhan** 5 months, 1 week ago

ChatGPT gave me option D

upvoted 3 times

 **Amac1979** 6 months 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 2 times

 **mfsec** 6 months ago

Selected Answer: D

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

upvoted 2 times

 **higashikumi** 6 months ago

The solution that meets the requirements most cost-effectively is 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.

upvoted 1 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: D

D -> No long term commitment. Please hourly jobs require 65% capacity

upvoted 1 times

 **dev112233xx** 6 months, 3 weeks ago

Selected Answer: C

I can't understand people who voted D.. Capacity Reserved instances are very expensive and have the same price of on-demand so it's not a "cost-effectively" solution .

C is the most cost effectively solution that also makes sense.

upvoted 1 times

 **NPN** 6 months, 3 weeks ago

Option-C uses savings plan and needs commitment; The question says no long-term commitment; Hence option-D is the best.

upvoted 6 times

 **sambb** 7 months ago

Selected Answer: D

D has no long term commitment (e.g. saving plans) and has 75% on demand instances / 25% spot instances which is near the requirements

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.

 **Untamables** Highly Voted  9 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 12 times

 **OnePunchExam** 5 months, 3 weeks 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 5 times

 **karma4moksha** Highly Voted  4 months, 2 weeks 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 6 times

 **whenthan** Most Recent  3 weeks, 3 days 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** 1 month, 1 week 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 1 times

 **chico2023** 1 month, 3 weeks ago

Selected Answer: A

Answer: A

upvoted 1 times

 **NikkyDicky** 2 months, 4 weeks ago

Selected Answer: A

it's n A

upvoted 1 times

 **rtguru** 4 months ago

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

upvoted 1 times

 **gameoflove** 4 months, 2 weeks ago

Selected Answer: A

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

upvoted 1 times

 **chiplyti** 5 months ago

Selected Answer: A

A correct

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

Secrets Manager RotationSchedule resource

upvoted 1 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: A

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

upvoted 1 times

 **_lasco_** 7 months 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

 **cudbyanc** 7 months ago

Selected Answer: A

The best solution is either A or C, but A may be the LEAST amount of operational overhead since it uses AWS Secrets Manager's built-in rotation functionality.

upvoted 3 times

 **God_Is_Love** 7 months ago

Logical answer : Secrets manager only can support password rotation, not parameter store.

Parameter store is just a location as its name suggest to refer to or

be referred from elsewhere. B,D are eliminated.C is wrong

because, there is no necessity for event bridge rule to capture known 90 days trigger.

Rotation schedule is already available when you configure a secret in Secrets manager.

That leaves option A as correct

upvoted 3 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: A

Secrets Manager support RotationSchedule.

upvoted 1 times

 **Musk** 8 months ago

Selected Answer: A

Option B is not wrong, but it has more operational overhead compared to option A. Option B uses AWS Systems Manager Parameter Store, which is less automated and requires manual intervention to perform password rotation. Option A uses AWS Secrets Manager, which provides a built-in mechanism to rotate secrets, reducing operational overhead.

upvoted 1 times

 **masetromain** 8 months, 2 weeks ago

Selected Answer: A

Option A is the correct answer because it meets the security engineer's requirements with the least amount of operational overhead. This option uses AWS Secrets Manager to generate the database password as a secret resource, which is a secure and managed service for storing and rotating secrets such as database credentials. The CloudFormation template also includes a Lambda function resource to rotate the password, and a Secrets Manager RotationSchedule resource to schedule the password rotation every 90 days.

This option is the correct answer because it is the best way to manage the password rotation, Secrets Manager is a fully managed service that encrypts and stores the credentials and rotates the credentials automatically, and CloudFormation is used to automate the deployment of the resources.

upvoted 3 times

Question #27

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 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.
- 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.

 **Untamables**  9 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 19 times

 **rodrod**  1 week, 4 days ago

Selected Answer: BC

I've read similar questions previously, keyword is "simple API".

REST API adds more features than HTTP API and is consider "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 1 times

 **bur4an** 3 weeks, 5 days 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** 1 month, 2 weeks 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** 1 month, 3 weeks ago

Selected Answer: AC

Answer: A and C

upvoted 1 times

 **pupsik** 2 months, 1 week ago

Selected Answer: AB

<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>

upvoted 1 times

 **pupsik** 2 months, 1 week 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** 2 months, 4 weeks ago

Selected Answer: AC

AC

B is not supported by HTTP API GWY

upvoted 1 times

✉ **Jonalb** 3 months ago

Selected Answer: AC

AAAACCCC

upvoted 1 times

✉ **chathur** 3 months, 4 weeks ago

Selected Answer: AC

HTTP API is a light-weighted REST API that only supports two types of backend, Lambda and HTTP while REST API supports three backend: Lambda, HTTP and AWS services (DynamoDB for example).

Source: <https://medium.com/@fengliplatform/api-gateway-talks-to-dynamodb-in-two-ways-f45356c87986>

This is a tutorial with screenshots, which means A & C are doable

upvoted 4 times

✉ **ailves** 3 months, 1 week ago

According to <https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>, HTTP API also support AWS Services (like DynamoDB)

upvoted 1 times

✉ **ailves** 3 months, 1 week ago

Really HTTP support: Lambda, HTTP backends

upvoted 1 times

✉ **mKrishna** 4 months ago

A & C.

Serverless pattern diagrams at <https://serverlessland.com/patterns?services=apigw%2CYNAMO>

upvoted 2 times

✉ **OnePunchExam** 5 months, 3 weeks ago

Selected Answer: AC

A & C.

A <https://aws.amazon.com/blogs/compute/using-amazon-api-gateway-as-a-proxy-for-dynamodb/>

C <https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-dynamo-db.html>

Also do learn when to use API GW REST vs HTTP

upvoted 1 times

✉ **mfsec** 6 months ago

Selected Answer: AC

AC is a good fit

upvoted 2 times

✉ **mKrishna** 6 months, 3 weeks ago

Ans is A & C

Option B: HTTP APIs do not currently support integrations with DynamoDB, and therefore this solution would not work.

Option D: AWS Global Accelerator and AWS Lambda@Edge, which both involve infrastructure management.

Option E: NLB does not meet the requirement of being serverless.

upvoted 2 times

✉ **kiran15789** 6 months, 3 weeks ago

Selected Answer: AC

going with A and C

upvoted 1 times

✉ **_lasco_** 7 months ago

Selected Answer: AC

I voted A and C

Api gateway REST APis support direct integration with DynamoDb

The same can be achieved with HTTP APIs using a lambda between the two

upvoted 2 times

✉ **Gabehcoud** 7 months ago

Think it should CD. snippet from the link <https://aws.amazon.com/api-gateway/faqs/> below

HTTP APIs are ideal for:

Building proxy APIs for AWS Lambda or any HTTP endpoint

Building modern APIs that are equipped with OIDC and OAuth 2 authorization

Workloads that are likely to grow very large

APIs for latency sensitive workloads

REST APIs are ideal for:

Customers looking to pay a single price point for an all-inclusive set of features needed to build, manage, and publish their APIs.

upvoted 1 times

 **God_Is_Love** 7 months ago

API Gateway is the solution for simple API. D is Cloudfront/Lambda@edge solution for faster response. Requirement says API. So D gets eliminated. E is irrelevant

of course. B is wrong because DynamoDB vs Dynamo DB.(no brainer) That leaves A and C as correct answers. (If question asks for more secure not exposing DynamoDB directly, I'd go for C)

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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 19 times

 **masetromain** 8 months, 2 weeks 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 4 times

 **Arnaud92** 6 months, 1 week ago

Wrong for B, Lambda can be an ALB target, you do not need web server

upvoted 4 times

 **Shahul75** 7 months, 3 weeks ago

SAN cannot handle redirects. We need to do http - https

upvoted 1 times

 **vjp_training** Most Recent  1 week ago

Selected Answer: BEF

trust me

upvoted 1 times

 **Simon523** 2 weeks, 2 days 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 1 times

 **Greyyeye** 1 month, 1 week 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 1 times

 **chico2023** 1 month, 3 weeks ago

Selected Answer: BCF

Answer: B, C and F.

upvoted 2 times

 **ggrodsckiy** 1 month, 3 weeks 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 2 times

 **softarts** 1 month, 3 weeks ago

Selected Answer: BEF

correct answer is BEF

explained in neal's practice test6,Q28

upvoted 1 times

 **softarts** 1 month, 3 weeks 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 1 times

 **softarts** 1 month, 3 weeks 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 1 times

 **NikkyDicky** 2 months, 4 weeks ago

Selected Answer: BCF

CEF . although BCF seems workable and low ope overhead too

upvoted 1 times

 **Parimal1983** 3 months 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

 **Maria2023** 3 months, 1 week ago

Selected Answer: CEF

Hopefully that will do the job for CloudFront origin, since that was my main concern -

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html#concept_lambda_function_ur

upvoted 1 times

 **bex** 3 months, 1 week ago

All the responses that say that D (API Gateway) has nothing to do here because it is an API are wrong. API Gateway would be a valid solution for the redirects and calling Lambda. HOWEVER, the question says that the solution MUST accept HTTP and HTTPS. API Gateway in HTTPS-only.

upvoted 2 times

 **chathur** 3 months, 4 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 4 times

 **aca1** 4 months ago

Selected Answer: BCF

Should be B, C and F.

I was in doubt about the ALB or CloudFront, but to use CloudFront you need a Oring (The Lambda@Edge is not the Orgin, if will work between

the User and CloudFront or CloudFront and the Origin), in this scenario you do not have a Origin, so using a CloudFront here is an incomplete solution.

upvoted 1 times

dev112233xx 4 months ago

Selected Answer: CDF

after long investigating i vote: C,D,F

API Gateway + Lambda a perfect serverless solution to redirect URLs

Lambda just needs to return the URL with http code 301

Cloudfront: is mainly used for caching. so i don't like this solution

ALB: i prefer API Gateway which is more light weight and faster and ofc it's serverless

upvoted 1 times

gameoflove 4 months, 2 weeks 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 3 times

MikelH93 4 months, 4 weeks ago

Selected Answer: CEF

Firstly, need serverless service because "LEAST amount of operational effort"

A Wrong because overhead

B wrong because ALB not serverless

C right because use lambda to redirect

D No sense here, no need.

E cloudfront is serverless and can handle http -> https and also handle lambda function close to user with Lambda@Edge

F Need certificate to https

upvoted 2 times

Sarutobi 5 months, 1 week ago

Selected Answer: BCF

I will use ALB instead of CloudFront here, but both can work.

upvoted 2 times

y0eri 4 months, 3 weeks ago

No: <https://stackoverflow.com/a/73395412>

upvoted 3 times

Sarutobi 4 months, 2 weeks ago

Thank you so much for pointing out this link; if you scroll down to the end, there is another link to <https://medium.com/trainingdock/http-redirects-with-lambda-c20cf7934060>; the link provides the TF code to deploy and test. The only change I made was to manually create a cert for the resource `aws_lb_listener.https_listener`. The only reason I would go with B instead of C here is that B states that we have both HTTP and HTTPS listeners, while E does not clarify that (it can be configured to HTTPS only, although the default is HTTP/HTTPS).

upvoted 1 times

Sarutobi 4 months, 2 weeks ago

In my previous post, I said, "with B instead of C here is", that was wrong I meant to say "with B instead of *E* here is".

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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 9 times

 **dkx** 3 months 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 6 times

 **chathur** 3 months, 4 weeks ago

User-defined tags can not be allowed from management accounts in AWS Organization. It must done from the management Account.

upvoted 1 times

 **Untamables** Highly Voted 9 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

 **whenthan** Most Recent 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/whitepapers/latest/tagging-best-practices/building-a-cost-allocation-strategy.html>

upvoted 1 times

 **bur4an** 3 weeks, 5 days 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 2 times

 **NikkyDicky** 2 months, 4 weeks ago

it's an A

upvoted 1 times

 **rtguru** 4 months ago

I go with D

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

Cost center tag int he management account.

upvoted 1 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: A

Management account for reports

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: A

Answer A

upvoted 2 times

 **yimicc** 9 months ago

Selected Answer: C

Should be a C

upvoted 1 times

 **yimicc** 9 months ago

Change to A, the activation of user tag for billing can only be done by management account

upvoted 5 times

 **tman22** 9 months, 1 week ago

A. You want the cost information across all accounts - So you use the management account.

upvoted 4 times

 **masetromain** 9 months, 2 weeks 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.

 **Simon523** 3 weeks, 1 day 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** 2 months, 4 weeks ago

AC of course

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: AC

AC are my choice.

upvoted 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: AC

A and C are the answer for me

upvoted 2 times

 **masetromain** 8 months, 2 weeks 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 4 times

 **Untamables** 9 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** 9 months, 2 weeks 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 7 times

 **SK_Tyagi** 1 month, 1 week ago

The catch is the "Create an organization root-level SCP to deny permissions". I'd refrain from creating a root-level SCP

upvoted 1 times

 **qxy** Most Recent 3 weeks ago

Selected Answer: C

Clearly, it's C.

upvoted 1 times

 **Karamen** 1 month, 1 week 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 1 times

 **SorenBendixen** 1 month, 2 weeks 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** 1 month, 2 weeks ago

Its C. D is wrong - missed : "procurement-manager-role in all AWS accounts that will be used by DEVELOPERS"

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

Its a C

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: C

C is correct-

upvoted 1 times

 **Maria2023** 3 months, 1 week 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 2 times

 **Jackhemo** 3 months, 1 week 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** 4 months ago

Correct answer is D

upvoted 1 times

 **chikorita** 3 months, 4 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** 5 months, 1 week 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 2 times

 **mfsec** 6 months ago

Selected Answer: C

Create an IAM role named procurement-manager-role in all the shared services accounts in the organization.

upvoted 1 times

 **cudbyanc** 7 months ago

Selected Answer: C

Confirmed

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

should be C i guess

upvoted 1 times

 **ask4cloud** 8 months, 1 week ago

Selected Answer: C

This approach allows the procurement managers to assume the procurement-manager-role in shared services accounts, which have the AWSPrivateMarketplaceAdminFullAccess managed policy attached to it and can then manage the Private Marketplace. The organization root-level SCP denies the permission to administer Private Marketplace to everyone except the role named procurement-manager-role and another SCP denies the permission to create an IAM role named procurement-manager-role to everyone in the organization, ensuring that only the procurement team can assume the role and manage the Private Marketplace. This approach provides a centralized way to manage and restrict access to Private Marketplace while maintaining a high level of security.

upvoted 3 times

 **masetromain** 9 months, 2 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/28410-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 3 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.

 **zhangyu20000** Highly Voted  9 months, 2 weeks ago

B is correct because default FullAWSAccess SCP is applied
upvoted 7 times

 **Six_Fingered_Jose** Most Recent  1 week, 3 days 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 1 times

 **AMohanty** 2 weeks, 1 day ago

A
SCP is a DENY statement, its NOT designed to PERMIT/ALLOW service access.
upvoted 1 times

 **chico2023** 1 month, 3 weeks ago

Selected Answer: A

Answer: A
upvoted 1 times

 **chico2023** 1 month, 3 weeks ago

As bad as it sounds, I still think it's the less wrong answer and I can explain my understanding below:

upvoted 1 times

chico2023 1 month, 3 weeks ago

By reading the answer "Remove the FullAWSAccess SCP from the developers account's OU", it's clear that you are removing the "FullAWSAccess SCP" from the developers OU, not from the Root OU. This way, if the company has a FullAWSAccess SCP (as AWS managed policy) in the Root OU, removing the same one from the Developer, won't change a thing.

C doesn't make much sense the way it was put. If it is a managed policy, you can't change. If it's not, why modify it with a deny? It would be much better to just detach it and attach a more restrictive one.

I wouldn't choose D as answer because if you have both a deny and an allow statement in a SCP, the deny statement takes precedence over the allow statement.

In summary, as we don't know if they have a FullAWSAccess SCP in their root account, or are using an allow list, the only way I can think (at least for now) to be sure that developers won't be able to use services outside the scope of the aforementioned policy, is by denying the rest described in A.

upvoted 2 times

Christina666 2 months, 3 weeks ago

Selected Answer: B

If you reenable SCPs on the organization root, all entities are reset to being attached to only the default FullAWSAccess SCP.

upvoted 1 times

SmileyCloud 2 months, 4 weeks ago

Selected Answer: D

It's D actually. If you remove the FullAWSAccess you are still inheriting the same policy from the root account. See this:
<https://imgur.com/a/2EMUm0S>

This means you have to remove the same SCP from root. On top of that, AWS has the same use case here ->
<https://aws.amazon.com/blogs/industries/best-practices-for-aws-organizations-service-control-policies-in-a-multi-account-environment/>

upvoted 2 times

Arnaud92 2 months, 2 weeks ago

Is it a recommended practice to have a FullAWSAccess + a Deny in another SCP?

upvoted 1 times

NikkyDicky 2 months, 4 weeks ago

Selected Answer: B

Replace default allow SCP

upvoted 1 times

Parimal1983 3 months ago

Selected Answer: B

Instead of creating explicit deny for each and every service, it is efficient way to remove root level allow SCP for all services and add explicit SCP with EC2, S3 and DynamoDB to developer OU

upvoted 3 times

ailves 3 months, 1 week ago

Selected Answer: B

According to https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_strategies.html we have to replace (not remove) SCP.

"To use SCPs as an allow list, you must replace the AWS managed FullAWSAccess SCP with an SCP that explicitly permits only those services and actions that you want to allow".

upvoted 3 times

gameoflove 4 months, 2 weeks ago

Selected Answer: B

FullAWSAccess must be resolved

upvoted 1 times

Maria2023 5 months, 1 week ago

Selected Answer: B

Initially I voted for A but then I saw the following statement : "AWS services that aren't explicitly allowed by the SCPs associated with an AWS account or its parent OUs are denied access to the AWS accounts or OUs associated with the SCP. SCPs associated to an OU are inherited by all AWS accounts in that OU"

upvoted 1 times

Sarutobi 5 months, 1 week ago

Selected Answer: D

B says: "Remove the FullAWSAccess SCP from the developers account's OU", with the information we have here there is no way to guarantee the SCP is applied to the developers account's OU. It can be any place from the root all the way down to the developer's OU.

upvoted 2 times

frfavoreto 5 months, 2 weeks ago

Selected Answer: B

'B' is the BEST answer, but not the only correct one.

'D' is also technically correct, because adding a wildcard DENY statement would override the FullAWSAccess SCP attached by default to the OU and it would have the same final result.

However 'B' is more appropriate here, the so called best practice. This is what 'Professional' exam certs are all about.

upvoted 2 times

✉ **mfsec** 6 months ago

Remove the FullAWSAccess SCP from the developers account's OU

upvoted 1 times

✉ **Ajani** 6 months, 3 weeks ago

An allow list strategy has you remove the FullAWSAccess SCP that is attached by default to every OU and account. This means that no APIs are permitted anywhere unless you explicitly allow them. To allow a service API to operate in an AWS account, you must create your own SCPs and attach them to the account and every OU above it, up to and including the root. Every SCP in the hierarchy, starting at the root, must explicitly allow the APIs that you want to be usable in the OUs and accounts below it

A deny list strategy makes use of the FullAWSAccess SCP that is attached by default to every OU and account. This SCP overrides the default implicit deny, and explicitly allows all permissions to flow down from the root to every account, unless you explicitly deny a permission with an additional SCP that you create and attach to the appropriate OU or account

If the developers can access other services it implies the "Deny List Strategy" hence FullAWSAccess is in place and should be removed

upvoted 3 times

✉ **Gabehcoud** 7 months ago

the question doesn't state that there is another SCP applied to developers account. By choosing B, are we just assuming ? Why can't it be D?

upvoted 2 times

✉ **atlasga** 5 months, 2 weeks ago

It's applied by default.

upvoted 2 times

✉ **moota** 7 months, 2 weeks ago

I was confused at first but the intersection of sets here allowed me to understand the flow of SCPs from root to child OUs
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_inheritance_auth.html

upvoted 2 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.

 **EricZhang** Highly Voted 9 months, 2 weeks ago

Selected Answer: A

Serverless requires least operational effort.

upvoted 22 times

 **dqwsmwvtgxwkvvcv** 1 month, 1 week 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

 **Jay_2pt0_1** 4 months, 1 week 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

 **lkyixoayffasdrilaqd** 7 months 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 8 times

 **scuzzy2010** 5 months, 2 weeks ago

Separating would be development overhead, but once done, the operational overheard (operational = ongoing day-to-day) will be the least.

upvoted 6 times

 **jooncco** Highly Voted 7 months, 4 weeks 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 14 times

 **scuzzy2010** 7 months 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 5 times

 **aviathor** 2 months, 3 weeks 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** 4 months, 4 weeks ago

A monolithic REST api likely has a gazillion individual APIs. This refactor would not be a small one.

upvoted 4 times

 **chathur** 3 months, 4 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 1 month, 2 weeks 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 1 times

AMohanty Most Recent 2 weeks, 1 day ago

A.

D doesn't talk of scaling in or scaling out based on Load. That eliminates D

C why do you require a lambda to update R53. EC2 <- ASG <- APIGW <- ALB R53 should do the job

B doesnt again talk about ScalingIn and Scaling out

Option A, is viable.

upvoted 1 times

Simon523 3 weeks, 1 day ago

Selected Answer: A

The problem here is "The app has not been able to keep up with the traffic." so it doesn't cause the EC2 not enough resource, so I guess C is not correct.

upvoted 1 times

tom10271 4 weeks, 1 day ago

Selected Answer: C

The core problem is '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 never solve the problem as the bottleneck is still on the EC2 instances.

B would take tons of efforts.

D uses ALB only which do not have any autoscaling feature.

C must be the only correct answer

upvoted 1 times

Sweetadad 1 month ago

Does ALB even support Rest API (unless you use it with APIGW)? I would go with either A (less right) or C

upvoted 1 times

dqwswwwvtgxwkvgcvc 1 month, 1 week ago

Selected Answer: D

Answer D uses ALB to balance to replace Route 53 multivalue answer routing policy for proper load balancing.

upvoted 2 times

chico2023 1 month, 3 weeks ago

Selected Answer: D

Answer: D

I can't believe that SAP-C02 has this type of questions. Least operational overhead should be A, however the question says exactly this: "A solutions architect needs to implement a solution so that the app can handle the new and varying load."

In any moment it says "...implement a solution so that the NEW app can handle..."

C is a possibility, but to "Create an AWS Lambda function that reacts to Auto Scaling group changes and updates the Route 53 record"? I wouldn't even think suggesting this, unless customer really wants it.

Answer D has the "where is the ASG to handle spikes in traffic" thing, but it's the less worse in my opinion as the issue seems to be related to poor distribution of requests as seen here: "The company has created a Route 53 multivalue answer routing policy with the IP addresses of all the EC2 instances"

upvoted 2 times

Asds 2 months, 2 weeks ago

Selected Answer: A

Can't be C as they don't mention elb at all

Which leads to....A

upvoted 1 times

softarts 2 months, 2 weeks ago

Selected Answer: D

should be D, from a developer point of view.

A - move implementation from EC2 to lambda? not possible to be least overhead

B - EKS also lot overhead

C - why use lambda to update route53 records?

D - correct answer

upvoted 1 times

✉  **awsrd2023** 2 months, 2 weeks ago

Selected Answer: A

A: Serverless - Least OPS overhead.

Rule Out Factors:

B: K8s - OPS overhead + Dev overhead.

C: ASG + Lambda seems impractical for sudden and large traffic surges.

D: ALB + EC2 is good, but ASG is missing so not addressing traffic surges.

upvoted 2 times

✉  **Christina666** 2 months, 3 weeks ago

I thought it was C, but the question is "least operational", serverless beats option C I guess, I choose A. Please delete my last comment @Examtopics

upvoted 1 times

✉  **Christina666** 2 months, 3 weeks ago

Selected Answer: A

I thought it was C, but the question is "least operational", serverless beats option C I guess, and this question only has 5 instances, so I choose A

upvoted 1 times

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

Selected Answer: A

It's A, keyword here is "least operational" not "least development". So, yes the development effort with A is higher than C, but operational is lower because i don't have to worry about EC2, patching, upgrades, monitoring etc.. "least operational" <<<---

upvoted 1 times

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

Selected Answer: A

Lambda - least ops overhead

upvoted 1 times

✉  **javitech83** 3 months ago

Selected Answer: C

I would discard A because the development overhead. D does not have ASG, so only valid options would be C

upvoted 1 times

✉  **gd1** 3 months ago

Selected Answer: D

GPT 4.0 Application Load Balancer (ALB) helps distribute incoming traffic across multiple targets, such as Amazon EC2 instances. This distribution helps to increase the availability of your application. ALB can scale automatically to the volume of incoming traffic. Moving the EC2 instances to private subnets in the VPC would also enhance the security posture by reducing the surface area of attack.

upvoted 3 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 8 times

 **duriselvan** Most Recent  1 month, 1 week 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** 2 months, 4 weeks ago

Selected Answer: B

B by elimination

upvoted 1 times

 **gameoflove** 4 months, 2 weeks ago

Selected Answer: B

B As AWS Organizations Management account is only correct option

upvoted 1 times

 **leehjworking** 5 months, 1 week ago

Can anyone explain why A is wrong? Thank you.

upvoted 1 times

 **scuzzy2010** 4 months, 4 weeks ago

AWS Resource Access Manager has nothing to do with creating CURs. It's for sharing resources with other accounts.

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: B

B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account.

upvoted 1 times

 **masetromain** 9 months, 2 weeks 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).

 **masetromain** Highly Voted  8 months, 2 weeks 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 8 times

 **rbm2023** 4 months, 3 weeks ago

EFS only support Linux FS. this is why we need to go for FSx . option B

upvoted 7 times

 **Karamen** 1 month, 1 week ago

thanks for this explaination.

> EFS only support Linux FS. this is why we need to go for FSx . option B

upvoted 1 times

 **Simon523** Most Recent  3 weeks ago

Selected Answer: B

the question is required the data can be access by both on-premises and on-cloud windows server (migrated part of its Windows-based workload), so A is wrong.

upvoted 2 times

 **victorHugo** 3 weeks, 4 days 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 3 times

 **vn_thanh tung** 3 weeks, 1 day ago

needs the data to be available on a file system in the cloud

upvoted 1 times

 **aviathor** 3 weeks, 5 days ago

Selected Answer: A

1) Any answer mentioning EFS is out since EFS is for Linux only.
2) We are now left with DataSync vs File Gateway. The difference is that DataSync is batch-oriented, meaning that data will be out of sync between on-premise and cloud in between 2 synchronisation jobs. File Gateway for FSx on the other hand will synchronise continuously.

I would chose A because that is the most "versatile" option, allowing access to the data from AWS as well as from on-premise.

upvoted 1 times

 **vn_thanh tung** 3 weeks, 1 day ago

needs the data to be available on a file system in the cloud. So A?

upvoted 1 times

 **CloudHandsOn** 1 month, 1 week ago

Selected Answer: B

B. To decide between B and A for me was in the last sentence of the question "Which migration strategy..". Best migration strategy is AWS DataSync for this use case.

upvoted 1 times

 **chico2023** 1 month, 3 weeks ago

Selected Answer: B

Answer: B

The company is migrating part of their Windows-based workload that taps into a Windows file server. This eliminates C and D right away.

A seems incorrect. It mentions the File Gateway option in AWS Storage Gateway, BUT, this File Gateway has to connect to something, like a FSx share or an S3 bucket. It doesn't specify it. Not to mention that it seems they are not looking for a way for the whole company to tap from the cloud (even with it being cached on-prem), they seem to only want "the data to be available on a file system in the cloud" for "part of their Windows-based workload" in AWS.

Due to that, B is the most correct option in my opinion.

upvoted 2 times

 **aviathor** 2 months, 3 weeks ago

Selected Answer: A

Amazon FSx File Gateway optimizes on-premises access to fully managed, highly reliable file shares in Amazon FSx for Windows File Server. Customers with unstructured or file data, whether from SMB-based group shares, or business applications, may require on-premises access to meet low-latency requirements. Amazon FSx File Gateway helps accelerate your file-based storage migration to the cloud to enable faster performance, improved data protection, and reduced cost.

upvoted 2 times

 **NikkyDicky** 2 months, 4 weeks ago

Selected Answer: B

B

1 - windows -> FSx

2 - a would've be an option if mentioned 1st migration to s3

upvoted 1 times

 **hglopes** 3 months ago

Selected Answer: A

A works towards full migration and allows migrated workloads to use fully up to date data at any point and not just a daily sync which might not be enough

upvoted 2 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

keyword = migration strategy

then B

upvoted 1 times

 **gameoflove** 4 months, 2 weeks ago

Selected Answer: B

B as AWS FSx support Windows Files system can also be mounted as External Drive

upvoted 2 times

 **Sarutobi** 5 months, 1 week ago

"The company migrated part of its Windows-based workload to AWS" so those Ec2 windows now need access to that data; I believe FSx is the best way. Option A, using storage gateway the data ends on S3 or... FSx. DataSync is also a great utility when teaming up with DX.

upvoted 1 times

 **Sin_ha** 5 months, 2 weeks ago

Since the company needs the data to be available on a file system in the cloud, the best option is to use Amazon FSx for Windows File Server to store and access the data. Therefore, option B is the correct choice, and the company should use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.

upvoted 1 times

 **aviathor** 2 months, 3 weeks ago

The problem I have with B is that it talks about a DAILY task. So the workload running on prem and in the cloud may be up to 24 hours out of sync.

upvoted 1 times

 **takecoffee** 5 months, 3 weeks ago

I will go with A ..

they are talking about migration to cloud. not a hybrid solution.

Which data migration strategy should the company use?

upvoted 2 times

 **OnePunchExam** 5 months, 3 weeks ago

Data migration is simply moving data from A to B, it doesn't mean it is a one-off thing like as part of cloud migration workload strategy. Answer is B.

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B
B is the right answer.
upvoted 2 times

 **testingaws123** 6 months, 2 weeks ago

Selected Answer: A
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. Here It is open to discussion. Do they want to migrate the entire data to the cloud or do they just want data to be available in the cloud. It sound like data will sync to the cloud and remain active on prem. Which leads to option A.
upvoted 4 times

 **zejou1** 6 months, 2 weeks ago

Selected Answer: B
<https://docs.aws.amazon.com/efs/latest/ug/trnsfr-data-using-datasync.html>
upvoted 1 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.

 **zhangyu20000** Highly Voted 9 months, 2 weeks ago

C is correct.

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

upvoted 9 times

 **Simon523** Most Recent 2 weeks, 2 days ago

Selected Answer: C

C, LEAST operational overhead

upvoted 1 times

 **TWOCATS** 3 weeks, 6 days 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** 1 month, 1 week ago

Selected Answer: C

upvoted 1 times

 **xplusfb** 1 month, 2 weeks ago

Selected Answer: C

Its completely asking CRR Right one is C

upvoted 1 times

 **Brightalw** 1 month, 2 weeks 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** 2 months, 2 weeks ago

Selected Answer: C

CCCCCCCCCC

upvoted 1 times

 **Jonalb** 2 months, 3 weeks ago

Selected Answer: C

its a C correct answ...

upvoted 1 times

 **NikkyDicky** 2 months, 4 weeks ago

C no doubt

upvoted 1 times

 **hglopes** 3 months ago

Selected Answer: A

With A you achieve better overall resiliency because if a region goes down you can still write to the other bucket and ensure all webapp features. Also does not require adding cloudfront if they don't use it already leading to less operational overhead. it may however decrease performance in writing to s3 writing and perhaps data consistency issues in the future

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: C

Option C is the most suitable solution with the least operational overhead compared to option D because it leverages the built-in replication functionality of Amazon S3.

In option C, by configuring replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region, the replication process is handled automatically by Amazon S3. This ensures that the static assets are consistently synchronized between the two regions without the need for manual intervention or custom code.

On the other hand, option D suggests configuring replication on the S3 bucket in us-east-1 and updating the application code to load objects from the second Region in case of failover. While this option can achieve resiliency across multiple regions, it introduces additional complexity and operational overhead.

upvoted 2 times

 **AmalArul** 3 months, 3 weeks ago

Selected Answer: C

C is the correct answer.

More information at https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html

upvoted 1 times

 **gameoflove** 4 months, 2 weeks ago

Selected Answer: C

C is the Only option as per the requirement

upvoted 1 times

 **rbm2023** 4 months, 3 weeks ago

Selected Answer: C

C is the most suitable, because it will use both buckets as CF distribution

upvoted 1 times

 **Sin_ha** 5 months, 2 weeks ago

The solution that will meet the requirements with the least operational overhead is to configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region and set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins. Therefore, the correct answer is C.

upvoted 3 times

 **mfsec** 6 months ago

Selected Answer: C

S3 + Cloudfront

upvoted 2 times

 **Cloud_noob** 6 months ago

Selected Answer: C

you can configure Amazon CloudFront to use two different Amazon S3 buckets from different regions as the origin for your content.

To do this, you would need to create two separate Amazon S3 bucket origins in your CloudFront distribution settings, each one pointing to a different S3 bucket in a different region.

When creating the CloudFront distribution, you can add multiple origins to the distribution configuration. You can specify the origin domain name for each origin, which will correspond to the domain name of the S3 bucket you want to use as the origin.

You can also specify the origin protocol policy, which determines whether CloudFront uses HTTP or HTTPS to communicate with the origin.

Keep in mind that you will need to configure cross-region replication between the two S3 buckets in order to keep the content in both buckets synchronized. Additionally, you will need to make sure that both S3 buckets are publicly accessible or that CloudFront has the appropriate permissions to access the buckets.

upvoted 2 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.

 robertohyena Highly Voted  9 months, 2 weeks 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 17 times

 masetromain 8 months, 2 weeks 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 5 times

 Perkuns 3 months, 1 week 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 2 times

 masetromain Highly Voted  8 months, 2 weeks 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 6 times

 Simon523 Most Recent  2 weeks, 2 days 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 3 weeks, 4 days 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** 3 weeks, 5 days 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** 1 month, 3 weeks 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** 2 months, 2 weeks ago

Selected Answer: B

bbbbbbbbbbbbb

upvoted 1 times

 **NikkyDicky** 2 months, 4 weeks ago

Selected Answer: B

Its a B

upvoted 1 times

 **Limlimwdw** 4 months ago

Selected Answer: B

Qn didnt mention there is a need for DR hence a HA within a region will suffice.
NLB is also not required.

This leave B & D.

B is the best choice as spot instance is not desired.

upvoted 1 times

 **rbm2023** 4 months, 3 weeks ago

Selected Answer: B

I removed the Beanstalk due to the use case. Between the cloud formation options one of them mentions the retention policy, which removes option D. You want to keep the DB in case the stack is destroyed.

upvoted 1 times

 **devopsy** 5 months, 2 weeks ago

B because high scalability and availability can be achieved using multi AZ. Multi Region is a not required unless question mentions global audience.

upvoted 1 times

 **Sin_ha** 5 months, 2 weeks ago

Option B's use of Aurora MySQL may be a better option due to its scalability and high availability, which will help in minimizing downtime. So, the correct answer is Option B.

upvoted 1 times

 **frfavoreto** 5 months, 2 weeks ago

Selected Answer: B

Both 'A' and 'B' are technically functional, however 'B' is more convenient because Aurora, instead of RDS. Aurora has much more scalability as a serverless DB service, in contrast to RDS which is more rigid in this aspect.

upvoted 1 times

 **soujora2** 5 months, 3 weeks ago

I have a question.

The question has the following wording.

"company management has ordered that the application be moved to AWS"

Looking at the answers, it seems that they do not consider moving the application.

There is no moving part of the application in the answers, so why is the answer "B"?

upvoted 1 times

 **OnePunchExam** 5 months, 3 weeks ago

The question is "Which steps should the solutions architect take to design an appropriate solution?". It is not asking for the full and complete steps, so as long the answer is part of a bigger picture, it can suffice. But actually Ans B does address the cloud 3 tier environment setup:

- web tier is ALB
- app tier is EC2 in ASG for hosting workloads
- db tier is the aurora

upvoted 1 times

✉  **mfsec** 6 months ago

Selected Answer: B

B is the answer

upvoted 2 times

✉  **dev112233xx** 6 months, 2 weeks ago

Selected Answer: B

B makes sense to me 

upvoted 2 times

✉  **zejou1** 6 months, 2 weeks ago

Selected Answer: B

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

AWS EB does support .NET and MySQL; the difference now is that it is not supported separate regions

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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 12 times

 **masetromain** Highly Voted  9 months, 2 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/47723-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 5 times

 **NikkyDicky** Most Recent  2 months, 4 weeks ago

Selected Answer: C

C no brainer

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

Create a stack set in the Organizations management account.

upvoted 2 times

 **spd** 7 months, 1 week ago

Selected Answer: C

Stack Set in Mgmt account

upvoted 2 times

 **Atila50** 9 months, 2 weeks 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.

 **bititan** Highly Voted 8 months, 1 week ago

Selected Answer: ADE

trusted advisor doesn't have option to upload data, so option F is irrelevant

upvoted 15 times

 **Simon523** Most Recent 2 weeks, 2 days 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 1 times

 **NikkyDicky** 2 months, 4 weeks ago

Selected Answer: ADE

ADE no brainer

upvoted 1 times

 **ZK000001qws** 3 months, 3 weeks 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 2 times

 **asifjanjua88** 5 months, 2 weeks ago

ADE is correct answer.

upvoted 1 times

 **Jacky_exam** 5 months, 2 weeks 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** 6 months ago

B is incorrect because the servers are on prem.

upvoted 1 times

 **dev112233xx** 6 months, 2 weeks ago

Selected Answer: ADE

ADE no doubts 

upvoted 1 times

 **God_Is_Love** 7 months 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** 7 months, 1 week ago

Why Option C Group servers into applications for migration by using AWS Systems Manager Application Manager is incorrect?

upvoted 1 times

 **sambb** 7 months ago

AWS SSM Application Manager is used for existing resources deployed to AWS

upvoted 1 times

 **moota** 7 months, 2 weeks 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** 8 months, 1 week ago

BDE. Trusted Advisor is not for onprem assessments. Migration hub does EC2 ones

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

ADE is my answer

upvoted 3 times

 **masetromain** 8 months, 2 weeks 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

 **God_Is_Love** 7 months 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

 **masetromain** 8 months, 2 weeks 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** 8 months, 1 week 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

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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 10 times

 **God_Is_Love** Highly Voted  7 months 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 6 times

 **anita_student** 7 months ago

B wouldn't be highly secure and data transfer would also be slower

upvoted 1 times

 **NikkyDicky** Most Recent  2 months, 4 weeks ago

C of course

upvoted 1 times

 **gameoflove** 4 months, 2 weeks ago

Selected Answer: C

C is the Correct option as S3 Gateway will reduce the cost for NAT gateway

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

Set up an S3 gateway VPC endpoint

upvoted 2 times

 **dev112233xx** 6 months, 2 weeks ago

Selected Answer: C

C - easy one 

upvoted 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

C for sure

upvoted 3 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.

 **zhangyu20000** Highly Voted  8 months, 1 week ago

A is correct. On demand mode is for unknown load pattern, auto scaling is for known burst pattern
upvoted 18 times

 **dqwswwwtgxwkvgcvc** 1 month ago

How AWS Application Auto Scaling scale the read/write performance of DynamoDB?
upvoted 1 times

 **tannh** 2 weeks, 3 days 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  8 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 14 times

 **Simon523** Most Recent  2 weeks, 2 days 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 1 times

 **awsent** 2 weeks, 6 days 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

 **sonts** 4 weeks, 1 day ago

aababasdasdasdasd
upvoted 1 times

 **venvig** 1 month, 1 week 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 1 times

 **uC6rW1aB** 1 month, 1 week 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 RCUs and WCUs, 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 2 times

 **dqwsmtwwvtgxwkvvcv** 1 month ago

Yes I am also not sure about option B & D

upvoted 1 times

 **ggrodsckiy** 1 month, 3 weeks 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 1 times

 **b3llman** 1 month, 2 weeks 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

 **Jonalb** 2 months, 2 weeks ago

Selected Answer: A

A is correct, very correct!

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

A won't work cause you reserve for average load, so peak demand will result in errors between B and D, D provides an addition, even if small benefit for reads

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Changing to A after re-reading DDB autoscaling - it actually changes provisioned capacity, so should work

upvoted 1 times

 **[Removed]** 3 months ago

Selected Answer: B

The question states the application is WCU heavy, so DAX will have minimal impact on reducing load/cost, and comes with its own costs, which excludes C and D.

It doesn't matter whether the performance needs are unpredictable or not, what matters is they are variable, and that under-performing has been ruled out by the question. So the choice is between provisioning at a constant level high enough to cope with the 4h peak, or provisioning at a level that varies. DDB provides no native mechanism other than on-demand to alter the provisioning levels over time, so B is the answer here. On-demand R/WCU usage isn't any more expensive than explicitly provisioned usage, per unit. The difference is that on-demand usage removes the upper limit on provisioning, so if the application wants to use more, it can, and you pay for it. So for the 4h a week the app needs double the WCU level, DDB will provide it, and the cost per hour will be twice as high, but for the rest of the week the cost will be the same as if you had explicitly provisioned the lower level.

upvoted 1 times

 **ailves** 3 months, 1 week ago

Selected Answer: A

because on-demand is cheaper for unpredictable patterns, we can't choose B, C, D

upvoted 2 times

 **Or3m** 3 months, 2 weeks ago

Selected Answer: D

This solution meets the requirements by using Application Auto Scaling to automatically increase capacity during the peak period, which will handle the double the average load. And by purchasing reserved RCUs and WCUs to match the average load, it will minimize the cost of the table for the rest of the week when the load is close to the average.

upvoted 1 times

 **andreitugui** 3 months, 4 weeks ago

Selected Answer: B

Since the application load is close to the average load for most of the week and the peak load only occurs once a week for a limited 4-hour period, it is not necessary to provision and pay for provisioned capacity (RCUs and WCUs) to match the peak load. On-demand capacity mode provides the flexibility to automatically scale based on the actual load, allowing you to optimize costs by paying only for the resources consumed during those peak periods.

upvoted 2 times

 **EricZhang** 4 months ago

A - incorrect. as when peak hour comes, the dynamodb table will throw throttling error

C & D - incorrect. DAX is for app which is read-intensive

B - have to choose this

upvoted 1 times

 **gameoflove** 4 months, 2 weeks ago

Selected Answer: A

On Demand Mode is cost optimize

upvoted 1 times

 **rajalek** 5 months ago

Utilize on-demand capacity mode for the DynamoDB table - this mode allows the table to automatically scale up and down its capacity based on the actual usage. This means that during the peak load, the table will scale up to handle the increased traffic and scale down during periods of lower traffic. Since the peak load occurs once a week for a 4-hour period, the table will only pay for the resources it actually uses during that time and will not be over-provisioned for the rest of the week.

Answer B

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.

 **masetromain** Highly Voted  8 months, 1 week 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 14 times

 **Simon523** Most Recent  2 weeks, 1 day 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** 3 weeks, 5 days 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 1 times

 **chico2023** 1 month, 3 weeks 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** 2 months, 3 weeks ago

Selected Answer: D

d for sure

upvoted 1 times

 **ailves** 3 months, 1 week 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** 4 months ago

D - <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

upvoted 1 times

 **huanaws088** 5 months, 2 weeks 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** 2 months, 3 weeks 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** 5 months, 3 weeks ago

Selected Answer: D

SQS and autoscaling no doubt answer is D

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: D

SQS and Auto Scaling

upvoted 2 times

 **dev112233xx** 6 months, 2 weeks 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** 7 months 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** 7 months, 1 week 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** 7 months, 4 weeks ago

Selected Answer: D

D is the right answer

upvoted 2 times

 **Musk** 7 months, 4 weeks ago

Selected Answer: D

Because A is not valid due to time

upvoted 2 times

 **pravi1** 8 months ago

D will be correct.

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

D is correct because it took 1 hour to process the file. Lambda only run 15 minutes

upvoted 1 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 13 times

 **masetromain** 8 months, 2 weeks 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** 7 months ago

B says to delete but question asks for saving on compliance purposes.

upvoted 3 times

 **God_Is_Love** 7 months ago

* I meant C says..

upvoted 3 times

 **venvig** Most Recent 1 month 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 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B I think :/

upvoted 1 times

 **Damijo** 6 months, 1 week 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

 **eddylynx** 2 months, 3 weeks 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://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_AuthorizeSecurityGroupIngress.html

upvoted 1 times

 **Jesuisleon** 3 months, 1 week 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

 **dev112233xx** 6 months, 2 weeks ago

Selected Answer: B

B - makes more sense

upvoted 4 times

 **Ajani** 6 months, 3 weeks 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** 7 months, 2 weeks 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** 7 months ago

This eliminates option A

upvoted 2 times

 **Musk** 7 months, 4 weeks 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.

 **masetromain**  8 months, 2 weeks 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 37 times

 **masetromain** 8 months, 2 weeks 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 4 times

 **MikelH93** 4 months, 1 week 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** 1 month, 2 weeks ago

have you actually tested it? if you haven't, please do it and then comment.

upvoted 1 times

 **Maria2023**  3 months, 1 week 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 18 times

 **dqwsmwvwvtgxwkvvcv** 1 month 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_thanh tung** 3 weeks, 4 days 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_thanh tung** 3 weeks, 4 days ago

Sorry typo.

you think C can "remove the ability to create" crazy ? SCP allow all by default

upvoted 1 times

 **b3llman** 1 month, 2 weeks ago

Tested and confirmed!

upvoted 3 times

 **Piccaso** Most Recent 1 month ago

Selected Answer: D

A is not reliable. D is supported.

upvoted 1 times

 **venvig** 1 month ago

Selected Answer: A

Option D is NOT correct.

There is no documented Condition named Sourcelp for ec2:AuthorizeSecurityGroupIngress

Refer https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonec2.html

upvoted 2 times

 **allen_devops** 1 month, 2 weeks ago

The correct answer is A. For C/D, the condition aws:Sourcelp is to check the requester's IP instead of the ingress rule's IP.

upvoted 2 times

 **xplusfb** 1 month, 2 weeks ago

Selected Answer: D

Question always says the keynote. Keynote is LEAST operational overhead. And we already using AWS Organizations so its 100 percent works D

upvoted 1 times

 **punkbuster** 1 month, 2 weeks ago

Selected Answer: A

Answer is A NOT D - The "aws:Sourcelp" condition key picks the IP Addr of the requester not the IP address being passed into the Security Group.

I would suggest, log into AWS account and try it out for yourself by changing the source of the ingress rule.

upvoted 2 times

 **CuteRunRun** 1 month, 3 weeks ago

Selected Answer: C

I think the default policy in scp is deny, you need to create a explicit allow policy

upvoted 2 times

 **CuteRunRun** 1 month, 3 weeks ago

I think the default policy of SCP is deny, you need to create a explicit allow rule.

So I select C

upvoted 1 times

 **MRL110** 2 months ago

Selected Answer: D

SCP only allows condition key in deny statements:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_syntax.html#scp-syntax-condition

upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

D would be nice if was suported by SCP

upvoted 2 times

 **NikkyDicky** 2 months, 2 weeks ago

D - actually was able to create that SCP and attach to member acct, but it didn't stop me from creating an SG with 0.0.0.0/0 sourcelp ...

upvoted 1 times

 **SmileyCloud** 2 months, 4 weeks ago

Selected Answer: D

It's D. I just tested it. This is the error that I am getting when I tried to create a sec group with 0.0.0.0/0 as source. "You may be missing IAM policies that allow AuthorizeSecurityGroupIngress. You are not authorized to perform this operation. Encoded authorization failure message: <some gibberish>

And this is the policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:Sourcelp": "0.0.0.0/0"
        }
      }
    }
  ]
}
```

upvoted 5 times

 **phongpg** 3 months, 1 week ago

Selected Answer: A

Correct answer is C. Its can't be option D, 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

 **phongpg** 3 months, 1 week ago

Sorry answer is A, not C/D

upvoted 1 times

 **SkyZeroZx** 3 months, 2 weeks ago

Selected Answer: A

: A

This is a really hard question cuz it really baits you with the SCP which would make a lot of sense here. Unfortunately that condition is not the correct one

upvoted 1 times

 **Roontha** 3 months, 3 weeks ago

Answer : A

Bases on AWS demo on following use case

<https://aws.amazon.com/blogs/security/how-to-automatically-revert-and-receive-notifications-about-changes-to-your-amazon-vpc-security-groups/>

upvoted 1 times

 **Rajivjain** 3 months, 3 weeks ago

Selected Answer: D

SCP support aws: Sourcelp condition key > Check point "e" carefully under "Creating an SCP"

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_create.html

upvoted 1 times

 **Rajivjain** 3 months, 3 weeks ago

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyIngressFromAnyIp",
      "Effect": "Deny",
      "Action": "ec2:AuthorizeSecurityGroupIngress",
      "Resource": "*",
      "Condition": {
```

```
"StringEquals": {  
    "aws:SourceIp": "0.0.0.0/0"  
}  
}  
}  
}  
]  
}
```

upvoted 1 times

 **Darkhorse_79** 3 months, 3 weeks ago

Selected Answer: D

Requirement is "Remove the ability to create a security group "

upvoted 4 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 14 times

 **masetromain** 8 months, 2 weeks 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 4 times

 **hobokabobo** 7 months 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(invoke Lambda directly) or curl(do a rest call).

Similar for other implementations.

upvoted 1 times

 **hobokabobo** 7 months 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 1 times

 **sam_cao** Most Recent  2 days, 6 hours 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

 **CuteRunRun** 1 month, 3 weeks ago

Selected Answer: B

I prefer B

upvoted 1 times

 **SmileyCloud** 2 months, 3 weeks ago

Selected Answer: B

API GW and Lambda. Here is your architecture: <https://aws.amazon.com/solutions/implementations/git-to-s3-using-webhooks/>

upvoted 3 times

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

Selected Answer: B

B makes sense

upvoted 1 times

✉ **emiliocb4** 3 months, 3 weeks 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 2 times

✉ **sam_cao** 2 days, 6 hours ago

I agree. We don't have any coding if we choose C.

upvoted 1 times

✉ **Sarutobi** 4 months, 2 weeks 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** 1 month, 2 weeks ago

Option A works for sure, but managing API gateway is easier than managing function URLs in every single lambda function.

upvoted 1 times

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

Selected Answer: B

B, Is the best option as per the question

upvoted 1 times

✉ **RaghavendraPrakash** 5 months, 2 weeks ago

I go with C. With the options, we have Lambda and AppRunner. We dont know if that functionality can be repurposed with Lambda. However, the functionality can be deployed with AppRunner with least Operational Overhead.

upvoted 3 times

✉ **dev112233xx** 6 months, 2 weeks ago

Selected Answer: B

B makes sense 

upvoted 3 times

✉ **moota** 7 months, 2 weeks ago

Selected Answer: B

Here's what ChatGPT has to say.

In general, if you're looking for the option with the least operational overhead and you're comfortable with a fully managed, serverless environment, then AWS Lambda with API Gateway may be the better choice. However, if you require more control over your environment or need to use containers, then AWS App Runner with ALB may be the better option.

upvoted 2 times

✉ **Untamables** 8 months ago

Selected Answer: B

<https://aws.amazon.com/solutions/implementations/git-to-s3-using-webhooks/>

upvoted 3 times

✉ **AjayD123** 8 months, 1 week ago

Selected Answer: B

Api Gateway with Lambda

<https://medium.com/mindorks/building-webhook-is-easy-using-aws-lambda-and-api-gateway-56f5e5c3a596>

upvoted 3 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.

 **masetromain** Highly Voted 8 months, 1 week 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 28 times

 **masetromain** 8 months, 1 week 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 4 times

 **masetromain** 8 months, 1 week 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 3 times

 **icassp** Highly Voted 8 months, 1 week ago

Selected Answer: D

Choosing between A and D. For A, how can S3 select query?

upvoted 5 times

 **oatif** 7 months, 3 weeks 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

 **punkbuster** Most Recent 1 month, 1 week 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** 1 month, 2 weeks 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 1 month, 3 weeks 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 1 month, 3 weeks 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 1 month, 3 weeks ago

Selected Answer: D

I prefer D

upvoted 1 times

ggrodsckiy 1 month, 3 weeks 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 2 months, 3 weeks ago

Selected Answer: D

it's a D

upvoted 1 times

Maria2023 3 months, 1 week 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 3 times

btx 3 months, 1 week ago

Selected Answer: A

The key is the VMWare environment, for that the obvious solution is A. IMHO.

upvoted 1 times

mfsec 6 months ago

Selected Answer: D

D is the answer because agentless cant grab everything

upvoted 2 times

dev112233xx 6 months, 2 weeks ago

Selected Answer: D

A is wrong.. because Agentless can't collect processes .. only CPU/RAM and disk IO

upvoted 4 times

Ajani 6 months, 3 weeks ago

If you have virtual machines (VMs) that are running in the VMware vCenter environment, you can use the Agentless Collector to collect system information without having to install an agent on each VM. Instead, you load this on-premises appliance into vCenter and allow it to discover all of its hosts and VMs.

Agentless Collector captures system performance information and resource utilization for each VM running in the vCenter, regardless of what

operating system is in use. However, it cannot “look inside” each of the VMs, and as such, cannot figure out what processes are running on each VM nor what network connections exist.

upvoted 1 times

 **Ajani** 6 months, 3 weeks ago

Going with D; Agentless discovery Connector does not gather process information; "THE" on premises HOSTs(physical servers?) will be running on esxi server.

You can deploy Discovery agent on Server(VM) . I might be overthinking it.

upvoted 2 times

 **sambb** 7 months ago

Selected Answer: D

With the agentless collector you cannot get running processes on the VMs, and you cannot export the data to CSV or to Athena for further querying

upvoted 2 times

 **God_Is_Love** 7 months ago

Even though question does not ask for least operational effort, performance, HA etc, the solution needs to be thinking those in mind. deploying on each server is not practically good solution. So D cannot be answer. Instead, an appliance which does this discovery job is good which is right there in A. Moreover A is exclusively for VMWare use case. I choose A

upvoted 2 times

 **monkeyfish** 7 months ago

Selected Answer: A

Answer is A.

The AWS Agentless Discovery Connector is used when performing migration of servers in vmware clusters. S3 Select can be used to query. AWS SA's would only recommend installing the agent on each on-prem server for physical hosts, not vmware server.

upvoted 1 times

 **c73bf38** 7 months ago

S3 Select supports querying one file at a time. With Amazon Athena, you can perform SQL against any number of objects, or even entire bucket paths.

upvoted 2 times

 **prav1** 8 months ago

D will be correct in my opinion.

upvoted 3 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 17 times

 **Jacky_exam** 5 months, 3 weeks 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 4 times

 **TWOCATS** Most Recent 3 weeks, 5 days 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** 1 month ago

Selected Answer: A

A is the best solution

<https://repost.aws/knowledge-center/internet-access-lambda-function>

upvoted 1 times

 **Russ99** 1 month, 1 week 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** 1 month, 2 weeks 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 3 times

 **chico2023** 1 month, 3 weeks 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 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

it's an A

upvoted 1 times

 **SmileyCloud** 2 months, 3 weeks ago

Selected Answer: A

A - step by step here. <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/generate-a-static-outbound-ip-address-using-a-lambda-function-amazon-vpc-and-a-serverless-architecture.html>

The elastic IP is attached to the NAT not IGW.

upvoted 4 times

 **ailves** 3 months, 1 week ago

Selected Answer: A

If we deploy Lambda in Public Subnet, Lambda will get IP address from Random range

upvoted 1 times

 **easytoo** 3 months, 1 week ago

d-d-dd-d-d-dd-

upvoted 1 times

 **easytoo** 2 months ago

Updated my answer to A.

upvoted 1 times

 **mKrishna** 4 months ago

Ans: A

Step-by-step instruction at <https://africanpearl.hashnode.dev/vpc-network-public-and-private-subnets-grant-subnets-access-to-the-internet-aws>

upvoted 1 times

 **aca1** 4 months ago

Selected Answer: A

No doubt about A.

A Lambda function in VPC need a NAT Gateway to access internet, it can not use the Internet Gateway:

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

"Note

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 2 times

 **rbm2023** 4 months, 3 weeks ago

Selected Answer: A

D and C are not ideal choices because involves moving the lambda to a public subnet since it mentions using an internet gateway. A would make more sense

upvoted 1 times

 **RaghavendraPrakash** 5 months, 2 weeks ago

C. egress internet gateway is for IPv6 traffic. NAT GW still needs internet GW for internet connectivity, half solution.

upvoted 3 times

 **Jacky_exam** 5 months, 3 weeks ago

Selected Answer: D

Option D is the correct solution.

In order to provide the Lambda function with a single public IP address, an internet gateway must be deployed and associated with an Elastic IP address. The Elastic IP address can then be provided to the external provider for use in the allow list.

upvoted 2 times

 **Jay_2pt0_1** 4 months, 1 week ago

Everyone voted A, but I think you are right. I need to research this one a bit more, though.

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

Deploy a NAT gateway. Associate an Elastic IP address with the NAT gateway.

upvoted 2 times

 **vvahe** 6 months, 1 week 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 4 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 26 times

 **masetromain** 8 months, 2 weeks 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 6 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: BD

BD for sure

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: BD

RDS proxy + Lambda function

upvoted 3 times

 **dev112233xx** 6 months, 2 weeks ago

Selected Answer: BD

RDX proxy & connecting outside the handler method is up to 5 times faster than connecting inside.

upvoted 3 times

 **kiran15789** 6 months, 3 weeks 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** 7 months 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** 7 months, 2 weeks 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** 7 months, 3 weeks ago

BD

<https://awstut.com/en/2022/04/30/connect-to-rds-outside-of-lambda-handler-method-to-improve-performance-en/>

upvoted 2 times

 **masssa** 8 months, 1 week 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** 8 months, 1 week 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** 8 months, 1 week 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.

 **pitakk** Highly Voted 8 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 27 times

 **hobokabobo** 7 months 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

 **Untamables** Highly Voted 8 months, 1 week 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 23 times

 **Ikyixoayffasdrlaqd** 7 months 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 8 times

 **Arnaud92** 6 months, 1 week 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

 **hobokabobo** 7 months ago

coorect. but they want to upload the the certificate to the NLB for unknown reasons.

upvoted 2 times

 **Greyeye** Most Recent 1 month, 1 week ago

D is the answer.

for NLB

The load balancer passes the request to the target as is, without decrypting it.

see

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html>

A , you cannot export ACM cert

<https://repost.aws/knowledge-center/acm-export-certificate>

B and C both end point will decrypt the traffic and proxy to origin/target. to meet end-to-end encryption D is only one.

upvoted 1 times

 **xplusfb** 1 month, 2 weeks ago

Selected Answer: C

Due to Question asking end-to-end encryption so we did before like a question same scenerio and we have a 3rd party ssl into EC2 servers also using CloudFront ACM. im going too C fellas. thank you

upvoted 2 times

 **chico2023** 1 month, 3 weeks ago

Selected Answer: C

Answer: C

Same reasons as most have put, plus this: <https://repost.aws/questions/QUlo7PWvZ3T6aFYCByhZ5f0A/load-certificate-on-alb-and-ec2>

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

it's a C

upvoted 1 times

 **SmileyCloud** 2 months, 3 weeks ago

Selected Answer: D

C is valid, see here. <https://faun.pub/end-to-end-ssl-encryption-with-aws-application-load-balancer-b43db918bd9e>

But, D is better, less overhead and no fake certs.

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: C

its a C

upvoted 1 times

 **[Removed]** 3 months ago

Selected Answer: D

D: An NLB is needed provide the complete end-to-end encryption the question calls for, the other answers all decrypt the traffic in the middle somewhere. The only confounding factor in the wording is it talks about "installing the certificate on the NLB" which isn't required for end-to-end, you'd just use pass-through TCP on port 443. You *can* install a certificate on an NLB if you want to use a TLS listener (<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html>) but that would a) decrypt in the middle, and b) shouldn't be required here.

upvoted 1 times

 **ailves** 3 months, 1 week ago

Selected Answer: C

I voted to C, as we need to have end-to-end encryption, and so we have to install third party certificates on EC2 instances (not ACM), and we have to use ALB so as HTTP traffic

upvoted 1 times

 **easytoo** 3 months, 1 week ago

a-a-a-a-a-a-a-a-a-a-

upvoted 1 times

 **easytoo** 3 months, 1 week ago

changed it to c-c-c-c-c-c-c-c

upvoted 1 times

 **Asds** 3 months, 2 weeks ago

I will go C, but I was hesitating with D.

So what convinced me: no need to install any certs at nlb's as you're doing passthrough, so no decryption AT that moment.

Drop D hence, and C is my choice

upvoted 2 times

 **papawed345** 4 months ago

Selected Answer: D

The only possible answer is an NLB. The ALB will always decrypt in the middle.

upvoted 1 times

 **emiiowan** 4 months, 1 week ago

Selected Answer: C

C is correct. Although D works, the fact that it states "install it on NLB" is wrong as you can only associate/add it to the listener but there is no install option. ALB with public ACM cert fw to target group with self signed cert listening on port 443 is correct (see the implementation steps here).

upvoted 4 times

 **Jesuisleon** 4 months ago

I agree with you. NLB can work by its tcp endpoint to forward encrypted connection through it but in this case there is no need to install cert on NLB. so C is better.

upvoted 1 times

✉  **meggie** 4 months, 3 weeks ago

vote for D.

NLB works at layer 7 and won't decrypt traffic. However, ALB works at layer 4.

upvoted 1 times

✉  **Sarutobi** 4 months, 2 weeks ago

I think you have that backward; Network actually works at L3 (Network Layer of OSI model), and L4 (Transport UDP/TCP). When introduced, the NLB could not do TLS work, although it is now. ALB works in L7 or the application layer of the OSI model. ALB is only an HTTP proxy, so it only supports HTTP traffic; you won't be able to use it for UDP traffic or any other TCP.

upvoted 4 times

✉  **F_Eldin** 4 months, 3 weeks ago

Selected Answer: A

you can also export private certificates for use on EC2 instances, on ECS containers, or anywhere.

<https://aws.amazon.com/certificate-manager/faqs/>

upvoted 1 times

✉  **Maria2023** 5 months ago

Selected Answer: C

Here is a similar scenario but for beanstalk <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/configuring-https-endtoend.html>

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.

 **OCHT** Highly Voted  5 months, 1 week 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 12 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: C

It's a c

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: C

Keywords = DMS & RDS Proxy

Then C

upvoted 1 times

 **leehjworking** 4 months, 3 weeks ago

Selected Answer: C

AD: restart = interruption?

B: ASG...Why?

upvoted 3 times

 **chikorita** 3 months, 3 weeks ago

why ...oh...why?

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

ill go with C

upvoted 1 times

 **dev112233xx** 6 months, 1 week 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 2 times

 **zejou1** 6 months, 2 weeks 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** 6 months, 3 weeks ago

Could anybody explain why ALB? I'd go with API Gateway

upvoted 1 times

 **zejou1** 6 months, 2 weeks 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** 7 months ago

Selected Answer: C

I would say C.

upvoted 1 times

 **hobokabobo** 7 months 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 of the approaches addresses that aggregation tasks fail because of inconsistency of the data base.

upvoted 1 times

 **hobokabobo** 7 months 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** 7 months 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 on-premises. 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 1 times

 **Fatouch** 7 months, 1 week ago

is it C or B?

Same person answers two times two different answers

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

C is correct

upvoted 3 times

 **masetromain** 8 months, 1 week 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** 8 months, 1 week 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** 8 months, 1 week ago

C is correct. need more read replica for aggregation jobs to read data

upvoted 3 times

✉ **masetromain** 8 months, 2 weeks ago

Selected Answer: B

The correct answer is B. Setting up an Amazon Aurora MySQL database and using AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora will ensure that data is continuously replicated to the new environment with minimal interruption. Moving the aggregation jobs to run against the Aurora MySQL database will ensure that the data is being read from the same database that is being loaded, which will resolve the data loading issue. Setting up collection endpoints behind an Application Load Balancer (ALB) as Amazon EC2 instances in an Auto Scaling group, and disabling the AWS DMS sync task after the cutover from on-premises to AWS, will ensure that the migration occurs without interruptions or changes for the company's customers.

upvoted 2 times

✉ **masetromain** 8 months, 2 weeks ago

Answer A is incorrect because it's not necessary to set up an Aurora Replica for the Aurora MySQL database, doing this will introduce additional complexity and cost. Using Amazon RDS Proxy is not necessary for this scenario, and disabling the replication job and restarting the Aurora Replica as the primary instance will cause an interruption to the service.

Answer C is incorrect because it's not necessary to set up an Aurora Replica for the Aurora MySQL database, doing this will introduce additional complexity and cost. Using Amazon RDS Proxy is not necessary for this scenario.

Answer D is incorrect because it's not necessary to use Amazon Kinesis data stream and Firehose to replicate the data when AWS DMS can be used to perform continuous data replication. Also, disabling the replication job and restarting the Aurora Replica as the primary instance will cause an interruption to the service.

upvoted 1 times

✉ **andctygr** 8 months ago

Dude can u pls stop copy-pasting from chatgpt I am so sick of it. It is not a reliable source. Just stop it for the god sake.

upvoted 13 times

✉ **Jesuisleon** 4 months, 1 week ago

Before I read your comments, I thought I was the only one so sick of it :)

upvoted 2 times

✉ **jojom19980** 7 months, 4 weeks ago

hhhhhhhhh.

upvoted 2 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.

 **masetromain**  8 months, 2 weeks 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 27 times

 **hamimelon** 3 weeks, 1 day 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 1 times

 **masetromain** 8 months, 2 weeks 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 6 times

 **hobokabobo** 7 months 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** 6 months, 2 weeks 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** 5 months, 3 weeks 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

 **Musk** 7 months, 4 weeks ago

What about the requirement of customer managed keys?

upvoted 8 times

 **Untamables**  8 months, 1 week ago

Selected Answer: D

I think D is correct.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html>

upvoted 15 times

 **awsent**  2 weeks ago

Answer: B

Customer could use KMS for managing the keys, they don't need "Key material" from the customer.

upvoted 1 times

 **FunkyFresco** 2 weeks, 3 days ago

Selected Answer: B

Option B is the right answer. <https://aws.amazon.com/blogs/storage/encrypting-existing-amazon-s3-objects-with-the-aws-cli/>

upvoted 1 times

 **aviathor** 3 weeks, 5 days ago

Selected Answer: B

A. SSE-S3 uses S3-managed keys which is not what we are looking for

C. Why should one set an S3 bucket policy to automatically encrypt objects on GetObject?

D. Although AES-256 is a cryptographic algorithm used by S3, it is not a mode of S3.

B. SSE-KMS supports server-side encryption both with AWS-managed and customer-managed keys, and we do indeed need to re-upload all objects in order to get them encrypted

upvoted 2 times

 **Simon523** 4 weeks, 1 day ago

Selected Answer: D

the key words is "by keys that the company's security team manages", so should be A or D, and I select D cause I think should apply policy then re-upload the files.

upvoted 2 times

 **xflare** 1 month ago

Selected Answer: B

It's B:

If you go to the docs, <https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html>, it clearly says "The only thing that you need to do is manage the encryption keys that you provide. " which seems to point to D.

HOWEVER, D says to select AES256 as default encryption, but such option does not exist.

Just go create a bucket and try to do it yourselves.

Therefore the answer must be B.

upvoted 1 times

 **CloudHandsOn** 1 month, 1 week ago

Selected Answer: D

I believe that it is D. the keys needs to be customer managed

upvoted 1 times

 **Piccaso** 1 month, 1 week ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html>

upvoted 1 times

 **xplusfb** 1 month, 2 weeks ago

Selected Answer: B

%100 B. I'm pretty sure. Believe me

upvoted 1 times

 **chico2023** 1 month, 3 weeks ago

Selected Answer: B

Answer: B

Funny that this question is VERY similar to one in a practice question you can buy at Udemy. Still, it's the best and only option that meet their requirements.

I don't know why one should choose D. If you take a look at the S3 properties console, or the documentation: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html>, you won't find this option.

upvoted 1 times

 **Zox42** 1 month, 3 weeks ago

Selected Answer: D

Answer D

upvoted 1 times

 **blehbleh** 1 month, 4 weeks ago

Selected Answer: D

I think its D per AWS "AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the cryptographic keys" The question is stating that the customer manages the keys. AWS KMS is a managed service so I think that would eliminate anything that offers AWS KMS to be a viable option.

upvoted 1 times

 **MRL110** 2 months ago

Selected Answer: D

The answer is spread all over this page:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html>

upvoted 1 times

 **Asamara** 2 months ago

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.

Options A, C, and D are incorrect:

Option A suggests changing the default encryption to SSE-S3 with a customer managed key, which does not meet the requirement for the company's security team to manage the encryption keys.

Option C mentions setting an S3 bucket policy to automatically encrypt objects on GetObject and PutObject requests, which is not necessary and does not align with the requirement to use customer managed keys for encryption.

Option D proposes using AES-256 with a customer managed key, which does not fulfill the requirement for the security team to manage the encryption keys through AWS KMS.

upvoted 1 times

 **aviathor** 2 months, 1 week ago

Selected Answer: D

I do not like neither B or C because they talk about KMS MANAGED keys (instead of KMS customer-managed) whereas the question says that the customer wants to manage its own keys. Therefore, the only viable option is D

upvoted 1 times

 **Jonalb** 2 months, 3 weeks ago

why not D guys?

upvoted 2 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 14 times

 **God_Is_Love** Highly Voted  7 months 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 6 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

it's a B

upvoted 1 times

 **[Removed]** 3 months 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 1 times

 **mfsec** 6 months ago

Selected Answer: B

Provision an ALB, an Auto Scaling group, and EC2 instances in a different AWS Region.

upvoted 1 times

 **dev112233xx** 6 months, 1 week ago

Selected Answer: B

B is the best solution with very high availability (compared to the R53 failover solution)

upvoted 1 times

 **Ajani** 6 months, 3 weeks ago

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

upvoted 1 times

 **Sarutobi** 7 months ago

Selected Answer: B

B looks good.
upvoted 1 times

 **masssa** 8 months, 1 week ago

Selected Answer: B

B is correct.
C is not correct, because ALB is regional service, so ALB have to be added too.
upvoted 1 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".

 **masetromain** Highly Voted  8 months, 2 weeks 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 16 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: C

C for sure

upvoted 1 times

 **Asds** 3 months, 2 weeks ago

Selected Answer: C

Definitely prefix

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

prefix list and RAM

upvoted 2 times

 **dev112233xx** 6 months, 1 week ago

Selected Answer: C

C makes sense 

upvoted 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/82131-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

 **AjayD123** 8 months, 1 week 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 3 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 13 times

 **zozza2023** Highly Voted  7 months, 4 weeks ago

Selected Answer: B

AWS compute optimizer+ lambda

upvoted 5 times

 **awsent** Most Recent  2 weeks ago

Selected Answer: B

Computer Optimizer could generate Export for Lambda Functions one-time. In order to schedule every 2 weeks, EventBridge Scheduler/Schedule Rule should be used.

upvoted 1 times

 **awsent** 2 weeks ago

Answer: B

<https://aws.amazon.com/blogs/compute/optimizing-aws-lambda-cost-and-performance-using-aws-compute-optimizer/>

upvoted 1 times

 **Simon523** 2 weeks, 1 day 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 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

its a B

upvoted 1 times

 **EricZhang** 3 months, 4 weeks ago

B - https://docs.aws.amazon.com/compute-optimizer/latest/APIReference/API_ExportLambdaFunctionRecommendations.html

upvoted 3 times

✉  karma4moksha 4 months, 2 weeks ago

Option D i would say as purchasing business support and truster advisor is money but not development time.
upvoted 1 times

✉  Pete987 6 months, 1 week 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 6 months, 1 week ago

Selected Answer: B

B

<https://docs.aws.amazon.com/compute-optimizer/latest/ug/exporting-recommendations.html>

upvoted 3 times

✉  massa 8 months, 1 week ago

Selected Answer: C

I vote C.

AWS compute optimizer can make lambda recommendation without any development.

<https://docs.aws.amazon.com/compute-optimizer/latest/ug/view-lambda-recommendations.html>

upvoted 1 times

✉  massa 8 months, 1 week ago

I correct answer C to B.

AWS compute optimizer itself cannot make recommendation file by oneself.

It need simple lambda.

upvoted 3 times

✉  AjayD123 8 months, 1 week ago

Selected Answer: B

https://docs.aws.amazon.com/compute-optimizer/latest/APIReference/API_ExportLambdaFunctionRecommendations.html

upvoted 3 times

✉  zhangyu20000 8 months, 1 week ago

B is correct

<https://aws.amazon.com/blogs/compute/optimizing-aws-lambda-cost-and-performance-using-aws-compute-optimizer/>

upvoted 2 times

✉  Pete987 6 months, 1 week ago

That's the old way of doing it. The new way does not require the creation of Lambda. Compute optimizer takes care of it

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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 20 times

 **masetromain** 8 months, 2 weeks 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 6 times

 **a_c_** 4 months, 3 weeks 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

|

upvoted 3 times

 **spd** Highly Voted 7 months, 1 week ago

Selected Answer: ADF

Correct ADF - Since resources are tagged, C may not require ?

upvoted 5 times

 **awsent** Most Recent 2 weeks 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

 **Simon523** 2 weeks, 1 day ago

Selected Answer: ACF

Cost Categories - AWS Cost Categories allow grouping accounts and grouping tags (“meta-tagging”) within an AWS Organization, which further provides capability to analyze the cost related to these categories through tools such as AWS Cost Explorer, AWS Budgets and AWS Cost and Usage Report.

upvoted 1 times

 **Zox42** 1 month, 3 weeks ago

Selected Answer: ACF

Answer ACF

upvoted 2 times

 **vn_thanh tung** 1 month ago

Sorry I mistake Answer ACF

upvoted 1 times

 **vn_thanh tung** 1 month ago

If you're signed into the management account with your root account credentials, you can enable Cost Explorer access. Your root account credentials are through the Billing and Cost Management console. Enabling Cost Explorer at the management account level enables Cost Explorer for all of your organization accounts. All accounts in the organization are granted access, and you can't grant or deny access individually.

upvoted 1 times

 **vn_thanh tung** 1 month ago

I think A,D,F

upvoted 1 times

 **vn_thanh tung** 1 month ago

<https://docs.aws.amazon.com/cost-management/latest/userguide/ce-access.html>

upvoted 1 times

 **qwertyui0** 2 months, 1 week ago

Selected Answer: ADF

how we get access to billing without any permissions? need the iam role

upvoted 1 times

 **Jonalb** 2 months, 2 weeks ago

Selected Answer: ADF

ADF "The teams use IAM access for daily activities."

upvoted 1 times

 **Jonalb** 2 months, 3 weeks ago

Selected Answer: ADF

IAM USER its ADF

upvoted 1 times

 **nicecurls** 2 months, 3 weeks ago

Selected Answer: ADF

how we get access to billing without any permissions? need the iam role

upvoted 1 times

 **NikkYDicky** 2 months, 3 weeks ago

Selected Answer: ACF

ACF makes sense.

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: ACF

ACF

<https://docs.aws.amazon.com/whitepapers/latest/tagging-best-practices/building-a-cost-allocation-strategy.html>

upvoted 2 times

 **Jonalb** 3 months ago

Selected Answer: ACF

ACF !!!!!!!

upvoted 1 times

 **javitech83** 3 months ago

Selected Answer: ADF

C is not needed as with A we cover Application and Team Costs.

D is needed in order to provide access to the Teams to their cost that they need to control

upvoted 2 times

✉  **Jackhemo** 3 months, 1 week ago

Selected Answer: ACF

From olabiba.ai:

- A. Activate the user-defined cost allocation tags that represent the application and the team. This will allow you to assign specific tags to resources and track costs based on those tags.
- C. Create a cost category for each application in Billing and Cost Management. Cost categories allow you to group costs based on specific criteria, such as application names, and generate reports based on those categories.
- F. Enable Cost Explorer. Cost Explorer provides a comprehensive set of tools and reports for analyzing costs, including the ability to view costs by application or team based on the activated cost allocation tags.

By activating user-defined cost allocation tags, creating cost categories, and enabling Cost Explorer, you will have the necessary tools and reports to track costs, compare them over time, and forecast future costs.

upvoted 1 times

✉  **Asds** 3 months, 2 weeks ago

Selected Answer: ADF

Users require appropriate authorization.

Hence, D

A, F are obvious

upvoted 1 times

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

Selected Answer: ADF

Answer : A,D,F

D is more appropriate than C as we already have user defined cost allocation.

upvoted 2 times

✉  **Roontha** 3 months, 3 weeks ago

Answer : A,D,F

D is more appropriate than C as we already have user defined cost allocation.

upvoted 2 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 12 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: B

its a B

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

KEYWORD = NAT gateways in the VPC

upvoted 1 times

 **AWS_Sam** 4 months, 1 week ago

B is the only option that makes sense.

upvoted 1 times

 **SkyZeroZx** 4 months, 1 week ago

Selected Answer: B

B make sense

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B

Register a block of customer owned public IP's

upvoted 2 times

 **dev112233xx** 6 months, 1 week ago

Selected Answer: B

B is the only solution

upvoted 2 times

 **zozza2023** 7 months, 4 weeks 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.

 **Atila50** Highly Voted 8 months, 1 week ago

Selected Answer: C

SCP doesn't grant permission

upvoted 12 times

 **c73bf38** 7 months 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 3 times

 **c73bf38** 7 months 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 5 times

 **zhangyu20000** Highly Voted 8 months, 1 week ago

C is correct

SCP policy allow everything except cloudtrail. SCP is boundary but it does not give allow to IAM users. You have to configure allow for every IAM

upvoted 9 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: C

it's a C

upvoted 1 times

 **javitech83** 3 months ago

Selected Answer: C

C is correct

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week 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 cloudtrail action. Being denied cloudtrail wouldn't deny s3 actions.

upvoted 2 times

 **bhanus** 3 months, 2 weeks 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 1 times

 **Asds** 3 months, 2 weeks ago

Selected Answer: C

Need to deal with iam policy auth now

upvoted 1 times

 **Asds** 3 months, 2 weeks ago

C is right

upvoted 1 times

 **leehjworking** 4 months, 2 weeks 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** 4 months, 2 weeks 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** 6 months ago

Selected Answer: C

C is correct

upvoted 2 times

 **dev112233xx** 6 months, 1 week ago

Selected Answer: C

SCP is not enough. IAM permission is needed

upvoted 2 times

 **Damijo** 6 months, 1 week 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** 7 months 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 permisions ?

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

 **bcx** 3 months, 1 week 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

 **deegadaze1** 4 months, 2 weeks ago

Correct !!!

Because of * after the CloudTrail;* at the second DENY RULE of the code.

upvoted 1 times

 **lkyixoayffasdrlaqd** 7 months ago

No not correct.

upvoted 2 times

 **God_Is_Love** 6 months, 4 weeks ago

then you need to explain why not and whats correct

upvoted 1 times

 **testingaws123** 6 months, 2 weeks 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** 4 months, 2 weeks ago

You are wrong ! God_Is_Love was right ...

Check the second code that deny All after CloudTrial

CloudTrail;* -- * Deny all , you will need to add S3 manually!

upvoted 1 times

 **btx** 3 months, 1 week 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

 **c73bf38** 7 months ago

Selected Answer: C

C as SCP is a guardrail, IAM grants permissions.

upvoted 2 times

 **DWsk** 7 months, 1 week 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 cloudtrail action. Being denied cloudtrail wouldn't deny s3 actions.

upvoted 3 times

 **klog** 7 months, 1 week ago

Agree C

upvoted 1 times

 **CloudFloater** 7 months, 2 weeks ago

Thinking A because perhaps you can do the below:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Sid": "DenyCloudTrail",
      "Effect": "Deny",
      "Action": "cloudtrail:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowS3CreateBucket",
      "Effect": "Allow",
      "Action": "s3:CreateBucket",
      "Resource": "*"
    }
  ]
}
```

The first "Allow" statement in the SCP allows all actions on all resources, which would allow the creation of S3 buckets. However, the second "Deny" statement specifically denies all cloudtrail actions, which could potentially impact the ability to create S3 buckets if there is a dependency on cloudtrail for that action. To ensure that the developers are able to create S3 buckets, a new statement with "Allow" effect for the s3:CreateBucket action should be added to the SCP.

upvoted 3 times

 **c73bf38** 7 months, 1 week ago

The s3:CreateBucket will grant the necessary permissions to the developers to create S3 buckets in that account.

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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 21 times

 **aviathor** 2 months ago

The question does not state that the SSM Daemon is running on the instance...

upvoted 1 times

 **mmendozaf** 8 months ago

Assuming that EBS is encrypted, I think that is much easier to run the copy command from AW system manager

upvoted 8 times

 **Atila50** 8 months, 2 weeks ago

thank you for correcting some of these answers and for the explanations to them

upvoted 3 times

 **bititan** Highly Voted  8 months ago

Selected Answer: A

taking a backup of the data to s3. aws doesn't allow up to view snapshots in s3

upvoted 7 times

 **Simon523** Most Recent  2 weeks, 1 day ago

Selected Answer: A

Session Manager provides secure and auditable node management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.

upvoted 1 times

 **AMohanty** 2 weeks, 3 days ago

A

you can log into EC2 using SSM Sessions Manager and copy data onto S3

upvoted 1 times

 **CuteRunRun** 1 month, 3 weeks ago

Selected Answer: C

I prefer C

upvoted 1 times

 **Asamara** 1 month, 3 weeks ago

C is the correct answer.

Explanation:

To meet the requirements of backing up the data without disruption and without having SSH access to the instance, the best approach is:

C) Take a snapshot of the EBS volume using Amazon DLM. Copy the data to Amazon S3.

This allows creating a backup of the EBS volume without needing SSH access to the instance. The snapshot can then be used to copy the data to S3 without impacting the running instance.

A) Attaching a role and using SSM Session Manager would require SSH access which is not available.

B) Creating an AMI and launching a new instance would disrupt the running application.

D) Similarly, launching a new instance from an AMI would disrupt the running application.

So C is the best approach to meet all the requirements - backing up the data without disruption and without SSH access.

upvoted 1 times

 **softarts** 1 month, 3 weeks ago

Selected Answer: C

A=> not mention agent

B=> reboot has downtime

C=> the best one, but not mention how to copy, it need to use an instance to attach to it

D=> assume it is no reboot, the data could be inconsistent

upvoted 1 times

 **chico2023** 1 month, 3 weeks ago

Amazon Linux 2 has the agent installed by default. The only problem with A is that it doesn't say to attach a role that gives you rights to use SSM Session Manager.

upvoted 2 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: A

A or C. I choose A as we have control to the s3 data

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A seems better, s taking a snapshot may impact the application

upvoted 2 times

 **Jonalb** 3 months ago

Selected Answer: A

A and C hmmm

i go A!

upvoted 1 times

 **javitech83** 3 months ago

Selected Answer: A

A is correct

C is not because EBS volume is encrypted and DLM does not support that. <https://repost.aws/knowledge-center/troubleshoot-data-lifecycle-manager-ebs>

upvoted 1 times

 **santi1975** 3 months ago

Sorry, no. DLM can backup encrypted EBS volume, if has access to the KMS keys used to encrypt (obviously). First paragraph:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dlm-access-cmk.html>

upvoted 2 times

 **EricZhang** 3 months, 4 weeks ago

Selected Answer: C

C - <https://aws.amazon.com/ebs/snapshots/>

upvoted 1 times

 **aca1** 4 months ago

Selected Answer: A

Should be A.

If we look deeply to C, take care when reading it:

"C. Take a snapshot of the EBS volume by using Amazon Data Lifecycle Manager (Amazon DLM). Copy the DATA to Amazon S3."

How are you taking a snapshot, but then copying the DATA to Amazon S3.

upvoted 2 times

 **Jesuisleon** 4 months, 1 week ago

A is correct and C is wrong, pls. read this sentence from the question " back up the data from the instance's encrypted Amazon Elastic Block Store (Amazon EBS) volume to an Amazon S3 bucket". You need to copy data inside ec2 instance not the ebs snapshot, so C is wrong

upvoted 2 times

 **Dehradoon** 5 months, 1 week ago

C is the right answer

upvoted 1 times

 **sergza** 5 months, 3 weeks ago

Selected Answer: A

I am leaning towards A due to statements of "Business critical and The application must continue to serve the users." When You do snapshots performance might be affected and essentially not all of the EBS volume needs to be copied just specific data

upvoted 6 times

 **violet99** 5 months, 3 weeks ago

DLM is classic example to backup EBS without downtime, and it doesn't require ssh key

upvoted 1 times

Question #59

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.

 **icassp** Highly Voted  8 months, 1 week 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 14 times

 **masetromain** 8 months, 1 week 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 3 times

 **masetromain** Highly Voted  8 months, 1 week 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 10 times

 **aviathor** Most Recent  3 weeks, 4 days 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 1 times

 **H4des** 1 month, 1 week 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** 1 month, 3 weeks ago

Selected Answer: BDF

I prefer BDF, I do not know why the correct answer is ADF

upvoted 1 times

 **Christina666** 2 months, 3 weeks 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** 2 months, 3 weeks ago

Selected Answer: BDF

it's BDF for sure

upvoted 1 times

 **Maria2023** 3 months, 1 week 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 1 times

 **huanaws088** 5 months, 2 weeks 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 2 times

 **God_Is_Love** 6 months, 4 weeks 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 5 times

 **hobokabobo** 7 months 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(push 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** 7 months, 4 weeks ago

Selected Answer: BDF

BDF are the answers

upvoted 4 times

 **zhangyu20000** 8 months, 1 week ago

BCE

Source user must have role that can write to destination bucket

upvoted 3 times

 **masetromain** 8 months, 2 weeks ago

Selected Answer: BDE

The question is asking for a combination of steps that will successfully copy the data using the AWS CLI.

The correct answer would be B, D and E.

Step B: You must create a bucket policy in the source account that allows the user in the destination account to list and read the source bucket's contents.

Step D: You must create an IAM policy in the destination account that allows the user to list, put and set object ACLs in the destination bucket

Step E: Run the aws s3 sync command as a user in the source account. Specify the source and destination buckets to copy the data.

By doing so, the solution architect will be able to copy the data from the source to the destination bucket.

upvoted 2 times

 **pengpeng** 8 months, 1 week ago

I think it is ADF especially option F as option D is using user in destination account.

upvoted 2 times

 **pengpeng** 8 months, 1 week ago

sorry, typo, BDF

upvoted 2 times

 **Nicocacik** 8 months, 1 week ago

I think that the answer is BDF. If you select steps B and D, you must use a user in the destination account (option F)

upvoted 3 times

 **lochesistemas** 8 months, 1 week ago

If you are specifying Step D where you create an IAM policy in the destination account that allow a user in the destination account to access the source bucket, why are you choosing Step E instead of Step F where it specifies a user on the destination account rather in the source?

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.

 **Atila50** Highly Voted 8 months, 1 week ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/28312-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 9 times

 **masetromain** Highly Voted 8 months, 1 week 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 8 times

 **masetromain** 8 months, 1 week 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 4 times

 **karma4moksha** 4 months, 2 weeks ago

Thank you masetromain, you have been really helpful for taking the time and providing explanation.

upvoted 1 times

 **Jesuisleon** 4 months, 1 week ago

He copied from chatgpt, you didn't find it ?

upvoted 3 times

 **Christina666** Most Recent 2 months, 3 weeks 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** 2 months, 3 weeks ago

Selected Answer: A

D would be an option if used Lambda-specific config

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week 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 1 times

 **AMEJack** 4 months, 3 weeks ago

Sorry OneAtTime

upvoted 1 times

✉  **AMEJack** 4 months, 3 weeks ago

Selected Answer: A

CodeDeploy: Although CodeDeploy can help but AllAtOnce is not used for canary traffic shifting.

upvoted 1 times

✉  **God_Is_Love** 6 months, 4 weeks 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** 7 months, 2 weeks 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** 3 months, 1 week ago

or you know, you could start thinking yourself rather than use glorified rubbish google

upvoted 1 times

✉  **aliasdoe110** 3 months, 1 week ago

Dont get mad, get Glad.

upvoted 1 times

✉  **zhangyu20000** 8 months, 1 week ago

A is correct.

D does not have routing to distribute load

upvoted 1 times

✉  **masetromain** 8 months, 2 weeks 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** 7 months, 1 week ago

You have 2 different answers.....I think it is better you delete this.

upvoted 5 times

✉  **chikorita** 3 months, 3 weeks ago

he can't....nobody can delete once posted

upvoted 1 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.

 **tinyflame** Highly Voted 7 months, 2 weeks 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 17 times

 **masetromain** Highly Voted 8 months, 2 weeks 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 6 times

 **masetromain** 8 months, 2 weeks 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 3 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: B

B of course
 upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

keyword = AWS Transfer for SFTP
 then B
 upvoted 1 times

 **mfsec** 6 months 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 8 times

 **masetromain** 8 months, 2 weeks 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 4 times

 **SorenBendixen** Most Recent 1 month, 1 week 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** 1 month, 2 weeks ago

what the B is wrong is that the VM format, should be OVA or VMDK or VHD, not OVF

upvoted 1 times

 **CuteRunRun** 1 month, 2 weeks ago

Selected Answer: B

I prefer B I do not know why the correct is D.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

it's a B

upvoted 1 times

 **rbm2023** 4 months, 3 weeks ago

Selected Answer: B

<https://www.learnitguide.net/2023/01/how-to-migrate-vmware-vm-to-aws-ec2.html>

upvoted 3 times

 **Brightalw** 1 month, 2 weeks ago

It said the VM fomat is OVA or VMDK, not OVF

upvoted 1 times

 **asifjanjua88** 5 months, 2 weeks ago

I vote to B. Why the admin has selected D as Answer.
upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B
B is the answer - OVF.
upvoted 2 times

 **God_Is_Love** 6 months, 4 weeks ago

Selected Answer: B
Use VM Import/Export. B is correct . <https://aws.amazon.com/ec2/vm-import/>
upvoted 4 times

 **God_Is_Love** 6 months, 4 weeks 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** 7 months, 4 weeks 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.

 **zhangyu20000** Highly Voted 8 months, 1 week 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 18 times

 **masetromain** 8 months, 1 week 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 4 times

 **masetromain** Highly Voted 8 months, 1 week 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 11 times

 **masetromain** 8 months, 1 week 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 4 times

 **CuteRunRun** Most Recent 1 month, 2 weeks ago

Selected Answer: AB

I think is AB

upvoted 1 times

 **Nikkidyky** 2 months, 3 weeks ago

Selected Answer: AB

it's AB

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: AB

AB

its correct!

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week 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** 6 months ago

Selected Answer: B

A + B.

upvoted 2 times

 **dev112233xx** 6 months, 1 week ago

Selected Answer: AB

A+B makes sense to me

upvoted 2 times

 **God_Is_Love** 6 months, 4 weeks 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 3 times

 **klog** 7 months, 1 week ago

Selected Answer: AB

C is not right, question clearly said no involve infrastructure, EC2 is a infrastructure, Lambda time out 15 mins.

upvoted 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: AB

Lambda will time out

A: create Docker image and save it to ECR

B: run this image on Fargate

upvoted 2 times

 **Musk** 7 months, 4 weeks ago

Selected Answer: AB

AB makes most sense

upvoted 2 times

 **masetromain** 8 months, 2 weeks ago

Selected Answer: BC

B and C are correct choices for this question.

B: Creating a new Amazon Elastic Container Service (ECS) task definition with a compatibility type of AWS Fargate and adjusting the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3 can help to prevent invocation failures by breaking up the image processing work into smaller tasks that can be processed concurrently.

C: Creating an AWS Step Functions state machine with a Parallel state to invoke the Lambda function and increasing the provisioned concurrency of the Lambda function can also help to prevent invocation failures by allowing the Lambda function to handle more requests in parallel.

upvoted 1 times

 **masetromain** 8 months, 2 weeks ago

Option A is not a correct answer because it does not address the issue of the Lambda function timing out.

Option D is not a correct answer because it is similar to option B, but it uses Amazon EC2 instead of AWS Fargate which is a more modern and serverless way to run containerized applications.

Option E is not a correct answer because it does not address the issue of the Lambda function timing out.

upvoted 1 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 10 times

 **dkx** Most Recent  2 months, 1 week 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 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

It's. B

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

A seems but previous exist rule

then B is more apropiate in this case

<https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#disallow-rds-storage-unencrypted>

upvoted 1 times

 **EricZhang** 3 months, 4 weeks ago

C - using AWS Config for detective action

upvoted 2 times

 **OCHT** 5 months, 3 weeks 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

 **passthataexam1** 5 months, 2 weeks 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** 6 months ago

Selected Answer: B

Enable the appropriate guardrail

upvoted 2 times

 **Ajani** 6 months, 3 weeks 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 3 times

 **God_Is_Love** 6 months, 4 weeks 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** 7 months, 1 week ago

Selected Answer: B

question is asking for detection, not mandate

upvoted 2 times

 **pitakk** 8 months ago

Selected Answer: B

<https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#disallow-rds-storage-unencrypted>

upvoted 4 times

 **Musk** 7 months, 4 weeks ago

The only thing is that this option talks about guardrails, while the article talks about controls, not mandatory.

upvoted 1 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 11 times

 **masetromain** 8 months, 2 weeks 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** 8 months, 2 weeks 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 3 times

 **God_Is_Love** Highly Voted  6 months, 3 weeks 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 9 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: D

It's D

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: D

keyword = AWS Systems Manager Session Manager
 then D

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: D

D for sure.

upvoted 2 times

 **Ajani** 6 months, 3 weeks 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 1 times

 **lygf** 7 months, 1 week ago

Selected Answer: D

Need to be able to audit the commands ran on the machine.

upvoted 2 times

 **DWsk** 7 months, 1 week 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

 **anita_student** 6 months, 3 weeks 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 2 times

 **lygf** 7 months, 1 week ago

Could option A audit the commands ran on the server, as required by the question? I knew D certainly can.

upvoted 1 times

 **moota** 7 months, 2 weeks 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** 7 months, 2 weeks ago

Selected Answer: B

provide auditing of commands run by the engineers = B Only

upvoted 3 times

 **joefrommnc** 4 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

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.

 **kiran15789** Highly Voted 7 months ago

Selected Answer: BCF

I prefer D over C as IAM cant be applied to Account

upvoted 11 times

 **spd** Highly Voted 7 months, 1 week ago

Selected Answer: BCF

Clear - BCF - SCP is preferable over IAM

upvoted 8 times

 **SK_Tyagi** Most Recent 1 month, 1 week 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 2 times

 **vn_thanhzung** 1 month ago

Sorry I mistake, IAM policies can applied on User.

upvoted 1 times

 **vn_thanhzung** 1 month ago

IAM policies for user ? <https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies-overview.html>

upvoted 1 times

 **CuteRunRun** 1 month, 2 weeks ago

Selected Answer: BCF

BCF is right.

I think SCP is more convenient than iam.

You need to config the IAM to all account manually

upvoted 1 times

 **3f30142** 2 months, 1 week ago

Selected Answer: BCF

prefer SCP over IAM in org accounts

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: BCF

It's a BCF

upvoted 1 times

 **PhuocT** 3 months, 1 week ago

Selected Answer: BCF

C - SCP would be prefer to control the services could be used in Organization's AWS accounts.

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: BCF

Clear - BCF - SCP is preferable over IAM
upvoted 1 times

 **Roontha** 3 months, 3 weeks 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 4 times

 **rbm2023** 4 months, 3 weeks 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

 **Anonymous9999** 5 months, 1 week ago

Selected Answer: BCF

From https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_attach.html

You can attach an SCP to the organization root, to an organizational unit (OU), or directly to an account.

Why attach it to the IAM role when you can make an SCP?

upvoted 3 times

 **yama234** 5 months, 1 week ago

BCF

<https://aws.amazon.com/blogs/mt/control-developer-account-costs-with-aws-cloudformation-and-aws-budgets/>

This solution utilizes integrations with AWS Organizations and AWS CloudFormation in order to deploy a budget to every account in a specific organizational unit in your organization. In turn, this budget will send notifications through Amazon Simple Notification Service (SNS) when forecasted thresholds are exceeded. Then, we will utilize these SNS notifications to execute an AWS Lambda function that will shut down every EC2 instance that is not tagged as critical in a single region.

upvoted 3 times

 **Roontha** 3 months, 3 weeks ago

you are correct. clear use case above mentioned URL

upvoted 1 times

 **Cassa** 5 months, 2 weeks ago

Selected Answer: BDF

Answer: BDF:

SCP it would be ideal but, the question doesn't inform us if the developers accounts are in inside on developers' s OU or if exist one OU for them. Because of this, we have to use an IAM policy to apply the limitation only on Developers account

upvoted 4 times

 **mfsec** 6 months ago

Selected Answer: BCF

BCF - SCP is more efficient at restrictions than using IAM across accounts.

upvoted 2 times

 **[Removed]** 5 months, 1 week ago

it is not possible to apply an SCP to individual user accounts in AWS. Instead, an SCP is applied to an entire account or an OU in AWS Organizations to restrict the permissions of all IAM users and roles within that account or OU.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_attach.html

upvoted 4 times

✉ **zejou1** 6 months, 1 week ago

Selected Answer: BCF

First sentence "A company that uses AWS Organizations..." -
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_ous.html

It is BCF - when they are granted access to the AWS Organization, you will want to set the SCP for the: OrganizationAccountAccessRole. Yes, you "could create" a new IAM role specific to developers, but you can create a SCP for only what is necessary for the developers to do their job.

upvoted 3 times

✉ **vherman** 6 months, 2 weeks ago

Invoke an AWS Lambda function to terminate all services
Is there a Lambda to terminate all services?

upvoted 1 times

✉ **lkyixoayffasdrlaqd** 7 months ago

I ignore everyone here answer includes C and D.
"deny access to costly services and components." What does that mean? WHO is going to decide which services are costly one by one? Come on guys.

upvoted 3 times

✉ **lkyixoayffasdrlaqd** 7 months ago

Answer should be A-B-F

- 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.
- 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.

upvoted 3 times

✉ **hobokabobo** 5 months, 3 weeks ago

good point. Again a question to dice about how to interpret the answers.

upvoted 1 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.

 **masetromain** Highly Voted 8 months, 2 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.

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 10 times

 **masetromain** 8 months, 2 weeks 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** 2 months, 3 weeks 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** Most Recent 1 month 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 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

it's B.

In A - automated snapshots are not shareable

upvoted 1 times

 **Maria2023** 3 months, 1 week 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** 3 months, 1 week 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** 3 months, 1 week 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** 3 months, 1 week 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** 4 months, 3 weeks 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 2 times

 **takecoffee** 5 months, 3 weeks ago

Selected Answer: B

You can share the following Amazon Aurora resources by using AWS RAM.

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: B

B is the way forward

upvoted 2 times

 **God_Is_Love** 6 months, 3 weeks 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** 5 months, 2 weeks 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** 7 months, 4 weeks ago

Selected Answer: B

B is correct. Move Lambda and Aurora both to target account

upvoted 4 times

 **Musk** 7 months, 4 weeks ago

Selected Answer: B

B can be done with this: https://aws.amazon.com/about-aws/whats-new/2019/07/amazon_aurora_supportscloningacrossawsaccounts-/

upvoted 3 times

 **SK_Cert_master** 8 months, 1 week ago

B.

It seems that Lambda cannot be shared via RAM

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

upvoted 2 times

 **Satya80** 6 months, 4 weeks ago

As per the above link, Lambda can be shared. Please see the "Subnets" section .

upvoted 1 times

 **Sarutobi** 6 months, 4 weeks ago

You cannot share lambda, but creating a Lambda in a shared subnet is allowed.

upvoted 2 times

 **Satya80** 6 months, 4 weeks ago

scratch that

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

B is correct. Move Lambda and Aurora both to target account

A: not move Aurora

C: Lambda not move

d: Lambda and Aurora both not moved

upvoted 3 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 12 times

 **hamimelon** 3 weeks ago

Agree. Also, it says the company does not wanna manage long-term overhead, which points to serverless.

upvoted 1 times

 **masetromain** 8 months, 2 weeks 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 2 times

 **zhangyu20000** Highly Voted 8 months, 1 week ago

A is correct, it provide HA, scale, less management. Task only need 5 minutes

B: even more complex

C: container still run on one EC2, not scale

D: need container, Fargate and Lambda. Complex than A

upvoted 6 times

 **kjcncjek** Most Recent 2 weeks, 1 day ago

running lambda for 5 minutes is not cost effective, so answer is D

upvoted 1 times

 **Greeye** 1 month, 1 week 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** 1 month, 2 weeks ago

Selected Answer: A

I prefer A

upvoted 1 times

 **chico2023** 1 month, 3 weeks 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** 2 months, 3 weeks ago

Selected Answer: A

it's A

upvoted 1 times

 **rbm2023** 4 months, 3 weeks 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** 4 months, 3 weeks 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 2 times

 **devopsy** 5 months, 2 weeks ago

If the process takes less than 15 mins, the answer is usually lambda

upvoted 2 times

 **SmileyCloud** 3 months, 2 weeks ago

Correct. Anytime you see a process or a batch script that needs to be moved off EC2 and execution time is less than 15 min, your best bet is that Lambda is the answer.

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

Migrate the data processing script to an AWS Lambda function.

upvoted 1 times

 **Asagumo** 6 months ago

Selected Answer: D

There are two points of concern when choosing Lambda in the following two ways

The fact that the original EC2 specs are so fast that it may take only 5 minutes to complete.

The fact that the average time is only 5 minutes, so there may be cases where the time exceeds 15 minutes.

upvoted 3 times

 **dev112233xx** 6 months, 1 week ago

Selected Answer: A

A best practice to handle files in S3

upvoted 1 times

 **hobokabobo** 6 months, 3 weeks ago

It asks for the most cost effective solution.

While Lambda may be simple and cheap for if you have only a few invocations and low memory requirements.

As processing is called every 10 minutes. The EC2 is indeed idle for 40% of the time, 60% of the time its under load. But we are asked to look at how it scales - in regards to cost.

We have a 60% used EC2. Lambda costs explode when it scales.

Lambda is the by far most expensive solution.

B) is more cost effective.

(Who votes for Lambda when it comes to cost for processing big load, never had to pay the AWS bill for it.)

upvoted 2 times

 **hobokabobo** 6 months, 3 weeks ago

Also "long-term management overhead" should be reduced. Ec2 the long term management overhead is way lower than maintaining Lambda.

upvoted 1 times

 **Greyeye** 1 month, 1 week ago

how would anyone say EC2 overhead is less than lambda?

You need to manage a server, patch them, nurture them and when service crashes for any reason, you need to restart for some means. (need monitoring.)

I agree Lambda cannot be used for 100% of usecases but I would make stuff run on lambda over managing EC2 any day. (I hate shit running on ec2 and fail)

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks ago

Selected Answer: A

A and D are good but A is most cost effective as asked in question. B has only one instance that means not highly available. C has container/ec2 combo with more work on ec2 which is cost ineffective and more operating effort.

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks ago

D is not cost effective and not good.. (meant C in above comment)

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: A

the script takes approximately 5 minutes==>Lambda is the simplest solution (compared to D)

upvoted 2 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 11 times

 **masetromain** 8 months, 2 weeks 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 2 times

 **masetromain** 8 months, 2 weeks 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 2 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: C

It's C

upvoted 1 times

✉  **mfsec** 6 months ago

Selected Answer: C

C for DR

upvoted 2 times

✉  **God_Is_Love** 6 months, 3 weeks 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** 6 months, 3 weeks 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** 7 months, 4 weeks ago

Selected Answer: C

active-passive failover==>a failover routing policy within route 53

upvoted 4 times

✉  **zhangyu20000** 8 months, 1 week 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.

 **masetromain** Highly Voted  8 months, 1 week 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 15 times

 **dev112233xx** Highly Voted  6 months, 1 week 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 6 times

 **3f30142** Most Recent  2 months, 1 week 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

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

It's D.

B would work if was supported

upvoted 1 times

 **karma4moksha** 4 months, 2 weeks 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 2 times

 **rbm2023** 4 months, 3 weeks 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 3 times

 **Cccb35** 4 months, 3 weeks 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 2 times

 **Amac1979** 6 months ago

Selected Answer: D

D as Vherman said below

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: D

Option D is the most cost-effective

upvoted 2 times

 **vherman** 6 months, 2 weeks ago

Selected Answer: D

D is correct

There is no IAM Identity Center feature in Organizations. hence, B is out

upvoted 3 times

 **senhorjorge** 6 months, 1 week ago

Yes there is and it should be all you need to enable, therefore B is correct.

upvoted 2 times

 **anita_student** 6 months, 3 weeks ago

Selected Answer: D

See pre-requisites for AWS SSO: <https://docs.aws.amazon.com/singlesignon/latest/userguide/get-started-prereqs-considerations.html>

upvoted 2 times

 **God_Is_Love** 6 months, 3 weeks ago

Selected Answer: B

Question : Does aws AD connector configuration needs aws organization features turned on ?

ChatGPT : Answer No, AWS Microsoft AD Connector does not require AWS Organization features to be turned on.

The AWS Microsoft AD Connector is a standalone service that enables you to connect your AWS resources to an existing Microsoft Active Directory (AD) domain or forest. It does not depend on or require any specific AWS organization features or settings.

However, if you are using AWS Directory Service to create a new AD directory in AWS, you can choose to enable AWS Organizations integration to simplify the management of multiple AWS accounts. This integration allows you to manage AWS Directory Service directories across multiple AWS accounts and regions from a single master account.

But again, this is an optional feature and does not affect the functionality of the AWS Microsoft AD Connector itself. You can use the AWS Microsoft AD Connector without enabling AWS Organizations integration if you prefer.

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks ago

This link someone posted <https://docs.aws.amazon.com/singlesignon/latest/userguide/get-started-prereqs-considerations.html> is in favor of D. but I think, here in question , its a single account only. I am resistant to choose D, I could be wrong though.

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks ago

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html

I assume single account is Management account and it does not need org features enabled.See above link and follow all steps listed there. no necessity to enable organizations features. I stick with B only.

upvoted 2 times

 **spd** 7 months, 1 week ago

Selected Answer: D

Correcting the Answer - Its D

upvoted 2 times

 **spd** 7 months, 1 week ago

Selected Answer: B

B - Why need all feature

upvoted 1 times

 **Musk** 7 months, 1 week ago

It's D. You need it s explained in <https://docs.aws.amazon.com/singlesignon/latest/userguide/get-started-prereqs-considerations.html>

upvoted 5 times

 **spd** 7 months, 1 week ago

Thanks, so its not B.

upvoted 1 times

 **Musk** 7 months, 1 week ago

Exactly, it's not B. Additionally, B refers to enabling IAM Identity Center in Organizations, and you would enable that in the IAM Identity Center console. What's confusing about D is that it does not refer to enabling it.

upvoted 1 times

 **DWsk** 7 months, 1 week ago

Selected Answer: D

This one is tricky because in order to enable SSO in Organizations you need to enable all features. Thanks @moota for the explanation

upvoted 4 times

 **klog** 7 months, 1 week ago

Selected Answer: B

just need a feature with AD connector

upvoted 1 times

 **moota** 7 months, 2 weeks ago

Selected Answer: D

There are only two feature sets to turn on.

All features – The default feature set that is available to AWS Organizations. It includes all the functionality of consolidated billing, plus advanced features that give you more control over accounts in your organization.

Consolidated billing – This feature set provides shared billing functionality, but doesn't include the more advanced features of AWS Organizations. For example, you can't enable other AWS services to integrate with your organization to work across all of its accounts, or use policies to restrict what users and roles in different accounts can do. To use the advanced AWS Organizations features, you must enable all features in your organization.

upvoted 3 times

 **c73bf38** 7 months, 1 week ago

The keyword is "Accounts" vs "single account", why is All Features required for a single account?

upvoted 1 times

 **Sarutobi** 6 months, 4 weeks ago

Take a look at this link: <https://docs.aws.amazon.com/singlesignon/latest/userguide/get-started-prereqs-considerations.html> scroll down to "If you've already set up AWS Organizations, make sure that all features are enabled."

upvoted 1 times

 **scuzzy2010** 7 months ago

Because the ONLY OTHER option is to enable Consolidated Billing, which is of no use here, hence All Features must be enabled

upvoted 1 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.

 **zozza2023** Highly Voted  7 months, 4 weeks ago

Selected Answer: AD

Transfer Accelerator + Multi-part uploads for files more 500MB

upvoted 6 times

 **chico2023** Most Recent  1 month 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** 2 months, 3 weeks ago

Selected Answer: AD

its AD

upvoted 1 times

 **Maria2023** 3 months, 1 week ago

Selected Answer: AD

A and D satisfy the requirement

upvoted 1 times

 **SkyZeroZx** 4 months, 1 week ago

Selected Answer: AD

Transfer Accelerator + Multi-part uploads for files more 500MB

Question similar to AWS Certified Solutions Architect Associate

upvoted 1 times

 **OCHT** 5 months, 3 weeks 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 4 times

 **mfsec** 6 months ago

Selected Answer: AD

AD all day

upvoted 2 times

 **aqiao** 6 months, 2 weeks ago

Selected Answer: AD

B is not suitable here, since it wants to improve upload experience, not download

upvoted 2 times

 **Musk** 7 months, 4 weeks 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** 8 months, 1 week ago

AD is correct

upvoted 1 times

 **masetromain** 8 months, 2 weeks 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** 8 months, 2 weeks 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** 6 months, 3 weeks 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

 **God_Is_Love** Highly Voted  6 months, 3 weeks 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 5 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: B

it's a B

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

keyword = RDS proxy

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B

Create an RDS proxy.

upvoted 1 times

 **klog** 7 months, 1 week ago

Selected Answer: B

proxy will be a buffer

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

B is correct.

C: Aurora is useless, Proxy is pointing to existing RDS

upvoted 4 times

 **masetromain** 8 months, 2 weeks 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** 6 months, 3 weeks ago

What?? Aurora does not support Multi AZ ? its a blunder !

upvoted 4 times

✉️ 🚩 **BabaP** 3 months, 3 weeks ago

they are copying the answers from chatgpt

upvoted 4 times

✉️ 🚩 **k8s_Seoul** 2 weeks, 6 days ago

masetromain ~> X

GPTromain ~> O lol

upvoted 1 times

✉️ 🚩 **chikorita** 3 months, 3 weeks ago

was about to point this

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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 11 times

 **masetromain** 8 months, 2 weeks 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 2 times

 **waoo** Most Recent  1 month, 3 weeks ago

答案是C

<https://aws.amazon.com/cn/iot-core/faqs/?nc=sn&loc=5&dn=2>

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

it's C

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

I choose C

upvoted 1 times

 **zejou1** 6 months, 1 week 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 1 times

 **forceli** 6 months, 2 weeks 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** 6 months, 2 weeks ago

Sorry I meant "C"

upvoted 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

C is correct (less op overhead than A)

upvoted 2 times

 **zhangyu20000** 8 months, 1 week 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.

 **God_Is_Love** Highly Voted  6 months, 3 weeks 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 11 times

 **rbm2023** Highly Voted  4 months, 3 weeks 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 6 times

 **venvig** Most Recent  1 month 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** 1 month, 2 weeks ago

Selected Answer: C

I prefer C, because you need to give permission to cloud formation

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C no doubt

upvoted 1 times

 **mfsec** 6 months 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** 7 months ago

Selected Answer: C

C IAM policy is allowing to provision of approved resources.

upvoted 3 times

 **Musk** 7 months, 4 weeks ago

Selected Answer: C

B does not enforce CF, otherwise it would work.

upvoted 3 times

Untamables 8 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 2 times

Nicocacik 8 months, 1 week ago

Selected Answer: C

You have to use a service role

upvoted 4 times

masetromain 8 months, 1 week 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 8 months, 1 week 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

upvoted 1 times

zhangyu20000 8 months, 1 week 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 2 times

masetromain 8 months, 1 week 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

masetromain 8 months, 2 weeks ago

Selected Answer: B

The correct answer is 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.

This solution will meet the requirement of enforcing the new restriction on the IAM role that the engineers use for access by only allowing the engineers to use AWS CloudFormation to provision the approved resources. By updating the IAM policy to only allow provisioning of approved resources and AWS CloudFormation, it will restrict the engineers from provisioning any other resources. Engineers will use AWS CloudFormation templates to create stacks with approved resources, which will ensure that only the approved resources are being provisioned.

upvoted 1 times

zhangyu20000 8 months, 1 week ago

it allows provision of approved resources and CF in same time. User can provision resources directly without CF

upvoted 3 times

masetromain 8 months, 2 weeks ago

Other options are not the correct answer because:

Option A only allows access to Amazon S3 and AWS CloudFormation, but it doesn't restrict the engineers from provisioning resources other than the approved ones

Option C only allows AWS CloudFormation actions, but it doesn't restrict the engineers from provisioning resources other than the approved ones

Option D is incomplete, it doesn't specify how to restrict the engineers from provisioning resources other than the approved ones

upvoted 2 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 13 times

 **masetromain** 8 months, 2 weeks 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 2 times

 **vjp_training** Most Recent  6 days, 21 hours ago

Selected Answer: B

B is the best for cost-effective.

D is more cost for S3 request

upvoted 1 times

 **uC6rW1aB** 3 weeks, 1 day 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 1 times

 **uC6rW1aB** 3 weeks, 1 day 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 2 times

 **Gmail78** 4 weeks, 1 day 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** 3 weeks, 4 days ago

D - S3 metadata search feature does not exist
upvoted 1 times

 **Soweetadad** 1 month ago

Selected Answer: D

Although both B and D are correct, Option D is more cost effective.

upvoted 1 times

 **dkx** 2 months, 1 week 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 relation 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 3 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: D

Going with D as it's more cost effective. Question didn't ask for more efficient.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

D is more cost effective, evenif more complex

upvoted 2 times

 **[Removed]** 3 months 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 1 times

 **geo1551** 3 months, 2 weeks 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** 5 months, 1 week 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** 4 months, 3 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** 6 months ago

Selected Answer: B

B DynamoDB

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B

B. Design the application to store each incoming record in an Amazon DynamoDB table

upvoted 1 times

 **DDONG** 8 months ago

B SAP01 #613

upvoted 3 times

 **zhangyu20000** 8 months, 1 week ago

C is correct

Dynamodb support 4KB size, low latency and TTL

upvoted 3 times

✉ **Atila50** 8 months, 1 week ago

do yo mean B
upvoted 1 times

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

<https://www.examtopics.com/discussions/amazon/view/28419-exam-aws-certified-solutions-architect-professional-topic-1/>

Option C is using RDS MySQL which is a relational database and will not be able to handle the scale of millions of small records per minute with low latency and it is not designed for automatic deletion of records based on time and it will be more expensive as well.

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.

 **zejou1** Highly Voted  6 months, 1 week 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 8 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: D

D for sure

upvoted 1 times

 **rbm2023** 4 months, 3 weeks 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** 6 months ago

Selected Answer: D

D makes the most sense

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks 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** 6 months, 4 weeks 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** 6 months, 4 weeks 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** 8 months, 1 week ago

Selected Answer: D

for B,C, Amazon RDS does not support global tables yet. Only Aurora supports.

upvoted 4 times

 **AlanKrish** 7 months, 1 week ago

Is Aurora not part of RDS? You can choose Aurora's compatibility with MySQL and PostgreSQL).

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

D is correct

upvoted 3 times

 **masetromain** 8 months, 1 week 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

 **[Removed]** 7 months, 1 week 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

 **Shahul75** 7 months, 3 weeks ago

B is not right. Only Aurora has global tables. RDS don't

upvoted 1 times

 **masetromain** 8 months, 1 week ago

<https://www.examtopics.com/discussions/amazon/view/69438-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

 **masetromain** 8 months, 2 weeks 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** 6 months, 4 weeks 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** 8 months, 2 weeks 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

 **btx** 3 months, 1 week 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.

 **rbm2023** Highly Voted 4 months, 3 weeks 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 a incorrect way. The soul purpose of the gateway is to have point for interconnectivity.

upvoted 5 times

 **Russ99** Most Recent 4 weeks, 1 day 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 1 times

 **CuteRunRun** 1 month, 2 weeks ago

Selected Answer: A

I think A is right, I do not know why other guys select D

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

surely A

upvoted 1 times

 **Tunstim** 4 months, 3 weeks 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 1 times

 **chikorita** 1 week, 6 days ago

please reply to him

upvoted 1 times

 **Parsons** 5 months 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** 6 months ago

Selected Answer: A

Solution A is the only one possible solution

upvoted 1 times

 **Arnaud92** 6 months 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

 **Arnaud92** 6 months 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 S2SVPN 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 attached to a single VPC. A S2S VPN cannot multiplex VPC

upvoted 4 times

 **mfsec** 6 months ago

Selected Answer: A

A. Create a transit gateway. Attach the Site-to-Site VPN

upvoted 1 times

 **dev112233xx** 6 months, 1 week ago

Selected Answer: A

A makes sense to me

upvoted 1 times

 **taer** 6 months, 1 week ago

Selected Answer: A

A for me

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks 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** 6 months, 3 weeks ago

oops this is wrong..VPN can be attached...

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks ago

Moderator, please delete this comment..

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks 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** 6 months 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 entities (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** 7 months, 1 week ago

Selected Answer: A

TGW is the solution

upvoted 1 times

 **CloudFloater** 7 months, 2 weeks 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

 **Arnaud92** 6 months 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

 **Sarutobi** 6 months, 4 weeks 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

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: A

solution is A

upvoted 1 times

 **masetromain** 8 months, 1 week ago

Selected Answer: A

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.

This option will allow you to connect from the on-premises servers to VPC B with the least operational effort, as it utilizes the transit gateway to connect all networks and allows for easy updates to the route tables. BGP propagation is not necessary and the use of transit gateway will simplify the traffic routing.

upvoted 4 times

 **masetromain** 8 months, 1 week ago

The correct answer is 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.

This option allows for all three networks (on-premises, VPC A and VPC B) to be connected through the transit gateway, which simplifies the traffic routing and makes it easy to update the route tables for all networks. It also eliminates the need for a separate Site-to-Site VPN connection between the on-premises network and VPC B, which would add unnecessary complexity.

upvoted 1 times

 **masetromain** 8 months, 1 week ago

Option B is not correct because it would require a separate Site-to-Site VPN connection between the on-premises network and VPC B, which would add unnecessary complexity and effort.

Option C is not correct because updating the route tables for all three networks and configuring BGP propagation can be a complex process, and waiting for BGP propagation to finish would add an unnecessary delay.

Option D is not correct because modifying the Site-to-Site VPN's virtual private gateway definition to include VPC A and VPC B and splitting the two routers of the virtual private gateway between the two VPCs would be overly complex and difficult to manage. It will not be the most efficient solution and adding unnecessary complexity to the existing solution.

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

A is correct. on-premise is connected to TGW, use TDW to talk to VPC A/B

B: too many VPN connections

C: VPC B cannot use VPC A to VPN

D: one VPN gateway cannot be associated with more than one VPC

upvoted 3 times

 **masetromain** 8 months, 1 week ago

Is correct that option A is the correct answer. Thank for you help.

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.

 scuzzy2010  7 months 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 11 times

 God_Is_Love 6 months, 3 weeks 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 4 times

 Untamables  8 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 6 times

 CuteRunRun  1 month, 2 weeks ago

Selected Answer: A

I selecte A

upvoted 1 times

 NikkyDicky 2 months, 3 weeks ago

Selected Answer: B

It's B - to preserve SMTP protocol

upvoted 1 times

 SkyZeroZx 3 months, 1 week 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 4 months, 2 weeks 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 4 months, 3 weeks 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 2 times

 **Cassa** 5 months, 1 week 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** 6 months ago

Selected Answer: B

B. Configure the application to connect to Amazon SES by using STARTTLS.

upvoted 1 times

 **Dimidrol** 6 months, 1 week ago

Selected Answer: B

B , <https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>

upvoted 3 times

 **dev112233xx** 6 months, 1 week 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** 3 months, 3 weeks 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** 6 months, 2 weeks 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** 6 months, 2 weeks 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** 6 months, 2 weeks 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 really work with smpt auth.(I didn't get it to work and it seems no one else either)

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>

For new apps, C should be correct. But here, Its re-platforming strategy migrating from SMTP to SES

STARTTLS vs TLS Wrapper is being tested here. (A or B) But A sounds 25 port communication which the existing app uses. So B should be correct

upvoted 3 times

✉ **Musk** 7 months, 4 weeks ago

Selected Answer: B

It's B, becuase D is discarded since "The application can use SMTP only."

upvoted 1 times

✉ **Musk** 7 months, 4 weeks ago

I doubt between B and D. Both seem correct to me.

upvoted 1 times

✉ **boomx** 8 months ago

Selected Answer: B

B

STARTTLS works over 25, less change. Also SES SMTP interface needs SMTP credentials

<https://docs.aws.amazon.com/ses/latest/dg/smtp-credentials.html>

upvoted 3 times

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

Selected Answer: A

The correct answer is option 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."

Option B is incorrect as it suggests to use SMTP with STARTTLS to connect to Amazon SES, which is a less secure method than using a secure wrapper such as TLS Wrapper. Option B also suggests using long-term SMTP credentials which could be a security concern.

Option C is incorrect as it suggests to use the SES API to send email messages, which is not necessary as the application can only use SMTP.

Option D is incorrect as it suggests to use AWS SDKs to send email messages, which is not necessary as the application can only use SMTP. Also, it suggests to use IAM user for Amazon SES which is also a security concern as it will involve long-term credentials as well.

upvoted 2 times

✉ **hobokabobo** 6 months, 2 weeks ago

A) what tls wrapper are you talking about?

B) "Starttls is less secure": SES AWS Mailservers support Starttls anf you have no way of reconfigure the AWS severs.

(With Starttls the *server* accepts unencrypted and encrypted incomming smtp mail. The client just connects with smpt encrypted or not, the server will accept both. ...)

upvoted 2 times

✉ **BabaP** 3 months, 3 weeks ago

lol the answers are copied from chatgpt.

upvoted 3 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 10 times

 **CuteRunRun** Most Recent 1 month, 2 weeks ago

Selected Answer: A

I prefer A

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

its n A

upvoted 1 times

 **Maria2023** 3 months, 1 week 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** 4 months, 2 weeks 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 2 times

 **mfsec** 6 months ago

Selected Answer: A

A. Create an AWS Cost and Usage Report for the organization.

upvoted 1 times

 **moota** 7 months, 2 weeks ago

Selected Answer: A

I can customize reporting in Cost Explorer but cannot find how to do templates.

upvoted 4 times

 **zhangyu20000** 8 months, 1 week 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.

 **masetromain**  8 months, 2 weeks 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 14 times

 **masetromain** 8 months, 2 weeks 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

 **SuperP43** 6 months, 4 weeks 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 3 times

 **Gmail78** 1 month, 1 week ago

not the best but not impossible <https://aws.amazon.com/blogs/big-data/near-zero-downtime-migration-from-mysql-to-dynamodb/>
upvoted 1 times

 **tromyunpak** 3 months, 3 weeks 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** 3 months, 3 weeks ago

also rds proxy is not used (sorry typo) to handle write operations properly
upvoted 1 times

 **kamaro** 6 months, 2 weeks 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 1 times

 **zejou1** 6 months, 1 week 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** 4 months, 2 weeks 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

 **OCHT** 5 months, 3 weeks 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

 **duriselman** Most Recent 1 month, 1 week 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

 **duriselman** 1 month, 1 week ago

c and E ans 100 %

upvoted 1 times

 **rizzu2023** 1 month, 2 weeks ago

CE

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

upvoted 1 times

 **easystoo** 2 months ago

b-c-b-c-b-c-b-c

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: CE

CE for sure. classic IoT use case

upvoted 1 times

 **Asds** 3 months, 1 week ago

Selected Answer: BD

Rds MySQL to Aurora to scale automatically and stay relational

upvoted 1 times

 **HussamShokr** 3 months, 1 week 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** 3 months, 1 week 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** 3 months, 2 weeks 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** 4 months 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

 **rbm2023** 4 months, 3 weeks ago

Selected Answer: CE

we really should consider the COST for adopting Dynamo, currently the expected data is 4TB which would be much more expensive than migrating to Aurora, still, adding READ replicas does not necessarily helps the issue. So this question is completely tricky.

combinations of B and C or C and E should be acceptable in my view.

voting for C and E anyway only because the read replicas in aurora would not fix the write issues

upvoted 2 times

 **petervu** 4 months, 3 weeks ago

Selected Answer: BC

We can't simply change database from SQL to noSQL so I think E is not appropriate. BC should be better choice.

upvoted 3 times

 **OCHT** 5 months, 3 weeks ago

Selected Answer: BD

B. Amazon Aurora is a high-performance and cost-effective alternative to using RDS MySQL. It is specifically designed for the cloud and is optimized for high concurrency and low latency. By migrating to Aurora, the company can take advantage of its ability to automatically scale resources to meet demand, while providing fast and consistent performance. Additionally, Aurora supports read replicas, which can help distribute the workload and improve query performance.

D. AWS X-Ray can help identify issues with the application and API servers. By analyzing X-Ray traces, the company can identify which API endpoints are experiencing high latency and prioritize optimization efforts accordingly. Additionally, adding more API servers can help distribute the load and improve performance. This approach allows for more granular scaling of the application tier, as opposed to simply adding more resources to the RDS instance, which may not fully address the underlying issues.

upvoted 1 times

 **OCHT** 5 months, 2 weeks ago

My mistake. The correct answers are B and C.

B. Re-architecting the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and adding read replicas can improve performance and scalability. Amazon Aurora is a MySQL-compatible database that can deliver up to five times the performance of MySQL without requiring changes to most of your existing applications. Adding read replicas can help offload read traffic from the primary instance and improve read performance.

C. Leveraging Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data can help reduce the load on the API servers and improve performance. Kinesis Data Streams can capture, store, and process large amounts of data in real-time, while AWS Lambda can automatically scale to process the data as it arrives.

These two options together will resolve the issues permanently and enable growth as new sensors are provisioned while keeping this platform cost-efficient.

upvoted 3 times

 **mfsec** 6 months ago

Selected Answer: CE

CE is the best choice. DynamoDB is the better choice for the IoT sensors growth.

upvoted 2 times

 **dev112233xx** 6 months, 1 week ago

Selected Answer: BD

BD fit the requirement. (Cost efficient)

CE are the opposite of the requirement, DynamoDB and Kinesis more expensive than Aurora for large scale apps .. even DynamoDB alone more expensive than Aurora for large scale apps

upvoted 1 times

✉️  **dev112233xx** 6 months, 1 week ago

I forgot to mention that DynamoDB is noSQL database, and requires also a big refactor in the NodeJS app. Does not make sense here to choose DynamoDB over Aurora (MySQL)..

upvoted 1 times

✉️  **Damijo** 6 months, 1 week ago

Selected Answer: BC

<https://www.examtopics.com/discussions/amazon/view/5011-exam-aws-certified-solutions-architect-professional-topic-1/> DynamoDB or other NoSQL options are not the solutions when organizations need to store predictable, structured data. In that case, Amazon Aurora is the best solution with high scalability and best performances.

upvoted 3 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 9 times

 **masetromain** 8 months, 2 weeks 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 3 times

 **masetromain** 8 months, 2 weeks ago

<https://www.examtopics.com/discussions/amazon/view/69470-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

 **bcx** 3 months, 1 week 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** 2 weeks, 4 days 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 1 times

 **AMohanty** Most Recent  2 weeks, 3 days 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** 3 weeks 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 4 weeks, 1 day ago

Selected Answer: CD

even though option D is complex, it would decrease the latency outside eu region.

upvoted 2 times

nharaz 1 month, 1 week 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 1 month, 2 weeks 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

chico2023 1 month, 3 weeks 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 São Paulo and the other in Cape Town? How much will it improve for users in Auckland, if that's the case?

There is a 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 2 times

easytoo 2 months 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

aviathor 2 months ago

Selected Answer: CD

C: <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-basic-concept.html#apigateway-definition-edge-optimized-api-endpoint>

D: If the users are globally distributed, it would be beneficial to provision the entire stack in other regions...

upvoted 2 times

aviathor 2 months ago

C: <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-basic-concept.html#apigateway-definition-edge-optimized-api-endpoint>

D: If the users are globally distributed, it would be beneficial to provision the entire stack in other regions...

upvoted 1 times

khksoma 2 months, 1 week ago

A and C

<https://www.blendedsoftware.com/articles/how-to-accelerate-file-uploads-with-aws-s-3>

upvoted 1 times

dkx 2 months, 1 week ago

C. Yes, because an edge-optimized API endpoint is best for geographically distributed clients. API requests are routed to the nearest CloudFront Point of Presence (POP).

D. Yes, because this question is NOT about cost-effectiveness, it is about a POC with its largest customer that seemingly went poorly, as they MUST improve latency outside of Europe.

A. No, because this only addresses part of the latency issue, S3 transfer speeds, but does not address the largest customer's geographic distance from the entire stack.

B. No, because endpoints for can be NLB, ALB, EC2 and Elastic IPs, but not CloudFront

E. No, because adding an Amazon RDS proxy between the Lambda functions would help with connection pooling, and does not match any other option

upvoted 1 times

hexie 2 months, 3 weeks ago

Selected Answer: BC

Why people are going for A if Transfer Acceleration is mainly to improve the upload and download speeds for objects in an S3 bucket? I'm sick of these ChatGPT answers tho.

Dude, in the given scenario, the requirement is to IMPROVE LATENCY outside of Europe, specifically for the web application and API Gateway endpoints.

Creating an accelerator with AWS Global Accelerator and attaching it to CloudFront, traffic will be routed through AWS global network, optimizing latency for users outside of Europe as requested :)

upvoted 1 times

lxrdm 2 months, 1 week ago

Global accelerator does not support CloudFront

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoints.html>

upvoted 2 times

nicecurls 2 months, 3 weeks ago

Selected Answer: CD

A is wrong!

upvoted 1 times

NikkyDicky 2 months, 3 weeks ago

Selected Answer: CE

C -- no brainer

E is totally supported (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>)

A not applicable (upload is not direct to s3), B make no sense. D is a dumb idea

upvoted 1 times

aviathor 2 months ago

E is "totally supported" but won't do much good with the latency...

upvoted 1 times

hexie 2 months, 3 weeks ago

Selected Answer: CD

Im going with C and D

Im sorry, but I cant get what do A option mean by "Transfer Acceleration signed URLs". Its a tricky option because it starts with S3 Transfer Acceleration.

D is right because If the users are globally distributed, it would be beneficial to provision the entire stack in other regions

upvoted 3 times

Parimal1983 3 months ago

Selected Answer: CD

Question asked to reduce latency. So with option C and D overall latency can be reduced. With option A, says signed URL which is wrong, instead if it would have mentioned Transfer Accelerator Endpoint then might be make more sense.

upvoted 2 times

Parimal1983 3 months ago

Moreover, setting up environment in 2 region will also helpful. Lambda is regional, using Aurora global database, improve performance and reduce latency ultimately.

upvoted 1 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 6 times

 **masetromain** 8 months, 2 weeks 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** 7 months, 4 weeks ago

Option D works for the reduction cost on retrieval request

upvoted 1 times

 **youngprinceton** 7 months, 4 weeks ago

take the test then tell us if your answers are valid, if they are share them with us ;)

upvoted 1 times

 **uC6rW1aB** Most Recent  3 weeks 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** 1 month, 2 weeks ago

Selected Answer: A

A is right

upvoted 1 times

 **aviathor** 2 months 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** 2 months, 3 weeks ago

Selected Answer: A

A of course

upvoted 1 times

✉ **Maria2023** 3 months, 1 week 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** 6 months ago

Selected Answer: A

A - easy question

upvoted 1 times

✉ **dev112233xx** 6 months, 1 week ago

Selected Answer: A

A - S3 Intelligent-Tiering can fit the requirement

upvoted 1 times

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

*I meant even after 30 days (not downloads in above comment)

upvoted 1 times

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

There are lots of wrong types. Please forgive me. English is not familiar with me yet.

upvoted 2 times

✉ **c73bf38** 7 months ago

The keyword is millisecond retrieval time, which rules everything out except A.

upvoted 2 times

✉ **klog** 7 months, 1 week 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** 7 months, 4 weeks ago

Selected Answer: A

typico A S3 Intelligent-Tiering

upvoted 2 times

✉ **jhonivy** 7 months, 4 weeks 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.

 **zejou1** Highly Voted  6 months, 1 week 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 7 times

 **Untamables** Highly Voted  8 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 6 times

 **zozza2023** 7 months, 4 weeks ago

agree with u gess aws want us to know about Lens

upvoted 2 times

 **Simon523** Most Recent  1 week, 1 day 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 1 times

 **AMohanty** 2 weeks, 2 days ago

C

Storage Class is only used for recommendation for Standard to Standard IA

upvoted 1 times

 **uC6rW1aB** 3 weeks 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** 2 months, 3 weeks 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** 2 months, 3 weeks ago

Selected Answer: C

a hard one ... I guess C, but could be B :/
upvoted 1 times

 **Limlimwdwd** 3 months, 3 weeks 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** 4 months, 2 weeks ago

Selected Answer: C

SCAs recommendations are based on the previous 30-90 days. <https://aws.amazon.com/s3/faqs>
upvoted 1 times

 **Maria2023** 5 months 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

 **Cassa** 5 months, 1 week ago

Selected Answer: C

Amazon S3 Storage Lens is the best choice in this case.

<https://aws.amazon.com/pt/getting-started/hands-on/amazon-s3-storage-lens/>
upvoted 2 times

 **OCHT** 5 months, 2 weeks ago

Selected Answer: C

The solutions architect can upgrade the default dashboard to include advanced metrics for storage trends. (Option C)

Amazon S3 Storage Lens provides organization-wide visibility into object storage usage and activity trends. The default dashboard provides a summary of storage usage and activity metrics, and the advanced metrics option provides additional insights into data access patterns and data transfer costs. By analyzing these metrics, the solutions architect can identify trends and determine the appropriate storage class for the objects to optimize costs.

upvoted 3 times

 **Amac1979** 6 months ago

Selected Answer: C

C - storage lens
upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: C

C - storage lens
upvoted 2 times

 **Damijo** 6 months, 1 week ago

Selected Answer: C

C - <https://aws.amazon.com/blogs/storage/5-ways-to-reduce-costs-using-amazon-s3-storage-lens/>
upvoted 2 times

 **andras** 6 months, 3 weeks ago

S3 is not among the cost optimization in trusted Advisor:
<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html>
upvoted 1 times

 **spd** 7 months, 1 week ago

Selected Answer: C

C - Storage Lens
upvoted 2 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 11 times

 **masetromain** 8 months, 2 weeks 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 3 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: C

C no doubt

upvoted 2 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: C

keywords = AWS Organizations && AWS CloudFormation StackSets.

upvoted 1 times

 **rbm2023** 4 months, 2 weeks 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** 6 months ago

Selected Answer: C

Use AWS Organizations and AWS CloudFormation StackSets

upvoted 2 times

 **zozza2023** 7 months, 4 weeks 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.

 **masetromain** Highly Voted  8 months, 2 weeks ago

same question of "Questions #84"

upvoted 9 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: C

C. a dup question

upvoted 1 times

 **rbm2023** 4 months, 2 weeks 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** 4 months, 3 weeks 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** 5 months, 3 weeks ago

Thought that my internet was interrupted. then i was wrong =)))

upvoted 3 times

 **Musk** 7 months, 3 weeks ago

This is repeated :-(

upvoted 2 times

 **tatdatpham** 7 months, 3 weeks ago

Selected Answer: C

Duplicate question with #84

upvoted 3 times

 **zhangyu20000** 8 months, 1 week 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 9 times

 **masetromain** 8 months, 2 weeks 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 3 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: B

probably B

upvoted 1 times

 **rbm2023** 4 months, 2 weeks 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** 6 months ago

Selected Answer: B

B. Specify AWS Elastic Beanstalk

upvoted 1 times

 **Untamables** 8 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 16 times

 **HussamShokr** 3 months, 1 week 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 2 times

 **masetromain** 8 months, 2 weeks 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 days, 21 hours ago

Security group is stateful. So you just need to set up inbound

upvoted 1 times

 **c73bf38** Highly Voted 7 months, 1 week 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 9 times

 **c73bf38** 7 months ago

B&C after doing a recreate in the AWS Console, stand corrected.

upvoted 3 times

 **c73bf38** 7 months 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 1 times

 **uC6rW1aB** Most Recent 3 weeks 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 1 times

 **uC6rW1aB** 3 weeks 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

 **vjp_training** 1 month ago

Selected Answer: AC

By default, all outbound rules are allowed

upvoted 1 times

 **vn_thanh tung** 3 weeks, 4 days ago

Don't provide wrong answer. Answer is B,C

upvoted 1 times

 **vn_thanh tung** 3 weeks, 4 days 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** 2 months, 3 weeks ago

Selected Answer: BC

BC of course

upvoted 2 times

 **bcx** 3 months, 1 week 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** 3 months, 3 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** 5 months 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** 6 months ago

Selected Answer: BC

BC gets my vote

upvoted 2 times

 **zejou1** 6 months, 1 week 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** 7 months 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

✉ **zejou1** 6 months, 1 week 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

✉ **Sarutobi** 6 months, 4 weeks 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

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

Selected Answer: BC

Flow connection: EC2 -> DB

So you need to configure Outbound EC2 and Inbound DB

upvoted 4 times

✉ **zozza2023** 7 months, 4 weeks ago

Selected Answer: BC

seems logic

outbound EC2 and inbound to DB

upvoted 2 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 19 times

 **masetromain** 8 months, 2 weeks 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

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: B

B for sure

upvoted 1 times

 **Maria2023** 3 months, 1 week 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** 1 month, 2 weeks ago

Billing > Budgets > Create budget > Customize (advanced) > Budget scope > Filter specific AWS cost dimensions

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

keyword = AWS Budgets in the organization's management
other more overhead each by account

upvoted 1 times

✉  **yama234** 5 months, 1 week 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 2 times

✉  **mfsec** 6 months ago

Selected Answer: B

B. Configure AWS Budgets in the organization's management account

upvoted 1 times

Question #89

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.

 **zejou1** Highly Voted  6 months, 1 week 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 9 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: A

A, basic `DeletionPolicy` use case

upvoted 1 times

 **aviathor** 3 weeks, 4 days ago

Yes but should be supplemented with deletion protection on the database.

upvoted 1 times

 **Maria2023** 3 months, 1 week 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 1 times

 **zak340** 3 months, 3 weeks 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 1 times

 **btx** 3 months, 1 week 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 1 times

 **rbm2023** 4 months, 2 weeks 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 2 times

 **rbm2023** 4 months, 2 weeks 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** 5 months, 1 week 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** 5 months, 1 week 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** 6 months ago

Selected Answer: A

A for sure

upvoted 2 times

 **kiran15789** 6 months, 3 weeks 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** 6 months, 3 weeks 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** 7 months, 1 week ago

Selected Answer: A

Clear A

upvoted 1 times

 **lunt** 7 months, 1 week 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 7 months, 2 weeks ago

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/protect-stack-resources.html>

upvoted 1 times

AC1984 7 months, 2 weeks 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 6 months, 3 weeks 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 7 months, 2 weeks 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 7 months, 4 weeks ago

Selected Answer: A

Option A

upvoted 1 times

masssa 8 months ago

Selected Answer: A

"`DeletionPolicy`" : "Retain" can prevent to delete resource

upvoted 4 times

masetromain 8 months, 1 week ago

Selected Answer: A

I switch to A:

<https://www.examtopics.com/discussions/amazon/view/5233-exam-aws-certified-solutions-architect-professional-topic-1/>

Modifying the CloudFormation templates to add a `DeletionPolicy` attribute to RDS and EBS resources, is another valid solution to prevent accidental deletion of data in this scenario. By adding a `DeletionPolicy` attribute of "Retain" to RDS and EBS resources in the CloudFormation templates, the company can ensure that these resources and their data are not deleted when the CloudFormation stack is deleted. This is a way to prevent accidental deletion of data by preserving the resources when the stack is deleted.

upvoted 3 times

masetromain 8 months, 1 week ago

Option B, Configuring a stack policy that disallows the deletion of RDS and EBS resources, would also prevent accidental deletion of data by RDS and EBS resources, but it does so by controlling access to the resources rather than preserving the resources as Option A does. Stack policies are a way to set up fine-grained access controls for the CloudFormation stack, so it would prevent users who are not authorized to delete RDS and EBS resources from doing so.

Option C, Modifying IAM policies to deny deleting RDS and EBS resources that are tagged with an "aws:cloudformation:stack-name" tag, is not a good solution because it only controls who can delete the resources, not whether they are deleted or retained when the stack is deleted.

Option D, Using AWS Config rules to prevent deleting RDS and EBS resources, is also not a good solution because AWS Config only records and monitors the configuration changes, it does not prevent any action on the resources.

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.

 **vsk12** Highly Voted 8 months ago

I would go with option B. Source will be public IP like 198.51.100.2.

upvoted 15 times

 **kiran15789** Highly Voted 6 months, 3 weeks 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 11 times

 **zejou1** 6 months, 1 week ago

For those that are choosing D - this is why D is incorrect and needs to be B

upvoted 2 times

 **AMohanty** Most Recent 2 weeks, 2 days 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** 1 month, 3 weeks 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

 **ggrodskiy** 1 month, 3 weeks 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** 2 months, 2 weeks ago

Selected Answer: B

bbbbbbbbbbb

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks 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** 2 months, 3 weeks 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 3 times

 **Maria2023** 3 months 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 2 times

 **SkyZeroZx** 3 months, 2 weeks ago

Selected Answer: B

we wanna check if its unsolicited traffic or not, so we gotta check if its a response for a outbound connection we made

upvoted 1 times

 **ZK000001qws** 3 months, 3 weeks ago

Selected Answer: B

The ask is "A solutions architect must determine whether the traffic represents unsolicited inbound connections from the internet".
inbound connections from the internet - if we are to check the inbound connection, wouldn't the source be internet IP and destination be VPC?
Thus I choose B too.

If it was outbound, initiated from VPC then it would make sense for D.

upvoted 3 times

 **johnballs221** 3 months, 4 weeks ago

Selected Answer: D

we wanna check if its unsolicited traffic or not, so we gotta check if its a response for a outbound connection we made

upvoted 1 times

 **andreitugui** 4 months ago

Selected Answer: B

So simple, CloudWatch logs to filter them(exclude aws cloudtrail), you need to check Inbound traffic to the vpc DESTINATION cidr 203.0 from SOURCE public ip 198.50.

upvoted 1 times

 **rbm2023** 4 months, 2 weeks ago

Selected Answer: B

This article

<https://repost.aws/knowledge-center/vpc-analyze-inbound-traffic-nat-gateway>

Talks about two reasons why a NAT Gateway would show inbound traffic from Public IP address to a private instance.

Reason 1 - Inbound internet traffic is permitted by your security group or network access control lists (ACL) - Check if the traffic is UNSOLICITED.

Run query:

filter (dstAddr like 'xxx.xxx' and srcAddr like 'public IP') | stats sum(bytes) as bytesTransferred by srcAddr, dstAddr | limit 10

upvoted 1 times

 **rbm2023** 4 months, 2 weeks ago

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.

Reason 2 - Traffic to the public IP was initiated from a private instance.

The question DOES NOT state which reason it would be except for the UNSOLICITED word in question.

I am choosing B for this one.

upvoted 1 times

 **Maria2023** 5 months ago

Selected Answer: D

Initially I went for B but when I saw the answer and read the documentation I am going for D due to the word "unsolicited" traffic. That for me means that we need to check if it's a return traffic, requested by a machine in the VPC. So we check whether any instance called that IP. B would more be for the associate exam

upvoted 5 times

 **Wobs1** 2 months, 3 weeks ago

It's the other way around. The traffic would be solicited if it was initiated from the EC2 instance.

upvoted 1 times

 **johnballs221** 3 months, 4 weeks ago

My thoughts exactly

upvoted 1 times

 **Sarutobi** 5 months, 1 week ago

Is this question even correct? It is possible, but what is the point of using a NAT-GW if the two IP addresses are public? Another issue is if you are initiating the traffic from the Internet, you cannot reach an EC2 instance behind a NAT-GW, because that instance has a private address. In other words, traffic is always Ec2->NAT-GW->Internet. Under normal circumstances, traffic through the NAT-GW always has a source address Private and a destination address Public. Obviously, the reply to this packet flips the source and destination.

upvoted 1 times

 **vandergun** 5 months, 3 weeks ago

Selected Answer: D

I vote for D

upvoted 1 times

 **Jay_2pt0_1** 5 months, 2 weeks ago

I'm curious as to why. Wouldn't the source be the public IP (that we want to research) and the destination our VPC?

upvoted 1 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.

 **testingaws123** Highly Voted  6 months, 2 weeks ago

Selected Answer: A

Answer is A

Keyword is "The S3 buckets have millions of objects"

If there are millions of objects then you should use Batch operations.

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

upvoted 12 times

 **forceli** 6 months, 1 week ago

good point, changing my answer to A

upvoted 1 times

 **deivid83** Most Recent  1 week, 5 days 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 1 times

 **uC6rW1aB** 3 weeks ago

Selected Answer: A

S3 Batch operation is the MOST operationally efficient way for millions of objects

upvoted 1 times

 **sachstarinfoaws** 2 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A more efficient

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: A

I vote for A. Batch operations are better for such a high number of objects

upvoted 1 times

 **rbm2023** 4 months, 2 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

The launch of S3 default encryption feature automates 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** 6 months ago

Selected Answer: A

A is much more efficient

upvoted 1 times

✉ **forceli** 6 months, 2 weeks 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** 6 months, 3 weeks 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** 6 months, 4 weeks 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

✉ **c73bf38** 7 months, 1 week ago

Encrypting existing objects

To encrypt your existing 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. For more information, see Performing large-scale batch operations on Amazon S3 objects and the AWS Storage Blog post Encrypting objects with Amazon S3 Batch Operations.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html?icmpid=docs_s3_hp_create_bucket_default_encryption

upvoted 3 times

✉ **mmendoza** 7 months, 3 weeks ago

Selected Answer: A

To encrypt you need to Re-copy the file and batch is more efficient.

upvoted 2 times

✉ **Musk** 7 months, 3 weeks ago

Selected Answer: A

As per Romidan's link, it is clear.

upvoted 1 times

✉ **mikeshop** 7 months, 4 weeks ago

Selected Answer: A

Batch operations are more efficient for millions of objects than running the CLI command.

upvoted 2 times

✉ **romidan** 8 months ago

Selected Answer: A

Option A seems efficient as per the blog -

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

upvoted 3 times

✉ **vsk12** 8 months ago

Option A is correct since manual copying (Option C) for millions of objects is time-consuming.

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.

 **masetromain** Highly Voted 8 months, 1 week 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 10 times

 **masetromain** 8 months, 1 week 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 5 times

 **uC6rW1aB** Most Recent 2 weeks, 6 days 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 1 times

 **chico2023** 1 month, 2 weeks 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 1 times

 **chico2023** 1 month, 2 weeks 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 1 times

 **chico2023** 1 month, 2 weeks 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 1 times

 **chico2023** 1 month, 2 weeks 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 1 times

 **Jonalb** 2 months, 2 weeks ago

Selected Answer: C

its a C , true question!

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

C for sure

upvoted 1 times

 **johnballs221** 3 months, 4 weeks ago

Selected Answer: B

redshift spectrum can run sql queries directly on s3

upvoted 1 times

 **rxhan** 2 months, 4 weeks ago

Not the best for cost.

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

C is the best choice for unstructured data

upvoted 3 times

 **God_Is_Love** 6 months, 3 weeks 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** 6 months, 3 weeks 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 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

AWS Glue Data Catalog to convert data to be structured before querying them

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.

upvoted 3 times

 **Untamables** 8 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 4 times

 **zhangyu20000** 8 months, 1 week ago

C is correct because it is unstructured data. You cannot use S3 select and must use Glue Crawler to generate catalog.

upvoted 2 times

 **masetromain** 8 months, 2 weeks ago

Selected Answer: A

A is the correct answer. S3 Select allows you to query the data stored in an S3 bucket, which can be useful when you need to retrieve specific subsets of data from a large amount of data. By creating an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive, you can save cost as it is a low-cost storage class for archival data that is infrequently accessed and for which retrieval times of several hours are acceptable. This solution is most cost-effective as it allows you to keep all the data indefinitely for compliance reasons while also reducing storage costs for older data that is not frequently accessed.

The other options are not as cost-effective as they would require additional costs for data transfer, storage and query in other services.

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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 5 times

 **masetromain** 8 months, 2 weeks 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 1 times

 **xplusfb** Most Recent  1 month, 2 weeks ago

Selected Answer: A

as we know snowball storage optimized NVMe up to 210 TB <3 A is the best and easy answer

upvoted 2 times

 **xplusfb** 1 month, 2 weeks ago

like several sorry for any confision :)

upvoted 1 times

 **chikorita** 3 weeks, 4 days ago

several thanks too :)

upvoted 1 times

 **NikkDicky** 2 months, 3 weeks ago

Selected Answer: A

A - basic snowball use case

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: A

Given the deadline (3 weeks) and the amount of data I would use Snowball Edge

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

A obviously
upvoted 3 times

 **God_Is_Love** 6 months, 3 weeks 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** 7 months, 4 weeks 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.

 **masetromain**  8 months, 2 weeks 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 9 times

 **masetromain** 8 months, 2 weeks 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

 **NikkyDicky**  2 months, 3 weeks ago

Selected Answer: D

D - basic use case for textract

upvoted 1 times

 **Maria2023** 3 months 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** 3 months, 2 weeks ago

Selected Answer: D

D : Managed AWS Services
upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: D
Amazon Textract..
upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks 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** 6 months, 3 weeks 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.

 **masetromain** Highly Voted  8 months, 2 weeks 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 11 times

 **masetromain** 8 months, 2 weeks 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 2 times

 **sambb** 6 months, 3 weeks 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 4 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: A

A no doubt

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

A is the best choice.

upvoted 1 times

 **Musk** 7 months, 1 week 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** 7 months 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

 **masetromain** Highly Voted 8 months, 2 weeks 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 6 times

 **masetromain** 8 months, 2 weeks 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

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: A

A - need data key for client-side encr

upvoted 1 times

 **Jesuisleon** 4 months, 1 week 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 3 times

✉ **venvig** 4 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 1 times

✉ **venvig** 4 weeks ago

Of course the answer is A

upvoted 1 times

✉ **btx** 3 months, 1 week ago

Indeed, the question says client side encryption but the answer is all about S3-KMS.

upvoted 1 times

✉ **mfsec** 6 months ago

Selected Answer: A

A for sure

upvoted 1 times

✉ **Untamables** 8 months ago

Selected Answer: A

<https://docs.aws.amazon.com/kms/latest/cryptographic-details/client-side-encryption.html>

upvoted 2 times

✉ **massa** 8 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.

 **God_Is_Love** Highly Voted 6 months, 3 weeks 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 13 times

 **Explorer_30** Most Recent 1 month, 1 week ago

vote A

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

Its an A

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

A. Set the action of the web ACL rules to Count. Enable AWS WAF logging.

upvoted 1 times

 **Untamables** 8 months ago

Selected Answer: A

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing.html>

upvoted 1 times

 **masetromain** 8 months, 2 weeks 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 4 times

 **masetromain** 8 months, 2 weeks 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

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.

 **masetromain** Highly Voted  8 months, 1 week 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 6 times

 **masetromain** 8 months, 1 week 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** Most Recent  2 weeks, 3 days ago

masetromain is ChatGPT and might have outdated answers since it doesn't know AWS latest update to services

upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C - basic RAM use case

upvoted 1 times

 **bcx** 3 months, 1 week 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** 3 months, 1 week ago

Selected Answer: C

KEYWORD = AWS Resource Access Manager

Then C

upvoted 1 times

 **johnballs221** 3 months, 4 weeks ago

Selected Answer: D

operational overhead

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

Prefix lists + RAM

upvoted 2 times

 **God_Is_Love** 6 months, 3 weeks ago

Prefix lists + Resource Access Manager RAM is the solution.

upvoted 4 times

 **Musk** 7 months, 3 weeks ago

Selected Answer: C

Clearly

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

Create a new customer-managed prefix list in the security team's AWS account

upvoted 1 times

 **Untamables** 8 months ago

Selected Answer: C

<https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html>

upvoted 3 times

 **zhangyu20000** 8 months, 1 week 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** 8 months, 2 weeks 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** 8 months, 2 weeks 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** 6 months, 3 weeks ago

Create an IAM role in each account in the organization. this does not add up to operational overhead right.

upvoted 1 times

 **BabaP** 3 months, 3 weeks 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.

 **masetromain** Highly Voted 8 months, 2 weeks 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 9 times

 **hexie** Highly Voted 2 months, 3 weeks 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 5 times

 **vn_thanh tung** 3 weeks, 4 days 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 1 times

 **bur4an** Most Recent 2 weeks, 3 days ago

masetromain voting is ruining the genuine most voted answers :(

upvoted 3 times

 **uC6rW1aB** 2 weeks, 6 days ago

Selected Answer: C

Ref: [#limitation](https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-basics.html)

Option B (just create a Client VPN endpoint in the main AWS account and set up routing via VPC peering) really won't meet the needs.

The transitive peering restriction states that traffic between VPC B and VPC C cannot be routed through VPC A, even if there are VPC peering connections between VPC A and VPC B, and between VPC A and VPC C. In other words, if employees connect to the VPC of the master AWS account through Client VPN, they will not be able to access other VPCs connected to that master VPC through VPC peering.

upvoted 2 times

 **aviathor** 2 months ago

Selected Answer: C

Although B might work, it is not scalable. It is limited to 50 VPCs, or maybe 125 if you increase the quota.

So the better option is C

<https://aws.amazon.com/blogs/networking-and-content-delivery/using-aws-client-vpn-to-scale-your-work-from-home-capacity/>

upvoted 1 times

✉ **dkx** 2 months, 1 week ago

Let's start by realizing they want a SCALABLE solution, so let's assume 1000 customers:

- A. No, because one Client VPN per account will obviously be expensive
- B. No, because the maximum active VPC peering connections per VPC is 125, thus not SCALABLE
- C. Yes, because Transit Gateway enables customers to connect thousands of VPCs
- D. No, because this is just bad

<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-connection-quotas.html>

upvoted 2 times

✉ **santi1975** 2 months ago

About your explanation in B. No, sorry, the answer says "Create a Client VPN endpoint in the main AWS account", then we should be worried by Concurrent client connections per Client VPN endpoint. Their maximum - even in the lowest scenario - is 7,000. Please check: <https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/limits.html>

I think that the answer is B

upvoted 2 times

✉ **azizmo** 2 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html>

upvoted 2 times

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

Selected Answer: B

B. since VPCs are already peered o need for TGW

upvoted 3 times

✉ **chikorita** 1 month ago

i missed this part, answer is B
without peering, answer is C

upvoted 1 times

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

Selected Answer: C

It's C. Use case : <https://aws.amazon.com/blogs/networking-and-content-delivery/using-aws-client-vpn-to-scale-your-work-from-home-capacity/>

upvoted 2 times

✉ **rbm2023** 4 months, 2 weeks ago

Selected Answer: B

In terms of cost effectiveness first there is a cost for VPN endpoints, so the cheapest option is to create the Client VPN Endpoint in the main account which leaves between options B and C. Since there is a cost for provisioning a Transit Gateway which is highlighted by option C, hence the answer should be B.

upvoted 1 times

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

Answer is C. VPC Peering does not allow transit connections.

upvoted 3 times

✉ **lxrdm** 2 months, 3 weeks ago

When using AWS Client VPN, your are essentially NATing your packets via the VPC.. your client machine is actually egressing from a VPC ENI which VPN client is using.. therefore its like your machine is actually inside the VPC and since all VPC's are peered in this case, b updating the route is enoug

upvoted 1 times

✉ **Sarutobi** 4 months, 2 weeks ago

Exactly right.

upvoted 1 times

✉ **Sarutobi** 4 months, 2 weeks ago

Exactly right, and that is when the source and destination IP addresses are not in the VPC, but in this case when you VPN into one VPC, you get an IP address of that VPC, so technically there is not "transit peering" here.

upvoted 2 times

✉ **mfsec** 6 months ago

Selected Answer: B

B is the answer

upvoted 1 times

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

Selected Answer: B

<https://docs.aws.amazon.com/images/vpn/latest/clientvpn-admin/images/client-vpn-scenario-peer-vpc.png>

upvoted 2 times

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

Tip - If there is no site-site gateway already and question asks for scalable solution then answer would be C

upvoted 3 times

✉ **Zek** 6 months, 3 weeks ago

Support B

upvoted 1 times

✉ **Musk** 7 months, 3 weeks ago

Selected Answer: B

It's B as explained here: <https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html>

upvoted 2 times

✉ **zozza2023** 7 months, 4 weeks ago

Selected Answer: B

should be B

upvoted 1 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.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A no brainer

upvoted 1 times

 **rbm2023** 4 months, 2 weeks 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 1 times

 **hpipit** 5 months, 4 weeks ago

Selected Answer: A

A : SQS QUEUE

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

SQS for decoupling

upvoted 1 times

 **c73bf38** 7 months ago

Selected Answer: A

SQS ---> Lambda is the correct option

upvoted 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: A

decouple ==> SQS

upvoted 1 times

 **Untamables** 8 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** 8 months ago

I vote for C - use Step Functions with its callback feature to throttle the third party api call.

upvoted 1 times

 **masetromain** 8 months, 2 weeks 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 3 times

 **masetromain** 8 months, 2 weeks 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

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.

 **masetromain** Highly Voted 8 months, 1 week 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 13 times

 **masetromain** 8 months, 1 week 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 3 times

 **masetromain** 8 months, 1 week 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

 **rsn** Most Recent 2 weeks, 2 days 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 1 times

 **uC6rW1aB** 2 weeks, 5 days 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** 1 month, 1 week ago

Selected Answer: D

D for sure

upvoted 1 times

 **Hyperdanny** 2 months, 1 week 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 2 times

 **rsn** 2 weeks, 2 days ago

I agree

upvoted 1 times

 **chikorita** 3 weeks, 3 days 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 2 times

 **NikkyDicky** 2 months, 3 weeks 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 2 times

 **Maria2023** 3 months 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 4 times

 **Jesuisleon** 4 months, 1 week 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

 **RaghavendraPrakash** 4 months, 3 weeks ago

C. Company needs to implement solution, not marketing team.

upvoted 2 times

 **passthatexam1** 5 months, 2 weeks ago

Least operational overhead - C -

upvoted 2 times

 **yama234** 5 months, 3 weeks ago

D

<https://repost.aws/knowledge-center/quicksight-cross-account-s3>

upvoted 3 times

 **mfsec** 6 months ago

Selected Answer: D

Since the S3 bucket belongs to the sales account, the marketing team cannot directly update the policy on the sales team's S3 bucket. In that case, option D would be the better option.

upvoted 1 times

 **zejou1** 6 months, 1 week ago

Selected Answer: C

LEAST operational overhead, you could do D and it would work, but honestly it is three steps w/ C.

upvoted 3 times

 **sambb** 6 months, 3 weeks ago

I just found the official documentation about cross-account s3 access by Quicksight : <https://aws.amazon.com/premiumsupport/knowledge-center/quicksight-cross-account-s3/>

Hence, the answer is C. No IAM role required because Quicksight uses a service role instead of a service-linked role.

upvoted 3 times

 **God_Is_Love** 6 months, 3 weeks ago

Selected Answer: D

Same as source bucket to destination bucket copy question in different form. first source should share its data. have a role created for destination bucket and that role will be assumed by dest bucket to get access to data. D is answer. C sounds wrong "Create KMS grant for encryption key" sounds weird.

upvoted 2 times

 **spd** 7 months, 1 week ago

Selected Answer: D

D is the answer but it does have enough information about KMS

upvoted 3 times

 **frfavoredo** 3 weeks, 4 days ago

Exactly. 'D' is correct but incomplete. You can't access KMS-key encrypted S3 objects without access to the key in order to decrypt them.

upvoted 1 times

 **Sarutobi** 6 months, 4 weeks ago

That is also my point; the other one, which is C, then is missing the S3 bucket permission in the sales account to provide access from the marketing account.

upvoted 1 times

 **Musk** 7 months, 3 weeks ago

Selected Answer: D

The rest of options have errors.

upvoted 1 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.

 **SK_Tyagi** 1 month, 1 week ago

Selected Answer: C

My 2 cents, Heterogeneous database migration and SCT go with each other

upvoted 1 times

 **xplusfb** 1 month, 2 weeks 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 3 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C of course

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: C

keyword = AWS Schema Conversion Tool

upvoted 1 times

 **rbm2023** 4 months, 2 weeks 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** 6 months ago

Selected Answer: C

Use the AWS Schema Conversion Tool

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks ago

Selected Answer: C

For heterogenous DBs, SCT is apt.

upvoted 1 times

 **Appon** 7 months, 3 weeks ago

Selected Answer: C

<https://aws.amazon.com/blogs/database/migrating-a-sql-server-database-to-a-mysql-compatible-database-engine/>

upvoted 1 times

 **Musk** 7 months, 3 weeks ago

Selected Answer: C

heterogenous -> frmo onee DB engine to another

upvoted 2 times

 **MasterP007** 7 months, 3 weeks ago

Straightforward - C

upvoted 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

C is the answer

upvoted 3 times

 **masetromain** 8 months, 2 weeks 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** 8 months, 2 weeks 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.

 **masetromain** Highly Voted 8 months, 1 week 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 7 times

 **masetromain** 8 months, 1 week 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 3 times

 **masetromain** 8 months, 1 week 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** Highly Voted 6 months, 1 week 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 5 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: ACE

ACE in this case

upvoted 1 times

 **MoussaNoussa** 3 months, 1 week ago

ACE is the correct choice of course

upvoted 1 times

 **leehjworking** 4 months, 1 week ago

Selected Answer: ACE

Vote for ACE

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: ACE

ACE is the best choice

upvoted 3 times

 **God_Is_Love** 6 months, 3 weeks 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 1 times

 **Musk** 7 months, 3 weeks ago

Selected Answer: ACE

I think it's clear

upvoted 1 times

 **tatdatpham** 7 months, 3 weeks ago

Selected Answer: ACE

ACE is correct answer

upvoted 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: ACE

ACE should works

upvoted 2 times

 **zhangyu20000** 8 months, 1 week ago

ACE is my answer

upvoted 2 times

 **masetromain** 8 months, 1 week 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** 8 months, 1 week 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.

 **Untamables** Highly Voted  8 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 10 times

 **CuteRunRun** Most Recent  1 month, 2 weeks ago

Selected Answer: C

I prefer C

upvoted 1 times

 **Spaco** 2 months 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** 2 months, 3 weeks ago

Selected Answer: C

its a C

upvoted 1 times

 **leehjworking** 4 months, 1 week ago

Anybody know why we should select all AZs?

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: C

Modify the existing environment's capacity configuration to use a load-balanced environment type.

upvoted 1 times

 **zejou1** 6 months, 1 week 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** 6 months, 3 weeks 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 1 times

 **spd** 7 months, 1 week ago

Selected Answer: C<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>

upvoted 2 times

 Musk 7 months, 3 weeks 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 8 months ago

A: Elastic Beanstalk environment can not be changed.

upvoted 2 times

 mikeshop 7 months, 4 weeks ago<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>

Yes they can.

upvoted 2 times

 romidan 8 months, 1 week 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

 masetromain 8 months, 1 week ago**Selected Answer: A**

The correct answer is 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.

This solution will create a new load-balanced environment which will increase the scalability and availability of the application, which will help mitigate the performance issues. Additionally, by adding a scale-out rule that triggers when the CPU utilization is high, the application will automatically scale to handle increased traffic, which will help alleviate the performance bottlenecks.

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 in the average CPU utilization is over 85% for 5 minutes.

This option is not correct because it only directs some traffic to the new environment but it does not scale out the instances.

upvoted 2 times

 masetromain 8 months, 1 week ago

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.

This option is not correct because you can't change the existing environment.

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.

This option is not correct because it rebuilds the environment but it does not scale out the instances.

In summary, option A is the correct answer because it creates a new load-balanced environment, which increases scalability and availability, and it also includes a scale-out rule that triggers when CPU utilization is high, which automatically scales the instances to handle increased traffic, thus alleviating performance bottlenecks.

upvoted 1 times

 hobokabobo 6 months, 2 weeks ago

"you can't change the existing environment.": since when?

2 years ago it was possible and I firmly believe AWS didn't change that without updating the documentation

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/GettingStarted.EditConfig.html>

upvoted 2 times

 BabaP 3 months, 3 weeks ago

lol... it is chatgpt typing

upvoted 1 times

 zhangyu20000 8 months, 1 week ago

A: You cannot change environment

upvoted 2 times

 keenian 8 months ago

Yes, you can. Try on your AWS account. The correct answer is C.

upvoted 4 times

 masetromain 8 months, 1 week ago**Selected Answer: C**

The correct answer is C. This solution will meet the requirements with the least operational overhead because it modifies the existing environment's capacity configuration to use a load-balanced environment type and selects all availability zones. This will allow the application to scale out automatically if the average CPU utilization is over 85% for 5 minutes. This will help alleviate the performance issues without the need to create a new environment or rebuild the existing one.

upvoted 4 times

 **masetromain** 8 months, 1 week ago

Option A, creating a new Elastic Beanstalk application, would require more operational overhead as it would involve creating a new environment and configuring it with a load-balanced environment type and selecting all availability zones.

Option B, creating a second Elastic Beanstalk environment and applying a traffic-splitting deployment policy, would also require more operational overhead as it would involve creating a new environment and configuring it to handle some of the incoming traffic.

Option D, selecting the Rebuild environment action with the load balancing option, would also require more operational overhead as it would involve rebuilding the existing environment and configuring it with a load-balanced environment type.

upvoted 1 times

 **masetromain** 8 months, 1 week ago

To modify the existing environment's capacity in Elastic Beanstalk, you can use the Elastic Beanstalk management console or the AWS Elastic Beanstalk API.

To do this using the management console:

- 1 - Open the Elastic Beanstalk management console.
- 2 - Select the application and environment that you want to modify.
- 3 - In the navigation pane, choose Configuration.
- 4 - In the Capacity configuration section, you can modify the number of instances in your environment and configure automatic scaling settings.

To do this using the AWS Elastic Beanstalk API, you can use the UpdateEnvironment API action. The UpdateEnvironment action allows you to change the number of instances in your environment, as well as other settings like the environment name and description.

upvoted 2 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.

 **masetromain** Highly Voted  8 months, 1 week 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 11 times

 **uC6rW1aB** Most Recent  2 weeks, 5 days 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** 3 weeks, 4 days 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** 1 month, 2 weeks ago

Selected Answer: B

all other sections not applicable i guess specially D its so funny. Each month none of technical person doesn't want to do like this task.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B of course

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

it slows down during the final three days of each month due to month-end reporting
then

high read in database == solution add read replicas

B

upvoted 2 times

 **nexus2020** 2 months, 3 weeks ago

month end reporting is to submit the financial data, aka write the new data to DB

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B

Performing a one-time migration

upvoted 1 times

 **zozza2023** 7 months, 4 weeks 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.

 **masetromain** Highly Voted 8 months, 1 week 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 11 times

 **masetromain** 8 months, 1 week 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 3 times

 **rbm2023** 4 months, 2 weeks 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

 **Musk** 7 months, 3 weeks ago

B does not say anything about Lambda. Where have you read that?

upvoted 1 times

 **Musk** 7 months, 3 weeks ago

You are right, I mixed A with B

upvoted 1 times

 **zejou1** Highly Voted 6 months, 1 week 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 5 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: A

it's an A

upvoted 1 times

 **Maria2023** 3 months 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** 5 months 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** 6 months 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** 6 months, 3 weeks ago

Selected Answer: A

least code changes

upvoted 2 times

 **keonlee** 7 months, 1 week ago

Selected Answer: A

Fargate, Modernize stack

upvoted 2 times

 **spd** 7 months, 1 week ago

Selected Answer: A

Least code changes

upvoted 2 times

 **moota** 7 months, 2 weeks ago

Selected Answer: A

A is much simpler with AWS Copilot. I also don't have to deal with Lambda's cold start time. You also need to do a little bit of coding to interact with Lambda's Runtime API that are part of Lambda's base images - <https://aws.amazon.com/blogs/aws/new-for-aws-lambda-container-image-support/>

upvoted 1 times

 **Musk** 7 months, 3 weeks ago

Selected Answer: B

B implies LEAST code changes.

upvoted 1 times

 **Musk** 7 months, 3 weeks ago

Sorry I meant A

upvoted 1 times

 **jojom19980** 7 months, 3 weeks ago

Selected Answer: B

B should be correct, why to use EKS, the question does not mention any details or complex design to use it so I will go with an easy and cost Solution

upvoted 2 times

 **hobokabobo** 6 months, 2 weeks ago

can't agree more, however A mentions how to migrate an app on an instance to container images. That seems to be an important step. B does not.

upvoted 1 times

 **hobokabobo** 6 months, 2 weeks ago

Also its an app not rest, that's more a job for a loadbalancer.

upvoted 1 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.

 **masetromain** Highly Voted 8 months, 1 week 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 16 times

 **masetromain** 8 months, 1 week 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

 **testingaws123** 6 months, 1 week ago

You always use ChatGPT to paste answers. Most of the time ChatGPT gives wrong answers do you know this?

upvoted 7 times

 **venvig** Most Recent 3 weeks, 4 days ago

Selected Answer: D

Refer <https://aws.amazon.com/blogs/architecture/implementing-multi-region-disaster-recovery-using-event-driven-architecture/>

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

clearly D

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: D

Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region

upvoted 1 times

 **zejou1** 6 months, 1 week 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** 6 months, 3 weeks 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** 7 months, 4 weeks ago

Selected Answer: D

The correct answer is D

upvoted 2 times

✉️  **zhangyu20000** 8 months, 1 week 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** 8 months, 1 week 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** 1 day, 15 hours 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

✉️  **CProgrammer** 1 day, 15 hours 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

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.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

surely C

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

C is the way to go

upvoted 1 times

 **kiran15789** 6 months, 3 weeks ago

Selected Answer: C

Management account --> Billing Dashboard --> Billing preferences, this option is there to choose enable/disable RI discounts sharing
upvoted 4 times

 **sambb** 6 months, 3 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

upvoted 3 times

 **God_Is_Love** 6 months, 3 weeks 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 2 times

 **testingaws123** 6 months, 3 weeks 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 2 times

 **SK_Tyagi** 1 month, 1 week 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

 **chikorita** 1 month, 1 week 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

✉️ **God_Is_Love** 6 months, 3 weeks 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 3 times

✉️ **jojom19980** 7 months, 3 weeks ago

Selected Answer: C

The correct answer is C

upvoted 1 times

✉️ **masetromain** 8 months, 1 week 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 2 times

✉️ **masetromain** 8 months, 1 week 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 1 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.

 **zozza2023**  7 months, 4 weeks ago

Selected Answer: D

The correct answer is D.

upvoted 8 times

 **venvig**  3 weeks, 4 days 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 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

d of course

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: D

keyword == Auto Scaling group's Terminate process.

upvoted 1 times

 **Alando** 1 week, 6 days ago

Have you cleared the exam?

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: D

Suspend the Auto Scaling group's Terminate process.

upvoted 2 times

 **zejou1** 6 months, 1 week 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 3 times

 **God_Is_Love** 6 months, 3 weeks ago

Selected Answer: D

Disabling health check won't let SA know which instance is unhealthy. So A is certainly wrong. D is correct.

upvoted 4 times

 **testingaws123** 6 months, 3 weeks 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** 6 months, 1 week 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 4 times

 **masetromain** 8 months, 1 week 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 4 times

 **masetromain** 8 months, 1 week 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 2 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.

 **masetromain** Highly Voted 8 months, 1 week 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 13 times

 **masetromain** 8 months, 1 week 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 2 times

 **Untamables** Highly Voted 8 months ago

Selected Answer: A

<https://aws.amazon.com/solutions/implementations/automations-for-aws-firewall-manager/>

upvoted 5 times

 **venvig** Most Recent 3 weeks, 4 days 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 1 times

✉  **CuteRunRun** 1 month, 1 week 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** 2 months, 3 weeks ago

Selected Answer: A

A is a good option

upvoted 1 times

✉  **SkyZeroZx** 3 months, 1 week ago

Selected Answer: A

keyword == AWS Firewall Manager

upvoted 1 times

✉  **tromyunpak** 3 months, 3 weeks ago

the correct answer is A <https://docs.aws.amazon.com/solutions/latest/automations-for-aws-firewall-manager/architecture-overview.html>

upvoted 1 times

✉  **rbm2023** 4 months, 2 weeks 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** 6 months ago

Selected Answer: A

Use AWS Firewall Manager to manage AWS WAF rules

upvoted 1 times

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

Selected Answer: A

Not D, KMS to store account numbers ?

upvoted 1 times

✉  **zozza2023** 7 months, 4 weeks 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.

 **zozza2023** Highly Voted  7 months, 4 weeks 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 12 times

 **task_7** Most Recent  2 days, 7 hours ago

Selected Answer: D

AWS Secrets Manager is meant for this job, why go with any other option

upvoted 1 times

 **task_7** 2 days, 7 hours ago

My bad it's A

D is not addressing this point

The data must not travel across the Internet

upvoted 1 times

 **CuteRunRun** 1 month, 1 week ago

I prefer A

upvoted 2 times

 **Jonalb** 2 months ago

Selected Answer: A

A

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

upvoted 1 times

 **Jonalb** 2 months, 3 weeks ago

Selected Answer: D

https://docs.aws.amazon.com/pt_br/secretsmanager/latest/userguide/vpc-endpoint-overview.html

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A for sure

upvoted 1 times

 **rbm2023** 4 months, 2 weeks 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** 4 months, 4 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** 4 months, 2 weeks 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** 5 months, 1 week 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** 6 months ago

Selected Answer: A

A for sure due to VPC endpoints.

upvoted 2 times

 **kiran15789** 6 months, 3 weeks 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** 6 months, 3 weeks 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

 **moota** 7 months, 2 weeks ago

Selected Answer: A

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
>Action": [
"rds-db:connect"
],
"Resource": [
"arn:aws:rds-db:<region>:<account-id>:dbuser:<DbiResourceId>/<db_user_name>"
]
}
]
}
```

upvoted 2 times

 **moota** 7 months, 2 weeks ago

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

upvoted 1 times

 **tinyflame** 7 months, 2 weeks ago

Selected Answer: D

Accessing S3 from Lambda does not use the internet. It's the foundation of AWS.

upvoted 2 times

 **tinyflame** 7 months, 2 weeks ago

postscript

All communication uses the AWS private network

upvoted 1 times

 **Untamables** 8 months ago

Selected Answer: A

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

upvoted 3 times

 **vsk12** 8 months ago

A: the critical point here - is "The data must not travel across the Internet". VPC endpoint for Amazon S3 help in this.

upvoted 1 times

 **masetromain** 8 months, 1 week ago

Selected Answer: A

You are correct. Option 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 is the best solution.

It is a combination of measures that work together to meet the requirements:

- IAM database authentication for the Aurora DB cluster allows for secure and centralized management of access to the database, and eliminates the need to store user credentials in the database.

- Deploying a gateway VPC endpoint for Amazon S3 ensures that data does not travel across the internet and is protected by VPC security. Changing the IAM role for the Lambda function allows it to access the database securely via IAM database authentication.

- By implementing the above steps, you can ensure that the data is protected in transit and at rest, and that the impact of a compromise of the database credentials is minimized.

upvoted 4 times

 **masetromain** 8 months, 1 week ago

Option 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. This option only covers the encryption of data in transit and doesn't address the security concerns of the data at rest.

Option 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.

This option addresses the security concern of rotating the credentials but doesn't cover the secure authentication to the database.

upvoted 2 times

 **masetromain** 8 months, 1 week ago

Option 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.

This option addresses the security concern of rotating the credentials but doesn't cover the secure authentication to the database and doesn't address the security concerns of the data at rest.

Option A is the best choice as it covers all the security concern in the question :

- secure authentication to the database
- encryption of data in transit
- protection of the data at rest.

It also provides centralised management of access to the database via IAM and protection of data while stored in S3 via a VPC endpoint.

upvoted 1 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.

 **masetromain** Highly Voted 8 months, 1 week 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 11 times

 **masetromain** 8 months, 1 week 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 6 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: C

Its a C

upvoted 1 times

 **Maria2023** 3 months 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 1 times

 **Parimal1983** 3 months ago

C is the correct solution remained. Typo mistake in the comments.

upvoted 1 times

 **easystoo** 3 months, 1 week ago

C-C-C-C-CC-C-C-CC-C-C-C-C-CC-

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

IAM policy..

upvoted 1 times

  **zozza2023** 7 months, 4 weeks 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.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: ABE

its ABE

upvoted 1 times

 **youngmanaws** 5 months 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 2 times

 **OCHT** 5 months, 3 weeks 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 1 times

 **OCHT** 5 months, 3 weeks 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 3 times

 **OCHT** 5 months, 3 weeks 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 3 times

 **mfsec** 6 months ago

Selected Answer: ABE

ABE is the better choice

upvoted 1 times

 **Damijo** 6 months, 1 week ago

what's the value of A and E together- it's either or ? the outcome is the same - thoughts?

upvoted 2 times

 **God_Is_Love** 6 months, 3 weeks 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 3 times

 **God_Is_Love** 6 months, 3 weeks 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 1 times

 **jaysparky** 7 months ago

ABE makes sense

upvoted 1 times

 **spd** 7 months, 2 weeks 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** 7 months, 3 weeks ago

Selected Answer: AE

BE makes sense

upvoted 1 times

 **zozza2023** 8 months ago

Selected Answer: ABE

the best way to deploy config rules accross accounts= SCP

upvoted 2 times

 **masssa** 8 months ago

Selected Answer: ABE

In adding tag, the keywords are config, scp, aggregagator.

upvoted 2 times

 **Untamables** 8 months ago

Selected Answer: ABE

A and E are correct. But the below is the best way to deploy config rules accross accounts.

<https://docs.aws.amazon.com/config/latest/developerguide/config-rule-multi-account-deployment.html>

<https://docs.aws.amazon.com/config/latest/developerguide/aggregate-data.html>

B is correct.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html

upvoted 2 times

 **ccort** 8 months ago

Selected Answer: ABE

ABE for me

D I am sure it is not, it would be too much trouble putting the policy in each account

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

BDE are correct

upvoted 1 times

 **masetromain** 8 months, 1 week ago

Selected Answer: BDE

The correct answer is BDE.

B: Creating an SCP (Service Control Policy) in the organization with a deny action for ec2:RunInstances if the Project tag is missing will prevent developers from launching instances without the necessary tag. This is a good option because it will prevent the problem from happening again in the future.

D: Creating an IAM policy in each account with a deny action for ec2:RunInstances if the Project tag is missing will also prevent developers from launching instances without the necessary tag. This is a good option because it will prevent the problem from happening again in the future.

E: Creating an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag will help the team identify which instances are missing the tag, so they can take action to add the tag. This is a good option because it will help resolve the problem that has already happened and also help the team identify any instances that are not compliant with the company's tagging policy.

upvoted 2 times

 **Arnaud92** 2 weeks, 2 days ago

stop asking to ChatGPT. The right answer is ABE. ChatGPT forgot to list the missing tags on the existing instances

upvoted 1 times

 **masetromain** 8 months, 1 week ago

The other options, A and C are not appropriate for this scenario, because they would only identify the instances that are missing the tag, but not prevent the problem from happening again. Using option F is also not appropriate for this scenario, because AWS Security Hub is not used for cost allocation.

upvoted 1 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.

 **God_Is_Love** Highly Voted 6 months, 3 weeks 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 9 times

 **OCHT** Highly Voted 5 months, 3 weeks 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 8 times

 **AMohanty** Most Recent 3 weeks 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 1 times

 **chikorita** 2 weeks 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** 2 months, 3 weeks ago

Selected Answer: AD

AD for unstructured data

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: AD

AD is my vote

upvoted 1 times

✉️ **Zek** 6 months, 3 weeks 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** 8 months, 1 week ago

AD are correct
upvoted 1 times

✉️ **masetromain** 8 months, 1 week 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 5 times

✉️ **masetromain** 8 months, 1 week 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 1 times

✉️ **Sarutobi** 6 months, 3 weeks 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 2 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.

 **God_Is_Love** Highly Voted 6 months, 3 weeks 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 7 times

 **NikkyDicky** Most Recent 2 months, 2 weeks ago

Selected Answer: D

It's a d

upvoted 1 times

 **Maria2023** 3 months 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 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: D

reduce cost == interface VPC endpoint

upvoted 2 times

 **SkyZeroZx** 3 months, 1 week ago

A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category.

upvoted 1 times

 **Anonymous9999** 5 months, 1 week 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** 4 months, 1 week 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** 6 months ago

Selected Answer: D

D is the best choice.

upvoted 1 times

 **Sarutobi** 6 months, 3 weeks 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** 7 months ago

Selected Answer: D

Allowing traffic from the application using the VPC endpoint is key to bypassing NAT Gateway.

upvoted 3 times

 **moota** 7 months, 2 weeks 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** 7 months, 3 weeks ago

Selected Answer: B

B seems correct too.

upvoted 3 times

 **zhangyu20000** 8 months, 1 week ago

D: by pass internet to save cost on NAT GW

upvoted 1 times

 **masetromain** 8 months, 1 week 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 2 times

 **masetromain** 8 months, 1 week 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 2 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.

 **God_Is_Love** Highly Voted  6 months, 3 weeks 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 9 times

 **God_Is_Love** 6 months, 3 weeks ago

Whichever option has this text is correct - "Peer the transit gateways with each other to support cross-Region routing"
 upvoted 3 times

 **frfavoredo** Most Recent  3 weeks 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 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

it's D

upvoted 1 times

 **happystrawberry** 4 months 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** 4 months ago

Actually, D is a proper answer.

upvoted 1 times

 **rbm2023** 4 months, 1 week 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** 4 months, 1 week 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** 5 months, 2 weeks 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** 6 months ago

Selected Answer: D

D is the answer

upvoted 2 times

 **zejou1** 6 months, 1 week 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** 6 months, 3 weeks 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** 7 months 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

 **spd** 7 months, 1 week ago

Selected Answer: D

D Seems Correct

upvoted 1 times

 **jojom19980** 7 months, 3 weeks ago

Selected Answer: D

D:

<https://aws.amazon.com/blogs/networking-and-content-delivery/aws-transit-gateway-now-supports-intra-region-peering/>

upvoted 1 times

 **Musk** 7 months, 3 weeks ago

Maybe you meant this one: <https://aws.amazon.com/blogs/aws/new-for-aws-transit-gateway-build-global-networks-and-centralize-monitoring-using-network-manager/>

upvoted 1 times

 **jojom19980** 7 months, 3 weeks ago

and this for connect two transit gateways with one direct connect gateway :

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html>

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: D

answer is D

upvoted 1 times

✉ **Untamables** 8 months ago

Selected Answer: C

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/virtualgateways.html>

https://docs.aws.amazon.com/directconnect/latest/UserGuide/high_resiliency.html

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html>

upvoted 1 times

✉ **zhangyu20000** 8 months, 1 week ago

D use DX GW for multi region to on-premise, direct TGW peer for cross regions

upvoted 1 times

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

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/91771-exam-aws-certified-solutions-architect-professional-topic-1/>

The correct answer is D.

In this solution, two transit VIFs are created - one from the DX-A connection and one from the DX-B connection - into the same Direct Connect gateway for high availability. Both the eu-west-1 and us-east-1 transit gateways are then associated with this Direct Connect gateway. The transit gateways are then peered with each other to support cross-Region routing.

This solution meets the requirements of the company by creating a highly available connection between the on-premises data center and the VPCs in both the eu-west-1 and us-east-1 regions, and by enabling direct traffic routing between VPCs in those regions.

upvoted 1 times

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

Option A is incorrect because a private VIF does not support inter-VPC traffic and cross-Region routing.

Option B is incorrect because it separates the two Direct Connect connections into separate Direct Connect gateways, which would not provide high availability.

Option C is incorrect because it does not mention how to peer the transit gateways to support cross-Region routing.

upvoted 1 times

✉ **Sarutobi** 6 months, 3 weeks ago

I think the reason why B is wrong is because there is no need to have 2 Direct Connect Gateways. DX-GW is a global object, separating the regions with 2 DX-GW only creates fragmentation of the routing, which can be good in some cases.

upvoted 1 times

✉ **youngmanaws** 5 months ago

Seems 1 DX-GW can connect to up to 3 Transit-GW, if you have more than 3 Transit-GW, you can use 2 DX-GW.

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.

 **God_Is_Love** Highly Voted  6 months, 3 weeks 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 9 times

 **Jay_2pt0_1** 4 months, 3 weeks ago

I agree with this.

upvoted 1 times

 **hobokabobo** 6 months, 2 weeks ago

this explanation makes sense to me.

upvoted 1 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: ADE

ADE. have to assume the step function calls lambda or some such to actually perform action

upvoted 1 times

 **Maria2023** 4 months, 1 week 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

 **OCHT** 5 months, 3 weeks 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 1 times

 **OCHT** 5 months, 3 weeks 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** 6 months ago

Selected Answer: ADE

ADE is right

upvoted 1 times

 **[Removed]** 7 months, 2 weeks ago

Selected Answer: ADE

ADE Step Functions works.

upvoted 1 times

 **Musk** 7 months, 3 weeks ago

Selected Answer: ACE

I like ACE better. I am not sure Step Functions would work.

upvoted 1 times

 **moota** 7 months, 2 weeks 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** 8 months, 1 week ago

ADE are correct

upvoted 1 times

 **masetromain** 8 months, 1 week 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** 6 months, 2 weeks 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** 4 months, 1 week ago

He just copied the answer from chatgpt for every question, really made me sick

upvoted 4 times

 **BabaP** 3 months, 3 weeks 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.

 **masetromain** Highly Voted 8 months, 1 week 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 9 times

 **masetromain** 8 months, 1 week 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** 8 months, 1 week 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

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: ACD

ACD easy

upvoted 1 times

 **Maria2023** 3 months 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 1 times

 **OCHT** 5 months, 3 weeks 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** 6 months ago

Selected Answer: ACD

ACD are the best choice

upvoted 1 times

 **spd** 7 months, 1 week ago

Selected Answer: ACD

By Elimination Rule

upvoted 2 times

 **zhangyu20000** 8 months, 1 week 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.

 **masetromain** Highly Voted 8 months, 1 week 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 6 times

 **Musk** Highly Voted 7 months, 3 weeks ago

Selected Answer: B

this is easy. I wish I'll have several of this in the exam.

upvoted 5 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: B

B for sure

upvoted 1 times

 **Maria2023** 3 months 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** 4 months, 1 week ago

Can anyone explain why B has less operational effort than A ?

upvoted 1 times

 **chikorita** 3 months, 3 weeks 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** 5 months, 2 weeks 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** 6 months ago

Selected Answer: B

B is the easy choice

upvoted 2 times

 **zhangyu20000** 8 months, 1 week ago

B is correct. Stop the instance that preserver all data.

C: is incorrect because it terminate instance that will loss data

upvoted 4 times

 **rbm2023** 4 months, 1 week ago

with the addition to the fact that to recreate those DBs from scratch would take a long time.

upvoted 1 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.

 **sambb** Highly Voted 6 months, 3 weeks 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 7 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: C

C of course

upvoted 1 times

 **dev112233xx** 5 months, 2 weeks 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** 6 months ago

Selected Answer: C

Company reached its limit

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

C is the answer

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

C is correct answer

upvoted 1 times

 **masetromain** 8 months, 1 week 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 3 times

 **masetromain** 8 months, 1 week 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 2 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.

 **OCHT** Highly Voted 5 months, 3 weeks 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 12 times

 **deegadaze1** 4 months ago

Correct for GLB---> https://www.youtube.com/watch?v=-j2smz_VCH4

upvoted 1 times

 **rbm2023** Highly Voted 4 months, 1 week 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 6 times

 **AMohanty** Most Recent 2 weeks, 6 days ago

AD

As the Service Consumers(Application) are provided in a different subnet but same VPC as the Service Providers(Security) we don't require a Transit gateway inbetween

upvoted 1 times

 **venvig** 3 weeks, 3 days ago

Selected Answer: AD

Gateway Load balancer is a combination of “Gateway” and “Load balancer”

GWLB are precisely used for this kind of use case: So option (D) is the first choice. (<https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/>)

Gateway Load Balancer helps you easily deploy, scale, and manage your third-party virtual appliances. It gives you one gateway for distributing traffic across multiple virtual appliances while scaling them up or down, based on demand

From the above AWS doc link,

Hitting the limit of what your virtual appliances can handle can bottleneck your entire network. To prevent this, Gateway Load Balancer automatically scales your virtual appliances up or down, based on demand.

This means that the Ec2 instances where the security tool are installed must scale

upvoted 2 times

Ganshank 1 month ago

The answer is BD.

B - Gateway Load balancer is a Layer 3 construct, and operates at the Network layer. So in order for it to redirect traffic to the web application, the web application must be hosted behind a NLB.

D - Gateway LB is a zonal construct, so it must be deployed in each availability zone.

upvoted 1 times

xav1er 1 month, 3 weeks ago

there is no need for Transit Gateway as GWLB uses endpoints and privatelink to process packet transportation between VPCs - as it is clearly stated here in this doc and on clear pic: <https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html>

so clearly B,C,E are bad answers. A and D left so it must be correct i suppose BUT i'm confused with D to be honest - why to create separate GWLB for each AZ? it can utilize Cross-zone load balancing so no need for that. Am i wrong ?

upvoted 1 times

khksoma 1 month, 3 weeks ago

Isn't the GWLB targeting the appliances available from AWS market place only? So, in that case how can D be right?

upvoted 1 times

MRL110 2 months ago

Selected Answer: DE

Only GLB option (D) mentions of a multi-AZ scenario which is one of the requirements.

"The EC2 instances will run in an Auto Scaling group in a dedicated VPC." So there's more than one VPC. This rules out option A. And this also means transit gateway is required for inter-VPC communication (E).

upvoted 2 times

MRL110 2 months ago

Selected Answer: DE

"The EC2 instances will run in an Auto Scaling group in a dedicated VPC."

This means there's definitely more than one VPC and transit gateway will be used for their communication.

upvoted 2 times

softarts 2 months, 1 week ago

AD

reason:

<https://www.examtopics.com/discussions/amazon/view/74155-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

BasselBuzz 2 months, 2 weeks ago

Selected Answer: AC

I would go with ALB. It shouldn't be more complicated than that.

upvoted 1 times

BasselBuzz 2 months, 2 weeks ago

Changed to AD. GLB is the case here.

upvoted 1 times

NikkyDicky 2 months, 3 weeks ago

Selected Answer: AD

its AD

upvoted 1 times

SmileyCloud 2 months, 3 weeks ago

Selected Answer: DE

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-gwlb-with-tg-for-cns.html>

upvoted 1 times

Maria2023 3 months ago

Selected Answer: AD

<https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html>

Here they say "e Gateway Load Balancer is deployed in the same VPC as that of the virtual appliances."

upvoted 1 times

khksoma 1 month, 4 weeks ago

That's correct. The point in contention is not the same VPC as the security appliances..Its a different VPC than the app servers. Per the guidelines, the GLB has to be in the same VPC as the Appliances, but a different subnet(so that it can be used as the next hop)

upvoted 1 times

easytoo 3 months, 1 week ago

a-b-a-b-a-b-a-b

upvoted 1 times

✉ **easytoo** 2 months ago

a-d-a-d-a-d-a-d

upvoted 1 times

✉ **Windows98** 3 months, 3 weeks ago

Selected Answer: AB

You can't use a GWLB because the traffic will be forwarded in GENEVE for the appliance to deal with.

<https://aws.amazon.com/blogs/networking-and-content-delivery/integrate-your-custom-logic-or-appliance-with-aws-gateway-load-balancer/>

What changes to the appliance must be made for them work with GWLB?

In order to work with GWLB, appliances need to:

Support Geneve protocol to exchange traffic with GWLB. Geneve encapsulation is required for transparent routing of packets between GWLB and appliances, and for sending extra information (aka metadata, explained below).

Support encoding/decoding GWLB related Geneve type-length-value (TLV) pairs.

Respond to TCP/HTTP/HTTPS health checks from GWLB.

And GWLB wants you to use a different VPC for the appliances.

upvoted 2 times

✉ **chathur** 3 months, 3 weeks ago

"the tool has no cloud solutions available from its vendor" Does not mean that you can not run it on an EC2. It says the solution is not provided as a cloud solution where you do not have to install and maintain.

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.

 **God_Is_Love** Highly Voted 6 months, 3 weeks 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 9 times

 **uC6rW1aB** Most Recent 2 weeks, 5 days 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** 2 months, 3 weeks ago

Selected Answer: A

A for sure

upvoted 1 times

 **Maria2023** 4 months, 1 week 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** 5 months, 2 weeks 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** 6 months ago

Selected Answer: A

Connect the IoT sensors to AWS IoT Core.

upvoted 2 times

✉ **spd** 7 months, 1 week ago

Selected Answer: A

A by Elimination rule

upvoted 3 times

✉ **Musk** 7 months, 3 weeks 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 3 times

✉ **Sarutobi** 5 months, 1 week 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** 7 months, 4 weeks ago

Selected Answer: A

i'll go for A

upvoted 4 times

✉ **masetromain** 8 months, 1 week 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** 8 months, 1 week 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** 7 months, 3 weeks 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

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.

 **masetromain** Highly Voted  8 months, 1 week 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 6 times

 **SK_Tyagi** Most Recent  1 month, 1 week ago

Selected Answer: BDF

Very logical
 upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: BDF

BDF for sure
 upvoted 1 times

 **Maria2023** 3 months 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** 4 months ago

Selected Answer: BDF

BDF is the right ans
 upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: BDF

BDF is the right combo
 upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks 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** 7 months, 4 weeks ago

Selected Answer: BDF

B D and F

upvoted 4 times

 **zozza2023** 7 months, 4 weeks ago

I agree with BD&F

upvoted 3 times

 **zhangyu20000** 8 months, 1 week 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.

 **masetromain** Highly Voted 8 months, 1 week 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 5 times

 **dkcloudguru** Most Recent 2 weeks, 6 days ago

A and D : is the best way

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: AD

AD. A so can use SCP

upvoted 1 times

 **Maria2023** 4 months, 1 week 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 1 times

 **mfsec** 6 months ago

Selected Answer: AD

AD easy

upvoted 3 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: AD

A and D

upvoted 4 times

 **zhangyu20000** 8 months, 1 week 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

 **RaghavendraPrakash** Highly Voted 4 months, 2 weeks 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 6 times

 **AjayD123** Highly Voted 8 months, 1 week 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** 7 months, 4 weeks ago

thanks for the information about RDS read replica

upvoted 2 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: CDE

CDE, agree with other comments

upvoted 1 times

 **Sarutobi** 5 months, 1 week 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 2 times

 **dev112233xx** 5 months, 2 weeks 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 4 times

 **mfsec** 6 months ago

Selected Answer: CDE

CDE is the best choice

upvoted 1 times

 **DWsk** 6 months, 1 week 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** 5 months, 1 week ago

I agree with your logic.

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks 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** 7 months, 4 weeks ago

Selected Answer: CDE

C D and E

upvoted 2 times

 **nyxs_19** 7 months, 1 week 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

 **masetromain** 8 months, 1 week 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 3 times

 **masetromain** 8 months, 1 week 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** 8 months, 1 week 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** 7 months, 2 weeks ago

C, D and E Correct

upvoted 1 times

 **zhangyu20000** 8 months, 1 week 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.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

it's D, but private link would be a better choice

upvoted 1 times

 **dev112233xx** 5 months, 2 weeks ago

Selected Answer: D

D

Well.. "external ID" is the keyword that you should look for in such scenario.

upvoted 3 times

 **mfsec** 6 months ago

Selected Answer: D

With the external ID.

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks 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 1 times

 **Musk** 7 months, 3 weeks ago

Selected Answer: D

Easy. The external ID is for sure the winner.

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: D

D seems the correct answer

upvoted 2 times

 **Untamables** 8 months ago

Selected Answer: D

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

upvoted 2 times

 **masetromain** 8 months, 1 week 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** 8 months, 1 week 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.

 **dev112233xx**  5 months, 2 weeks 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 5 times

 **n_d1**  1 week 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 1 times

 **Ganshank** 1 month ago

Real-world answer - B.

Certification answer - D.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

going with D

upvoted 1 times

 **rbm2023** 4 months, 1 week 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** 5 months ago

B is correct

Anytime you need Docker containers with a custom configuration use EKS

upvoted 2 times

 **Jay_2pt0_1** 5 months, 1 week 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** 6 months ago

Selected Answer: D

D is easier

upvoted 1 times

 **taer** 6 months, 1 week ago

Selected Answer: D

I vote for D

upvoted 1 times

 **rtgfdv3** 6 months, 2 weeks 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** 4 months, 3 weeks ago

Agree and for the same reason.

upvoted 1 times

 **kiran15789** 6 months, 3 weeks 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** 6 months, 3 weeks 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** 7 months ago

Selected Answer: D

<https://docs.aws.amazon.com/cli/latest/reference/ecs/run-task.html>

upvoted 1 times

 **kiran15789** 7 months ago

Selected Answer: B

Option B and D are both valid solutions to meet the requirements, but option B is the better choice for the following reasons:

It uses AWS Fargate, which is a serverless compute engine for containers, eliminating the need for managing EC2 instances.

It allows for more efficient resource allocation as Fargate automatically scales the containers based on demand, reducing operational overhead.

It allows for tagging resources directly in the EKS cluster, simplifying management and reducing the potential for errors.

Therefore, option B is the best solution for the delivery company's requirements.

upvoted 2 times

 **Musk** 7 months, 1 week ago

Selected Answer: B

tag-resource is the right option. I don't think --tags is a valid option for that

upvoted 1 times

 **Musk** 7 months, 1 week ago

Now I am not sure. I believe it's D

upvoted 1 times

 **c73bf38** 7 months ago

You tag the Task, not the pods. That's the difference between B and D.

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: D

ECS and Fargate cost effective

upvoted 2 times

 **masetromain** 8 months, 1 week ago

Selected Answer: D

The correct answer is 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.

AWS Fargate is a serverless compute engine for containers that eliminates the need to provision and manage servers, which reduces operational overhead. Additionally, Fargate automatically scales resources based on the number of running containers, providing cost-effective resource allocation. Using the AWS CLI run-task command and setting enableECSManagedTags to true allows for easy tagging of resources for organization and cost tracking.

upvoted 2 times

 **masetromain** 8 months, 1 week ago

The other options, A and C, are using Amazon Elastic Kubernetes Service (Amazon EKS) and Amazon Elastic Container Service (Amazon ECS) on Amazon EC2, which require provisioning and management of servers and may not provide the same cost-effective resource allocation as Fargate. Option B is using EKS on Fargate but it's not recommended because EKS is intended for more complex and advanced use cases, whereas ECS is a more simple service for running Docker container.

upvoted 2 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

 **Appon** Highly Voted 7 months, 2 weeks ago

Selected Answer: AE

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudformation-vpc-peering-error/>
upvoted 6 times

 **SK_Tyagi** Most Recent 1 month, 1 week ago

Selected Answer: AE

This is correct, per Appon's link
upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: AE

AE for sure
upvoted 1 times

 **ThaiNT** 4 months, 2 weeks ago

Selected Answer: BE

VPCs are not in the same Region.
upvoted 3 times

 **ThaiNT** 4 months, 2 weeks ago

My bad, option B is incorrect.
upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: AE

AE is the best choice
upvoted 2 times

 **God_Is_Love** 6 months, 3 weeks 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** 7 months, 4 weeks ago

Selected Answer: AE

A and E
upvoted 1 times

 **masetromain** 8 months, 1 week 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

 **Arnaud92** 2 weeks ago

stop asking to ChatGPT

upvoted 1 times

 **clownfishman** 3 months, 2 weeks ago

us-east-1 is in virginia, us-east-2 is in ohio - they are separate regions

upvoted 3 times

 **zhangyu20000** 8 months, 1 week ago

AE is correct

D is not correct because you cannot share VPC via RAM, subnet can

upvoted 3 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.

 **God_Is_Love** Highly Voted  6 months, 3 weeks 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 8 times

 **God_Is_Love** 6 months, 3 weeks 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 5 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: B

B - basic access analyzer use case

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

keyword == Access Management Access Analyzer to generate IAM

upvoted 1 times

 **Alabi** 3 months, 2 weeks ago

Selected Answer: B

B definitely

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B

B - Identity and Access Management Access Analyzer

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: B

Identity and Access Management Access Analyzer
upvoted 1 times

 **masetromain** 8 months, 1 week 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 1 times

 **zhangyu20000** 8 months, 1 week 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.

 **God_Is_Love** Highly Voted 6 months, 3 weeks 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 8 times

 **God_Is_Love** 6 months, 3 weeks ago

fyi Pricing looks cheap too - <https://aws.amazon.com/compute-optimizer/pricing/>

upvoted 1 times

 **God_Is_Love** 6 months, 3 weeks 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 1 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: C

C. need CW agent for RAM util

upvoted 1 times

 **Fredonly** 5 months, 1 week ago

Selected Answer: C

C- Compute Optimizer is the easiest solution

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

C - cost optimizer

upvoted 1 times

 **mfsec** 6 months ago

*Compute

upvoted 1 times

 **spd** 6 months, 3 weeks ago

Selected Answer: C

C is correct - Optimizer

upvoted 2 times

✉ **kiran15789** 7 months ago

Selected Answer: A

Option C may be a good solution to rightsize 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** 6 months, 3 weeks ago

Bro, install cost is 0. Simple linux command > sudo yum install amazon-cloudwatch-agent

upvoted 2 times

✉ **masetromain** 8 months, 1 week 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** 8 months, 1 week 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.

 **bititan** Highly Voted 7 months 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 8 times

 **uC6rW1aB** Most Recent 2 weeks, 3 days 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** 2 weeks, 1 day 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 1 times

 **venvig** 3 weeks, 3 days 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** 2 months, 3 weeks ago

Selected Answer: B

its a b

upvoted 1 times

 **Jackhemo** 3 months, 2 weeks 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** 4 months, 4 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** 3 months ago

I couldn't find any option to share Secret Manager resources via RAM, did anyone try it?

upvoted 3 times

 **Sarutobi** 5 months, 1 week 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 4 times

 **dev112233xx** 5 months, 2 weeks 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** 6 months ago

Selected Answer: B

B is the best choice

upvoted 2 times

 **DWsk** 6 months, 1 week 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** 6 months, 2 weeks ago

Selected Answer: B

cross account assume role

upvoted 2 times

 **sambb** 6 months, 3 weeks ago

Selected Answer: B

Cross account assumerole is needed. You can't directly grant access to the secret from the DBA account to the application account because the key policy for the default KMS key is not modifiable.

upvoted 4 times

 **God_Is_Love** 6 months, 3 weeks ago

Selected Answer: B

<https://d2908q01vomqb2.cloudfront.net/887309d048beef83ad3eabf2a79a64a389ab1c9f/2020/09/17/PatternSecretsManager2.png>

App account has the RDS and Secrets manager. So, first, app team should allow to share the secret with DBA account thru "DBA-Secret" IAM role. and DBA (thru DBA-Admin role) should assume that role to access secret. This is common design pattern. So option which has DBA-Secret IAM role is the answer which is B

upvoted 3 times

 **God_Is_Love** 6 months, 3 weeks ago

* I meant option which says DBA-Secret role in app account (owner account) is the answer

upvoted 1 times

 **kiran15789** 7 months ago

Selected Answer: B

Option B is the correct answer because it creates an IAM role named DBA-Secret in the application account and grants the required permissions to access the secrets. In the DBA account, it creates an IAM role named DBA-Admin, grants the required permissions to assume the DBA-Secret role in the application account, and attaches the DBA-Admin role to the EC2 instance for access to the cross-account secrets. This eliminates the need to manually share the secrets and provides access to the database administrators to the database.

upvoted 3 times

 **[Removed]** 7 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/blogs/database/design-patterns-to-access-cross-account-secrets-stored-in-aws-secrets-manager/> the diagram here is pretty much exactly the scenario described in this question. B for the win

upvoted 2 times

 **c73bf38** 7 months, 1 week ago

Selected Answer: B

Option B is the correct solution to meet the requirements.

In this solution, an IAM role named DBA-Secret is created in the application account, and the required permissions to access the secrets are granted to this role. In the DBA account, an IAM role named DBA-Admin is created, and the required permissions to assume the DBA-Secret role in the application account are granted to this role. The DBA-Admin role is then attached to the EC2 instance to access the cross-account secrets.

This solution follows the principle of least privilege, where the IAM roles have only the necessary permissions to access the secrets. Also, it eliminates the need for manual sharing of secrets and provides a secure way to access the secrets by leveraging cross-account IAM roles.

upvoted 3 times

 **spd** 7 months, 2 weeks ago

Selected Answer: C

It can not be B - How one role assume to other role ?

upvoted 1 times

 **lunt** 7 months, 1 week ago

Why not? It's called role chaining and been available since cross-accounts IAM permissions. Used it numerous times. The userY>Acct1:RoleA>Acct2:RoleB. Acct2:RoleB permissions is only valid for 1hr on CLI/API.

upvoted 4 times

 **spd** 7 months, 1 week ago

Thanks, it should be B then

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.

 **venvig** 3 weeks, 3 days ago

Selected Answer: CE

Very straightforward

upvoted 1 times

 **dtha1002** 1 month, 4 weeks ago

Selected Answer: CE

C for all resources region
and E for DataOps OU launch instance type

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: CE

its CE

upvoted 1 times

 **OCHT** 5 months, 3 weeks 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 3 times

 **OCHT** 5 months, 3 weeks 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** 6 months ago

Selected Answer: CE

SCP's are the most efficient here

upvoted 1 times

 **tatdatpham** 7 months, 3 weeks 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** 8 months, 1 week 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 1 times

 **masetromain** 8 months, 1 week 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** 8 months, 1 week 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.

 **SK_Tyagi** 1 month, 1 week ago

Selected Answer: AC

SNS being the publisher, SQS is subscribing

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: AC

It's an AC

upvoted 1 times

 **Maria2023** 3 months 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 1 times

 **Parsons** 5 months ago

Selected Answer: AC

A, C is correct.

It looks like Fan out pattern.

upvoted 3 times

 **Kampton** 5 months, 1 week ago

Why would need to deploy SQS with Lambda? Makes no sense! It's BE.

upvoted 1 times

 **Diego1414** 4 months, 3 weeks ago

It's SNS that publishes not SQS

upvoted 1 times

 **Asagumo** 5 months, 3 weeks ago

What does it mean in Option A that Lambda deploys SQS?

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: AC

AC - SQS

upvoted 2 times

 **Zek** 6 months, 3 weeks ago

support A,C. <https://www.examtopics.com/discussions/amazon/view/74009-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

 **MasterP007** 7 months, 3 weeks ago

A & C - Deploy & Subscribe SQS.

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: AC

A and C

upvoted 3 times

  **masetromain** 8 months, 1 week 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** 8 months, 1 week 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.

 **zhangyu20000** Highly Voted  8 months, 1 week ago
C is correct. only eventbridge can run scheduled task
upvoted 9 times

 **task_7** Most Recent  1 day 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 1 times

 **uC6rW1aB** 2 weeks, 3 days 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 regually, 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 involved lambda to achive.
upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C
C. schedule -> eventbridge
upvoted 1 times

 **Maria2023** 3 months 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** 4 months, 1 week 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 2 times

 **mfsec** 6 months ago

Selected Answer: C
C - Fargate is the best choice here
upvoted 1 times

 **masetromain** 8 months, 1 week 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** 8 months, 1 week 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.

 **zozza2023**  7 months, 4 weeks ago

Selected Answer: C

DynamoDB global tables + S3 replication+Cloudfront

upvoted 10 times

 **uC6rW1aB**  2 weeks, 3 days 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 1 times

 **dkcloudguru** 2 weeks, 5 days ago

option c is the easiest way to do

upvoted 1 times

 **ProMax** 3 weeks, 4 days 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** 1 month, 1 week ago

Selected Answer: C

Option C has another differentiator - DynamoDBStreams that will assist in Reliability

upvoted 1 times

 **ggrodsckiy** 1 month, 4 weeks ago

Correct A.

CloudFront does not support origin failover with two origins accessing the S3 buckets in each Region. According to the AWS documentation https://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** 3 weeks, 3 days 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** 2 months, 3 weeks ago

Selected Answer: C

weird question wording, but C fit more

upvoted 1 times

✉  **mfsec** 6 months ago

Selected Answer: C

Create another S3 bucket in a new Region, and configure S3 Cross-Region Replication between the buckets

upvoted 2 times

✉  **masetromain** 8 months, 1 week 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 2 times

✉  **masetromain** 8 months, 1 week 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 1 times

✉  **zhangyu20000** 8 months, 1 week 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.

 **uC6rW1aB** 2 weeks, 3 days ago

Selected Answer: C

C correct

DocumentDB only have on-demand instance but not on-demand capacity mode, the mode is for DynamoDB
upvoted 3 times

 **ProMax** 3 weeks, 4 days ago

Selected Answer: C

Amazon DocumentDB does NOT have on-demand capacity mode, so its option C.

upvoted 1 times

 **SK_Tyagi** 1 month, 1 week 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 MongoDB. On-demand instances serve the purpose here, they are offered by DocumentDB, see the link
<https://aws.amazon.com/documentdb/pricing/>

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

its a c

upvoted 1 times

 **easytoo** 3 months, 1 week ago

c-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** 3 months, 2 weeks 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** 4 months, 1 week 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** 4 months, 1 week ago

The correct link <https://www.appliytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/743016963590682>
upvoted 2 times

 **leehjworking** 4 months, 1 week ago

Selected Answer: C

See best practices for amazon documentdb - instance sizing in docs.

upvoted 1 times

 **Sarutobi** 5 months, 1 week 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** 5 months, 2 weeks 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** 6 months ago

Selected Answer: C

C - there is no on-demand capacity mode.

upvoted 1 times

 **zejou1** 6 months, 1 week 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

 **kiran15789** 6 months, 2 weeks ago

Selected Answer: C

No on-demand capacity mode for DocumentDB

upvoted 2 times

 **sambb** 6 months, 3 weeks ago

Selected Answer: C

No on-demand capacity mode for DocumentDB

upvoted 1 times

 **andras** 6 months, 3 weeks ago

Selected Answer: C

<https://dynamodb.dev/dynamodb-vs-documentdb/>

upvoted 1 times

 **Sarutobi** 6 months, 3 weeks ago

Selected Answer: C

Is C, DocumentDB On-Demand is not a thing. You need to create On-Demand instances as part of the cluster, but nothing like DynamoDB. The cluster can either be Instance base or Elastic.

upvoted 2 times

 **Mahakali** 7 months, 1 week ago

Selected Answer: D

On-demand capacity mode is there for document DB

<https://aws.amazon.com/blogs/database/running-spiky-workloads-and-optimizing-costs-by-more-than-90-using-amazon-dynamodb-on-demand-capacity-mode/>

upvoted 1 times

 **c73bf38** 7 months ago

That blog is for Dynamodb, not document DB. Nowhere is mentioned capacity mode for documentDB, there's on-demand
<https://aws.amazon.com/documentdb/pricing/>.

upvoted 3 times

 **spd** 7 months, 1 week ago

Is this ref for DocumentDB ?

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.

 **God_Is_Love** Highly Voted 6 months, 3 weeks 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 6 times

 **God_Is_Love** 6 months, 3 weeks 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 2 times

 **leehjworking** Highly Voted 4 months, 1 week ago

Selected Answer: ACF

B full permission ? X
 D anonymous? X
 E encryption not needed for strategy team

upvoted 5 times

 **SK_Tyagi** Most Recent 1 month, 1 week ago

Selected Answer: ACF

By rule of elimination
 BDE are wrong. God_Is_Love is spot on
 upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: ACF

its ACF
 upvoted 1 times

 **OCHT** 5 months, 3 weeks 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** 6 months ago

Selected Answer: ACF

ACF is the best choice

upvoted 2 times

 **taer** 6 months, 1 week 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** 7 months, 4 weeks ago

Selected Answer: ACF

A C AND F

upvoted 3 times

 **Untamables** 8 months ago

Selected Answer: ACF

<https://repost.aws/knowledge-center/cross-account-access-denied-error-s3>

upvoted 3 times

 **masetromain** 8 months, 1 week ago

Selected Answer: ACF

A, C, and F are the correct options.

upvoted 4 times

 **masetromain** 8 months, 1 week 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 1 times

 **zhangyu20000** 8 months, 1 week 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.

 **dev112233xx** Highly Voted  5 months, 2 weeks 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 9 times

 **Kampton** 5 months, 1 week 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 1 times

 **God_Is_Love** Highly Voted  6 months, 2 weeks 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 7 times

 **God_Is_Love** 6 months, 2 weeks 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 3 times

 **uC6rW1aB** Most Recent  2 weeks, 3 days 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** 1 month 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** 1 month, 1 week 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_thanhung** 3 weeks, 4 days ago

S3 event can't trigger direct AWS Batch job. => C

upvoted 1 times

 **RGR21** 1 month, 2 weeks ago

Does the AWS DataSync support SAN?

upvoted 1 times

 **ggrodskiy** 1 month, 4 weeks ago

Correct D.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks 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** 3 months, 1 week 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** 3 months, 2 weeks ago

Lambda can run only for 15 minutes.

upvoted 1 times

 **rbm2023** 4 months, 1 week 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

 **Parsons** 5 months ago

Selected Answer: D

Option D is a valid solution to the given scenario.

By using an AWS Storage Gateway file gateway to transfer the sequencing data to Amazon S3, the company can leverage the Direct Connect connection to transfer data quickly and securely.

Using S3 events to trigger an AWS Batch job that executes on Amazon EC2 instances running the Docker containers to process the data, the company can take advantage of the scalability and flexibility of AWS Batch to process genomics data.

This solution allows the company to process the data quickly and scale based on workload demands while reducing the turnaround time from weeks to days.

upvoted 2 times

 **Eshu2009** 6 months ago

Cannot be D. S3 events cannot trigger Batch jobs. Only Eventbridge can trigger but that's not an option in D. Both Storage FileGW and Datasync don't support SAN. File GS supports NAS via NFS/SMB. DataSync NAS via NFS/SMB.

Data Pipeline can be an option.

upvoted 2 times

 **Asagumo** 6 months ago

Selected Answer: C

正解はCです。

SANについての記載がありますが、それはあくまで現状の説明であって、次期の仕組みの話ではないです。

また、S3イベントで起動できるものにAWS Batchはありません。

upvoted 5 times

 **easytoo** 3 months, 1 week ago

summed it up nicely.

upvoted 3 times

✉️  **chikorita** 1 month, 1 week ago

translate for others too
upvoted 1 times

✉️  **Arnaud92** 6 months ago

For me, none of these answer are correct.
C: DataSync is not working with SAN
D: Storage gateway have multiple gateway type. Answer is talking about "file gateway" which is not compatible with SAN. The gateway compatible would be "Volume gateway".
B: Data Pipeline, i'm not sure it's working with SAN.
A: snow is not a solution for regular and automatic process ..
upvoted 2 times

✉️  **mfsec** 6 months, 1 week ago

Selected Answer: D

D because of the SAN. Its more efficient to use Storage Gateway.
upvoted 1 times

✉️  **taer** 6 months, 1 week ago

Selected Answer: C

C is correct
upvoted 2 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.

 **God_Is_Love** Highly Voted  6 months, 2 weeks 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 7 times

 **uC6rW1aB** Most Recent  2 weeks, 3 days ago

Selected Answer: C

Option B FSx for Lustre is not for Linux POSIX-compliant
 Option C correct
 upvoted 1 times

 **dkcloudguru** 2 weeks, 4 days ago

C FSx for windows is a good fit for this
 upvoted 1 times

 **Sam202** 2 months, 2 weeks ago

FSx for Lustre can only be used by Linux-based instances.
 upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C for windows
 upvoted 1 times

 **SkyZeroZx** 3 months, 2 weeks ago

Selected Answer: C

EFS and FSx for Lustre == Linux
 FSx Windows File == Windows
 upvoted 2 times

 **mfsec** 6 months, 1 week ago

Selected Answer: C

EFS and Windows is not straight forward. C is the best solution.
 upvoted 2 times

 **zejou1** 6 months, 1 week 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** 7 months 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** 7 months, 3 weeks ago

Selected Answer: C

FSX for WIndows is the only option. The rest of options are not supported.

upvoted 2 times

 **jojom19980** 7 months, 3 weeks ago

Selected Answer: C

FSx for Lustre can only be used by Linux-based instances.

upvoted 2 times

 **zozza2023** 7 months, 4 weeks 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** 7 months, 4 weeks 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** 2 months, 3 weeks ago

Also that means each instance launched from the AMI will have 2TB EBS volume.. which is not ideal

upvoted 1 times

 **ARLV** 8 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** 8 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** 8 months, 1 week 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 3 times

 **masetromain** 8 months, 1 week 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** 8 months, 1 week 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

 **masetromain** 8 months, 1 week ago

Selected Answer: D

The correct answer is D, as it meets all of the requirements with the least management overhead.

In this solution, an Amazon Elastic File System (Amazon EFS) file system is created and an Auto Scaling group is created that extends across three Availability Zones and maintains a minimum size of three instances. A new AMI is created from the current EC2 instance that is running, and the instances in the Auto Scaling group are then launched from this new AMI.

A seamless domain join is then performed to join the instances to the AD domain, and the Amazon EFS file system is mounted on the instances. This solution uses an existing EC2 instance, so there is no need to use a user data script to install the application or join the instances to the AD domain, which reduces the management overhead.

upvoted 1 times

 **masetromain** 8 months, 1 week ago

The other choices are not correct because they either require a user data script to install the application or to join the instances to the AD domain, which increases the management overhead, or they use a different file system that may not be compatible with the application or the AD domain.

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

D is only one make sense

A: No AMI creation, have to use user data to install app, more complex

B: need user data

C: need user data

D: has least management overhead

upvoted 1 times

 **Musk** 7 months, 3 weeks ago

D: EFS does not work for Windows.

upvoted 1 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.

 **God_Is_Love** Highly Voted  6 months, 2 weeks ago

Selected Answer: D

SendTemplatedEmail
SendEmail
SendRawEmail are email api methods used in SES
upvoted 7 times

 **masetromain** Highly Voted  8 months, 1 week 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 5 times

 **Maria2023** 3 months 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 chatgpt

upvoted 3 times

 **SK_Tyagi** Most Recent  1 month, 1 week ago

Selected Answer: D

D - Can send templated email with request parameters
upvoted 1 times

 **Jonalb** 2 months, 2 weeks ago

Selected Answer: D

DDDDDDDD
upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

its a d

upvoted 1 times

 **Maria2023** 3 months 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** 1 month, 1 week ago

https://docs.aws.amazon.com/ses/latest/APIReference-V2/API_CreateEmailTemplate.html

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: D

keyword = SendTemplatedEmail API

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: D

Template - easy one.

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: D

D should be the answer

upvoted 3 times

 **zhangyu20000** 8 months, 1 week 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.

 **masetromain** Highly Voted 8 months, 1 week 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 15 times

 **3f30142** 2 months, 1 week ago

fully agree, option d is incorrect because 0 is an invalid value for maxReceiveCount

upvoted 1 times

 **Bwutch** 4 months ago

ChatGPT confirms this reasoning.

upvoted 3 times

 **Russs99** Most Recent 4 days, 19 hours ago

Selected Answer: D

checked 4 Al, 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** 3 weeks, 2 days 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 2 times

 **SK_Tyagi** 1 month, 1 week ago

Selected Answer: C

Going with C only because D has value of maxReceiveCount set to 0

upvoted 2 times

 **rtguru** 2 months, 1 week ago

I go with C

upvoted 1 times

 **YodaMaster** 2 months, 3 weeks 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 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C more likely

upvoted 1 times

 **Maria2023** 3 months 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** 4 months, 1 week 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 3 times

 **F_Eldin** 4 months, 1 week 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** 5 months 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** 4 months, 1 week 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** 5 months 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

 **mfsec** 6 months ago

Selected Answer: C

Scale-in protection
upvoted 1 times

 **mfsec** 6 months ago

the visibility timeout might still need to be adjusted, but the scale-in protection is the primary solution to prevent instances from being terminated during processing, which would cause the messages to end up in the dead-letter queue.

upvoted 1 times

 **kiran15789** 7 months ago

Selected Answer: C

Setting maxReceiveCount to 0 in the redrive policy of an Amazon SQS queue means that if a message is not successfully processed by any of the consumers after one attempt, the message will be deleted from the queue immediately instead of being moved to the dead-letter queue.

upvoted 4 times

 **Jesuisleon** 4 months, 1 week ago

Although your answer is right, your description for maxReceiveCount is WRONG.

maxReceiveCount represents the max count if app fails to deal with the message, after that the message is ALWAYS moved to dead-letter queue.

see " The maxReceiveCount is the number of times a consumer tries receiving a message from a queue without deleting it before being moved to the dead-letter queue. "

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

upvoted 1 times

 **spd** 7 months, 1 week ago

Selected Answer: C

C Correct Answer
upvoted 1 times

 **c73bf38** 7 months, 1 week ago

Selected Answer: D

I'm conflicted on this question, D updating the redrive sounds like the best solution because it's addressing the root cause. C is a workaround, not solving the problem of processing the videos.

upvoted 1 times

 **c73bf38** 7 months, 1 week ago

moderator dont approve, I figured it out.

upvoted 1 times

 **c73bf38** 7 months, 1 week ago

B is the correct option.

The issue seems to be that the videos are taking longer than the visibility timeout to process, so they are being sent to the dead-letter queue even though they are still being processed. By updating the visibility timeout for the SQS queue to 3 hours, the videos will have more time to process before being sent to the dead-letter queue, which should solve the problem.

upvoted 2 times

 **Sarutobi** 6 months, 3 weeks ago

Interesting point, I understood the problem in a different way. I think the problem is that while an EC2 Instance is still working on the video, there was a scale-in event and that instance was selected for termination. I will use personally lifecycle hooks, option C defeats the purpose of AutoScaling in some way like you said is a workaround.

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

for me, should be C
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.

 **zozza2023** Highly Voted 7 months, 4 weeks 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 7 times

 **venvig** Most Recent 3 weeks, 2 days ago

Selected Answer: C

Refer <https://aws.amazon.com/blogs/compute/introducing-amazon-api-gateway-private-endpoints/>
upvoted 1 times

 **Explorer_30** 3 weeks, 2 days ago

Answer is C as explain in <https://repost.aws/knowledge-center/api-gateway-vpc-connections>
upvoted 1 times

 **SK_Tyagi** 1 month, 1 week ago

Selected Answer: C

Regional to Private fits the use-case
upvoted 1 times

 **rtguru** 2 months ago

the best possible answer from all the options is C
upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

it's C, although it begs the questions about APIs that need to stay public...
upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: C

C. Update the API endpoint from Regional to private in API Gateway.
upvoted 1 times

 **masetromain** 8 months, 1 week 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** 8 months, 1 week 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.

 **sambb** Highly Voted 6 months, 3 weeks 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 10 times

 **rtguru** Most Recent 2 months ago

BD, I was initially looking at BE, I think global accelerator is used more for write requests.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: BD

BD makes more sense

upvoted 1 times

 **SmileyCloud** 2 months, 3 weeks ago

Selected Answer: BD

<https://godof.cloud/dynamic-origin-s3-spa/>

Use case

upvoted 1 times

 **Eshu2009** 6 months ago

BE- global accelerators improve performance by providing edge location for onboarding traffic.

upvoted 3 times

 **Eshu2009** 6 months 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** 6 months ago

Selected Answer: BD

I'll go with BD

upvoted 1 times

 **kiran15789** 7 months ago

Selected Answer: BD

Since only one additional region we don't need global accelerators

upvoted 4 times

 **bititan** 7 months ago

Selected Answer: BC

S3 transfer acceleration is more efficient

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: BD

A and E are not correct as there isn't a need to use aws global accel

upvoted 2 times

 **masetromain** 8 months, 1 week 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 4 times

 **zhangyu20000** 8 months, 1 week 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.

 **God_Is_Love** Highly Voted 6 months, 2 weeks 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 5 times

 **rtguru** Most Recent 2 months ago

B is the correct answer

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

it's B
upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

keyword == update-file-system
upvoted 1 times

 **leehjworking** 4 months, 1 week 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** 3 months ago

Perhaps the metric is used to trigger the step functions

upvoted 1 times

 **OCHT** 4 months, 4 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** 4 months, 1 week 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** 4 months, 4 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** 5 months, 2 weeks ago

Selected Answer: B

<https://chat.openai.com/chat>

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: B

B is correct

upvoted 2 times

 **zozza2023** 7 months, 4 weeks 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** 8 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

 **masetromain** 8 months, 1 week 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 4 times

 **zhangyu20000** 8 months, 1 week 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.

 **masetromain** Highly Voted  8 months, 1 week 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 10 times

 **venvig** Most Recent  3 weeks, 2 days 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 2 times

 **rtguru** 2 months ago

This one of those tricky questions. I'm not sure if to go with A or C

upvoted 1 times

 **rrrrrrrrrr1** 2 months, 2 weeks 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** 2 months, 3 weeks ago

Selected Answer: C

its a c

upvoted 1 times

✉ **Maria2023** 3 months 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** 3 months, 1 week 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** 6 months ago

Selected Answer: C

C is the most efficient

upvoted 3 times

✉ **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

C is correct

upvoted 3 times

✉ **zhangyu20000** 8 months, 1 week 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.

 **masetromain** Highly Voted  8 months, 1 week 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 6 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: A

its an A

upvoted 1 times

 **Goatin** 4 months, 1 week 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 2 times

 **mfsec** 6 months ago

Selected Answer: A

Replica

upvoted 4 times

 **God_Is_Love** 6 months, 2 weeks 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** 7 months, 4 weeks ago

Selected Answer: A

A is correct

upvoted 4 times

 **zhangyu20000** 8 months, 1 week 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.

 **God_Is_Love** Highly Voted  6 months, 2 weeks 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 so big data..So I choose C
upvoted 14 times

 **tycho** 5 months, 2 weeks ago

EMR and Glue are the same; Glue is managed cluster by AWS , EMR customer manages the clutster
upvoted 1 times

 **dkcloudguru** Most Recent  2 weeks, 2 days 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** 2 months, 3 weeks ago

Selected Answer: C

its a C
upvoted 1 times

 **SkyZeroZx** 3 months, 1 week 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** 6 months, 1 week ago

Selected Answer: C

C makes the most sense.
upvoted 2 times

 **Musk** 7 months, 3 weeks 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** 6 months, 3 weeks ago

That, I agree. Honestly, I will use it from day one, regardless.

upvoted 1 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: C

C is correct.

upvoted 4 times

 **masetromain** 8 months, 1 week 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 3 times

 **zhangyu20000** 8 months, 1 week 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.

 **God_Is_Love**  6 months, 2 weeks 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 18 times

 **God_Is_Love** 6 months, 2 weeks 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

 **Untamables**  8 months ago

Selected Answer: B

<https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html>

<https://docs.aws.amazon.com/drs/latest/userguide/recovery-workflow-gs.html>

Option C is wrong. That just mentions the migration method. I think this question asks us the DR architecture between on-premises and AWS cloud.

upvoted 6 times

 **AMohanty**  3 weeks, 1 day ago

C

We are looking for a Business Continuity Solution

Meaning RTO should be low

upvoted 1 times

 **chikorita** 2 weeks, 1 day 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** 3 weeks, 1 day 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** 4 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 2 times

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

Selected Answer: B

B for BC

upvoted 1 times

✉ **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

keyword = AWS Elastic Disaster Recovery

B

upvoted 1 times

✉ **rbm2023** 4 months, 1 week 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** 4 months, 4 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** 5 months, 2 weeks ago

Selected Answer: C

C seems correct to me (DMS with SCT and CDC)

upvoted 1 times

✉ **mfsec** 6 months, 1 week ago

Selected Answer: B

B has less operational overhead.

upvoted 3 times

✉ **taer** 6 months, 1 week ago

Selected Answer: B

B, tricky

upvoted 2 times

✉ **kiran15789** 7 months ago

Selected Answer: B

<https://aws.amazon.com/disaster-recovery/>

upvoted 3 times

✉ **Yowie351** 7 months ago

Selected Answer: B

The answer is definitely B. Database recovery is included as a feature with EDR.

<https://aws.amazon.com/blogs/storage/achieving-data-consistency-with-aws-elastic-disaster-recovery/>

upvoted 2 times

✉ **Mahakali** 7 months, 1 week ago

Selected Answer: B

Disaster recovery solution should be B , this option mentions AWS replication agent with reference to context of Elastic Disaster Recovery

upvoted 2 times

✉ **spd** 7 months, 2 weeks ago

Selected Answer: C

Selecting C

upvoted 1 times

✉ **moota** 7 months, 2 weeks ago

Selected Answer: B

It should be B. The frequent failover and fallback should be mostly a drill like here <https://docs.aws.amazon.com/drs/latest/userguide/failback-overview.html#drill-recover-instance-faq>

The sentence does not make sense. CDC is not with SCT.

- > Create a local AWS Schema Conversion Tool (AWS SCT) change data capture (CDC) task to keep the data synchronized
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.

 **tatdatpham** Highly Voted 7 months, 3 weeks 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 5 times

 **dkcloudguru** Most Recent 2 weeks, 2 days ago

B is correct

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

its a b

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B

In the company's AWS account, create an IAM role that trusts the auditors' AWS account.

upvoted 2 times

 **zozza2023** 7 months, 4 weeks ago

Selected Answer: B

B seems to be the right answer

upvoted 3 times

 **masetromain** 8 months, 1 week 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 2 times

 **masetromain** 8 months, 1 week 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 1 times

 **zhangyu20000** 8 months, 1 week 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.

 **Untamables**  8 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 8 times

 **Ganshank**  1 month 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 5 times

 **frfavoredo** 1 week, 4 days 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

 **dkcloudguru**  2 weeks, 2 days 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 1 times

 **duriselvan** 2 weeks, 5 days ago

<https://aws.amazon.com/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>

upvoted 1 times

 **duriselvan** 2 weeks, 5 days 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** 2 weeks, 5 days 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 3 weeks, 1 day ago

A

Once u enable DAX you cant directly write onto or Read from Dynamo DB.

upvoted 1 times

ggrodskiy 2 months ago

Correct B.

upvoted 1 times

Just_Ninja 2 months, 1 week ago

Selected Answer: B

AWS recommend 3 nodes for production workloads.

So it must B

upvoted 1 times

NikkyDicky 2 months, 3 weeks ago

Selected Answer: B

B for DAX HA

upvoted 1 times

Maria2023 3 months 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

rbm2023 4 months, 1 week ago

Selected Answer: B

I initially went for option A, but I agree with B. Not only because of the 3-node option which eliminates A completely. But also due to the read and write pattern suggested on B. The application is latency sensitive and if need to reduce the latency as much as possible you need to write directly to Dynamo and read from DAX which is a Write-Around pattern.

<https://aws.amazon.com/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>

upvoted 2 times

mfsec 6 months ago

Selected Answer: B

B is the answer

upvoted 1 times

God_Is_Love 6 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.concepts.cluster.html>

2 node is not fault tolerant and in fact more nodes less latency. If there's an option with > 3nodes, I'd go for that instead.

upvoted 2 times

kiran15789 7 months ago

Selected Answer: B

DynamoDB Accelerator (DAX) is an in-memory cache for DynamoDB that can significantly improve read performance. In this scenario, since the platform is latency-sensitive, the goal is to reduce read latency.

upvoted 2 times

saurabh1805 7 months ago

Selected Answer: B

As per below link B is best option.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.html#DAX.use-cases>

upvoted 1 times

c73bf38 7 months ago

The write-through behavior of DAX is appropriate for many application patterns. However, there are some application patterns where a write-through model might not be appropriate.

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.write-around>

upvoted 3 times

Question #151

Topic 1

A company has migrated an application from on premises to AWS. The application frontend is a static website that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB). The application backend is a Python application that runs on three EC2 instances behind another ALB. The EC2 instances are large, general purpose On-Demand Instances that were sized to meet the on-premises specifications for peak usage of the application.

The application averages hundreds of thousands of requests each month. However, the application is used mainly during lunchtime and receives minimal traffic during the rest of the day.

A solutions architect needs to optimize the infrastructure cost of the application without negatively affecting the application availability.

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

- A. Change all the EC2 instances to compute optimized instances that have the same number of cores as the existing EC2 instances.
- B. Move the application frontend to a static website that is hosted on Amazon S3.
- C. Deploy the application frontend by using AWS Elastic Beanstalk. Use the same instance type for the nodes.
- D. Change all the backend EC2 instances to Spot Instances.
- E. Deploy the backend Python application to general purpose burstable EC2 instances that have the same number of cores as the existing EC2 instances.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: BE

it's BE

upvoted 1 times

 **rbm2023** 4 months, 1 week ago

Selected Answer: BE

You cannot move all backend to Spot Instances this will break the requirement for not affecting the application availability.
You can improve by moving the static site to S3, front end, and change the on demand instances to burst capacity.

upvoted 2 times

 **OCHT** 5 months, 3 weeks ago

Selected Answer: BE

Amazon EC2 Spot Instances allow you to take advantage of unused EC2 capacity in the AWS Cloud at a steep discount compared to On-Demand Instance prices. Spot Instances are well-suited for workloads that can be interrupted, such as batch processing, data analysis, and image or video processing. They can also be used for fault-tolerant workloads that can withstand the loss of an instance, such as web services or stateless applications.

upvoted 2 times

 **OCHT** 5 months, 3 weeks ago

Option C suggests deploying the application frontend using AWS Elastic Beanstalk and using the same instance type for the nodes. Elastic Beanstalk is a fully managed service that makes it easy to deploy, run, and scale applications. It automatically handles the deployment and management of the underlying infrastructure, including capacity provisioning, load balancing, and auto-scaling. However, using Elastic Beanstalk with the same instance type as the existing EC2 instances may not necessarily reduce costs.

upvoted 1 times

 **OCHT** 5 months, 3 weeks ago

Option E suggests deploying the backend Python application to general purpose burstable EC2 instances that have the same number of cores as the existing EC2 instances. Burstable instances provide a baseline level of CPU performance with the ability to burst above the baseline when needed. This can be a cost-effective option for workloads that have variable CPU usage and can benefit from the ability to burst during periods of high demand. However, if the workload consistently requires high CPU usage, using burstable instances may not provide significant cost savings compared to using larger general purpose instances.

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: BE

BE makes the most sense here

upvoted 1 times

 **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: BE

Burstable because peak performance is needed at lunch time and its cost effective based on this -
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html>

S3 static website hosting is cost effective

upvoted 4 times

 **kiran15789** 7 months ago

Selected Answer: BE

Burstable EC2 instances, also known as T instances, provide a baseline level of CPU performance with the ability to burst CPU usage when additional cycles are available. They are designed for workloads that do not require sustained high CPU performance but occasionally need more CPU power. Burstable instances can be a cost-effective option for workloads that have moderate CPU requirements but still require flexibility to handle occasional spikes in demand.

upvoted 4 times

 **tatdatpham** 7 months, 3 weeks ago

Selected Answer: BE

The correct answer is B, E.

Option B of moving the frontend to a static website hosted on Amazon S3 will reduce the cost of running the frontend, as S3 is a lower cost storage option than EC2 instances.

Option E of deploying the backend Python application to general purpose burstable EC2 instances will ensure that the backend EC2 instances have the capacity to handle spikes in usage, as burstable instances are designed to handle unpredictable workloads. This will help to optimize the cost of running the backend, as burstable instances are less expensive than On-Demand instances and more cost-effective than Spot instances.

upvoted 1 times

 **Untamables** 8 months ago

Selected Answer: BE

B and E.

Option D is wrong. A spot instance is not appropriate for a production server.

By the way, I would like another option that mentions changing the backend Python API Gateway and Lambda because Option B mentions changing the frontend serverless. I think this question is a typical use case of the serverless architecture.

upvoted 4 times

 **vsk12** 8 months ago

Selected Answer: BE

Correct answers are

B & E

Option B as S3 is a cost-effective storage solution for static websites.

Option E as burstable general-purpose instances provides a cost-effective solution for this kind of workload.

upvoted 2 times

 **masetromain** 8 months, 1 week ago

Selected Answer: BD

B. Move the application frontend to a static website that is hosted on Amazon S3.

D. Change all the backend EC2 instances to Spot Instances.

Step 1: Moving the application frontend to a static website that is hosted on Amazon S3 will reduce the cost and increase the scalability of the application. S3 is a highly scalable object storage service that can handle large amounts of data and traffic at a lower cost than running EC2 instances.

Step 2: Changing the backend EC2 instances to Spot Instances can help reduce cost without negatively affecting the application availability. Spot Instances allow customers to bid on unused Amazon EC2 capacity, which can result in significant cost savings. You can also use AWS Auto Scaling to automatically increase or decrease the number of Spot Instances based on the application's traffic.

upvoted 3 times

 **masetromain** 8 months, 1 week ago

Option A, C: Changing to compute optimized instances or using Elastic Beanstalk will not help reducing the cost, it will only change the instances type and not helping the cost optimization.

Option E: Deploying the backend Python application to general purpose burstable EC2 instances will not help reducing the cost, as it still using On-Demand instances.

It is important to note that using spot instances comes with the risk of instances being terminated when the spot price goes up. To mitigate this risk, you could use the EC2 Auto Scaling group with a combination of on-demand and spot instances. This way, if a spot instance is terminated, the Auto Scaling group can automatically replace it with an on-demand instance to ensure the application is always available.

upvoted 1 times

 **zhangyu20000** 8 months, 1 week ago

BE are correct

A: Compute optimized instance is expensive than burstable instance

B: S3 hosted static web server is cheaper

C: Not save money

D: Spot instance affect availability

E: Burstable EC2 is cheaper

upvoted 2 times

 **masetromain** 8 months, 1 week ago

To mitigate this risk, you could use the EC2 Auto Scaling group with a combination of on-demand and spot instances. This way, if a spot instance is terminated, the Auto Scaling group can automatically replace it with an on-demand instance to ensure the application is always available.

upvoted 1 times

Question #152

Topic 1

A company is running an event ticketing platform on AWS and wants to optimize the platform's cost-effectiveness. The platform is deployed on Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 and is backed by an Amazon RDS for MySQL DB instance. The company is developing new application features to run on Amazon EKS with AWS Fargate.

The platform experiences infrequent high peaks in demand. The surges in demand depend on event dates.

Which solution will provide the MOST cost-effective setup for the platform?

- A. Purchase Standard Reserved Instances for the EC2 instances that the EKS cluster uses in its baseline load. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet predicted peak load for the year.
- B. Purchase Compute Savings Plans for the predicted medium load of the EKS cluster. Scale the cluster with On-Demand Capacity Reservations based on event dates for peaks. Purchase 1-year No Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale out database read replicas during peaks.
- C. Purchase EC2 Instance Savings Plans for the predicted base load of the EKS cluster. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale up the DB instance manually during peaks.
- D. Purchase Compute Savings Plans for the predicted base load of the EKS cluster. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale up the DB instance manually during peaks.

 **Untamables**  8 months ago

Selected Answer: B

Option A, C and D are wrong. They all mention using spot instances and EKS based on EC2. A spot instance is not appropriate for a production server and the company is developing new application designed for AWS Fargate, which means we must plan the future cost improvement including AWS Fargate.

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 12 times

 **zhangyu20000**  8 months, 1 week ago

B is correct. Compute saving plan will also cover Fargate

A: use spot instance is not reliable

CD: manually scale up DB

upvoted 7 times

 **Hyperdanny**  2 months, 1 week ago

Selected Answer: C

I am leaning towards C, since Instance savings provide the biggest discount.

I also couldn't find a way to scale EKS based on dates, which B suggests: "Scale the cluster with On-Demand Capacity Reservations based on event dates for peaks"

upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

its a b

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

Option A, C and D are wrong. They all mention using spot instances and EKS based on EC2. A spot instance is not appropriate for a production server and the company is developing new application designed for AWS Fargate, which means we must plan the future cost improvement including AWS Fargate.

upvoted 1 times

 **Roontha** 3 months, 3 weeks ago

I go with B post reading aws portal.

<https://aws.amazon.com/savingsplans/compute-pricing/>

Compute Savings Plans

Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, Region, OS or tenancy, and also apply to Fargate or Lambda usage. For example, with Compute Savings Plans, you can change from C4 to M5 instances, shift a workload from EU (Ireland) to EU (London), or move a workload from EC2 to Fargate or Lambda at any time and automatically continue to pay the Savings Plans price.

upvoted 1 times

 **y0eri** 4 months, 1 week ago

Selected Answer: D

Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance [...], and also apply to Fargate or Lambda usage. For example, with Compute Savings Plans, you can [...] move a workload from EC2 to Fargate.

Vertical scaling is the most straightforward approach to adding more capacity in your database. [...] You can vertically scale up [or down] your RDS instance with a click of a button.

Suppose that you purchase a db.t2.medium reserved DB instance, [...] if you have one db.t2.large instance running in your account in the same AWS Region, the billing benefit is applied to 50 percent of the usage of the DB instance.

<https://aws.amazon.com/savingsplans/compute-pricing/>

<https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/>

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

upvoted 1 times

 **yama234** 5 months, 1 week ago

B

Compute Savings Plans saving EC2 and Fargate.
production don't using Spot Instances

upvoted 1 times

 **dev112233xx** 5 months, 2 weeks ago

Selected Answer: A

A makes sense to me

upvoted 2 times

 **Amac1979** 6 months ago

Selected Answer: D

capacity reservations do not offer discounts. D is correct

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B

Purchase Compute Savings Plans for the predicted medium load of the EKS cluster.

upvoted 2 times

 **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: B

Out of some research initially against B, had to choose B because of this - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>

On Demand capacity reservations can be done anytime, so before events they can reserve and after events they can release to save costs
From above link -

Events — you can create Capacity Reservations before your business-critical events to ensure that you can scale when you need to.

"You can create Capacity Reservations at any time, without entering into a one-year or three-year term commitment. The capacity becomes available and billing starts as soon as the Capacity Reservation is provisioned in your account. When you no longer need the capacity assurance, cancel the Capacity Reservation to release the capacity and to stop incurring charges. You can also use the billing discounts offered by Savings Plans and Regional Reserved Instances to reduce the cost of a Capacity Reservation."

upvoted 5 times

 **kiran15789** 6 months, 2 weeks ago

Selected Answer: B

spot instances never a good answer

upvoted 2 times

 **[Removed]** 7 months, 1 week ago

Selected Answer: B

Surely B

upvoted 3 times

 **spd** 7 months, 1 week ago

Selected Answer: B

agree with B

upvoted 2 times

 **moota** 7 months, 2 weeks ago

Selected Answer: B

A is not good because the DB will be underutilized (1yr RI to meet the _predicted peak_). You need a reliable on-demand on event dates. There is little incentive but more downside of unreliability if you choose Spots on event dates.

upvoted 3 times

 **tatdatpham** 7 months, 3 weeks ago

Selected Answer: B

Agree with zhangyu20000

upvoted 3 times

Question #153

Topic 1

A company has deployed an application on AWS Elastic Beanstalk. The application uses Amazon Aurora for the database layer. An Amazon CloudFront distribution serves web requests and includes the Elastic Beanstalk domain name as the origin server. The distribution is configured with an alternate domain name that visitors use when they access the application.

Each week, the company takes the application out of service for routine maintenance. During the time that the application is unavailable, the company wants visitors to receive an informational message instead of a CloudFront error message.

A solutions architect creates an Amazon S3 bucket as the first step in the process.

Which combination of steps should the solutions architect take next to meet the requirements? (Choose three.)

- A. Upload static informational content to the S3 bucket.
- B. Create a new CloudFront distribution. Set the S3 bucket as the origin.
- C. Set the S3 bucket as a second origin in the original CloudFront distribution. Configure the distribution and the S3 bucket to use an origin access identity (OAI).
- D. During the weekly maintenance, edit the default cache behavior to use the S3 origin. Revert the change when the maintenance is complete.
- E. During the weekly maintenance, create a cache behavior for the S3 origin on the new distribution. Set the path pattern to \ Set the precedence to 0. Delete the cache behavior when the maintenance is complete.
- F. During the weekly maintenance, configure Elastic Beanstalk to serve traffic from the S3 bucket.

 **masetromain** Highly Voted 8 months, 1 week ago

Selected Answer: ACD

- A. Upload static informational content to the S3 bucket.
- C. Set the S3 bucket as a second origin in the original CloudFront distribution. Configure the distribution and the S3 bucket to use an origin access identity (OAI).
- D. During the weekly maintenance, edit the default cache behavior to use the S3 origin. Revert the change when the maintenance is complete.

Step 1: The solutions architect should upload static informational content to the S3 bucket, this content will be shown to the users when the application is down for maintenance.

Step 2: The solutions architect should set the S3 bucket as a second origin in the original CloudFront distribution. To keep the S3 bucket secure, the solutions architect should configure the distribution and the S3 bucket to use an origin access identity (OAI). This will ensure that only CloudFront has access to the S3 bucket.

upvoted 9 times

 **masetromain** 8 months, 1 week ago

Step 3: During the weekly maintenance, the solutions architect should edit the default cache behavior of the CloudFront distribution to use the S3 origin. This will redirect all incoming traffic to the S3 bucket and show the static informational content to the users. Once the maintenance is complete, the solutions architect should revert the change back to the original Elastic Beanstalk origin.

Option B: Creating a new CloudFront distribution and setting the S3 bucket as the origin is unnecessary and could cause confusion for the users.

Option E: During the weekly maintenance, creating a cache behavior for the S3 origin on the new distribution is unnecessary, it is more complex and prone to human error.

Option F: Configuring Elastic Beanstalk to serve traffic from the S3 bucket is not necessary because CloudFront is already being used as the web request server.

upvoted 1 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: ACD

ACD morelikely

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: ACD

A C D

E is good option but is more overhead and prone to error than C is more accessible

upvoted 2 times

 **Jesuisleon** 3 months, 1 week ago

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

upvoted 1 times

✉  **mfsec** 6 months ago

Selected Answer: ACD

ACD is the best fit

upvoted 2 times

✉  **Musk** 7 months, 2 weeks ago

Selected Answer: ACD

About E, the lowest possible value for the "Origin Priority" field in AWS CloudFront is 1

upvoted 3 times

✉  **zozza2023** 7 months, 4 weeks ago

Selected Answer: ACD

ACD is correct

upvoted 4 times

✉  **zhangyu20000** 8 months, 1 week ago

ABD is correct

upvoted 1 times

✉  **zhangyu20000** 8 months, 1 week ago

ACD is correct

upvoted 2 times

Question #154

Topic 1

A company gives users the ability to upload images from a custom application. The upload process invokes an AWS Lambda function that processes and stores the image in an Amazon S3 bucket. The application invokes the Lambda function by using a specific function version ARN.

The Lambda function accepts image processing parameters by using environment variables. The company often adjusts the environment variables of the Lambda function to achieve optimal image processing output. The company tests different parameters and publishes a new function version with the updated environment variables after validating results. This update process also requires frequent changes to the custom application to invoke the new function version ARN. These changes cause interruptions for users.

A solutions architect needs to simplify this process to minimize disruption to users.

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

- A. Directly modify the environment variables of the published Lambda function version. Use the SLATEST version to test image processing parameters.
- B. Create an Amazon DynamoDB table to store the image processing parameters. Modify the Lambda function to retrieve the image processing parameters from the DynamoDB table.
- C. Directly code the image processing parameters within the Lambda function and remove the environment variables. Publish a new function version when the company updates the parameters.
- D. Create a Lambda function alias. Modify the client application to use the function alias ARN. Reconfigure the Lambda alias to point to new versions of the function when the company finishes testing.

 **tatdatpham** Highly Voted 7 months, 3 weeks ago

Selected Answer: D

D is correct

By using a function alias, the custom application invokes the latest version of the Lambda function without the need to modify the application code every time the company updates the image processing parameters. This reduces the risk of causing interruptions for users.

upvoted 7 times

 **SK_Tyagi** Most Recent 1 month, 1 week ago

Selected Answer: D

Look for ALIAS

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

D

B is ok, but more overhead

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: D

keyword = Lambda ALIAS

then D

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: D

Create a Lambda function alias.

upvoted 1 times

 **masetromain** 8 months, 1 week ago

Selected Answer: D

D. Create a Lambda function alias. Modify the client application to use the function alias ARN. Reconfigure the Lambda alias to point to new versions of the function when the company finishes testing.

Creating a Lambda function alias allows the solutions architect to change the version of the Lambda function that the alias points to without modifying the client application. This eliminates the need for frequent updates to the custom application and minimizes disruption to users. The solutions architect can test different parameters by using different versions of the function and reconfigure the alias to point to the new version after validating results. This allows the company to update the image processing parameters without affecting the users.

upvoted 4 times

 **masetromain** 8 months, 1 week ago

- Option A: Directly modifying the environment variables of the published Lambda function version would cause all clients to use the updated environment variables immediately and would not allow for testing.
- Option B: Using DynamoDB to store image processing parameters increases complexity and operational overhead, and it would not eliminate the need for updating the custom application.
- Option C: Directly coding the image processing parameters within the Lambda function and publishing new versions would not eliminate the need for updating the custom application.

upvoted 2 times

 **zhangyu20000** 8 months, 1 week ago

D is correct

upvoted 1 times

Question #155

Topic 1

A global media company is planning a multi-Region deployment of an application. Amazon DynamoDB global tables will back the deployment to keep the user experience consistent across the two continents where users are concentrated. Each deployment will have a public Application Load Balancer (ALB). The company manages public DNS internally. The company wants to make the application available through an apex domain.

Which solution will meet these requirements with the LEAST effort?

- A. Migrate public DNS to Amazon Route 53. Create CNAME records for the apex domain to point to the ALB. Use a geolocation routing policy to route traffic based on user location.
- B. Place a Network Load Balancer (NLB) in front of the ALB. Migrate public DNS to Amazon Route 53. Create a CNAME record for the apex domain to point to the NLB's static IP address. Use a geolocation routing policy to route traffic based on user location.
- C. Create an AWS Global Accelerator accelerator with multiple endpoint groups that target endpoints in appropriate AWS Regions. Use the accelerator's static IP address to create a record in public DNS for the apex domain.
- D. Create an Amazon API Gateway API that is backed by AWS Lambda in one of the AWS Regions. Configure a Lambda function to route traffic to application deployments by using the round robin method. Create CNAME records for the apex domain to point to the API's URL.

 **God_Is_Love** Highly Voted  6 months, 2 weeks ago

Selected Answer: C

No, an apex domain cannot use CNAME records in AWS. This is because of the way DNS resolution works. A CNAME record specifies an alias for a domain name, which points to the canonical name of another domain. However, the DNS standard does not allow CNAME records for apex domains, as they should only have A or AAAA records.

When you try to create a CNAME record for an apex domain in AWS Route 53, you will receive an error message indicating that the record set type is not valid for the apex domain. To work around this limitation, you can use an alias record instead.

upvoted 13 times

 **zhangyu20000** Highly Voted  8 months, 1 week ago

C is correct

ABD all have CNAME record that is not allowed for apex domain

upvoted 6 times

 **Explorer_30** Most Recent  3 weeks, 2 days ago

The answer is C

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C

no CNAME for apex

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: C

A , B no seems because reference geolocation

D no seems because apex domain with API Gateway ?

then C Global Accelerator is good option

upvoted 1 times

 **chikorita** 3 months, 2 weeks ago

fun fact: CNAME records does not support APEX domain

which simply rules out the options with CNAME in it

answer is C

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: C

Create an AWS Global Accelerator accelerator with multiple endpoint groups that target endpoints in appropriate AWS Regions.

upvoted 3 times

 **masetromain** 8 months, 1 week ago

Selected Answer: C

C. Create an AWS Global Accelerator accelerator with multiple endpoint groups that target endpoints in appropriate AWS Regions. Use the accelerator's static IP address to create a record in public DNS for the apex domain.

This solution meets the requirements with the least effort because it uses AWS Global Accelerator, which automatically routes traffic to the optimal endpoint based on health and geography, eliminating the need for manual configuration or additional routing policies. It also eliminates the need to create a CNAME record for the apex domain to point to the ALB or NLB's IP address, which can be less efficient and less reliable.

upvoted 4 times

 **masetromain** 8 months, 1 week ago

A. Migrate public DNS to Amazon Route 53. Create CNAME records for the apex domain to point to the ALB. Use a geolocation routing policy to route traffic based on user location.

While this solution uses Route 53 and geolocation routing, it requires manual configuration and maintenance of the routing policy and could introduce additional latency as traffic is routed through the ALB first.

B. Place a Network Load Balancer (NLB) in front of the ALB. Migrate public DNS to Amazon Route 53. Create a CNAME record for the apex domain to point to the NLB's static IP address. Use a geolocation routing policy to route traffic based on user location.

This solution is similar to the first one, but it uses a Network Load Balancer (NLB) instead of an Application Load Balancer (ALB). It has the same downsides as the first solution.

upvoted 1 times

 **masetromain** 8 months, 1 week ago

D. Create an Amazon API Gateway API that is backed by AWS Lambda in one of the AWS Regions. Configure a Lambda function to route traffic to application deployments by using the round robin method. Create CNAME records for the apex domain to point to the API's URL.

This solution uses Amazon API Gateway and AWS Lambda to route traffic, but the round-robin method is not the best way to ensure optimal performance and availability for a multi-region deployment. Additionally, routing traffic through a Lambda function can introduce additional latency.

AWS Global Accelerator is a more efficient solution that automatically routes traffic to the optimal endpoint based on health and geography, eliminating the need for manual configuration or additional routing policies.

upvoted 1 times

Question #156

Topic 1

A company is developing a new serverless API by using Amazon API Gateway and AWS Lambda. The company integrated the Lambda functions with API Gateway to use several shared libraries and custom classes.

A solutions architect needs to simplify the deployment of the solution and optimize for code reuse.

Which solution will meet these requirements?

- A. Deploy the shared libraries and custom classes into a Docker image. Store the image in an S3 bucket. Create a Lambda layer that uses the Docker image as the source. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the Lambda layer.
- B. Deploy the shared libraries and custom classes to a Docker image. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Create a Lambda layer that uses the Docker image as the source. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the Lambda layer.
- C. Deploy the shared libraries and custom classes to a Docker container in Amazon Elastic Container Service (Amazon ECS) by using the AWS Fargate launch type. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the deployed container as a Lambda layer.
- D. Deploy the shared libraries, custom classes, and code for the API's Lambda functions to a Docker image. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Configure the API's Lambda functions to use the Docker image as the deployment package.

 **Iunt** Highly Voted 7 months, 1 week ago

Selected Answer: D

Don't understand why so many people are choosing B. Read up. A container image cannot be used with Lambda layers. That means A B C are out instantly. Its literally one of the first things they mention about Lambda layers. Answer is D and ABC simply impossible to configure.

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

upvoted 21 times

 **Gabehcoud** 1 month, 2 weeks ago

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

Previously, Lambda functions were packaged only as .zip archives. This includes functions created in the AWS Management Console. You can now also package and deploy Lambda functions as container images.

You can use familiar container tooling such as the Docker CLI with a Dockerfile to build, test, and tag images locally. Lambda functions built using container images can be up to 10 GB in size. You push images to an Amazon Elastic Container Registry (ECR) repository, a managed AWS container image registry service. You create your Lambda function, specifying the source code as the ECR image URL from the registry.

upvoted 1 times

 **c73bf38** 7 months, 1 week ago

B suggests deploying the shared libraries and custom classes to a Docker image, uploading it to Amazon Elastic Container Registry (Amazon ECR), creating a Lambda layer that uses the Docker image as the source, and deploying the API's Lambda functions as Zip packages. Configuring the packages to use the Lambda layer simplifies deployment, and the Docker image allows for code reuse. This option takes advantage of the built-in features provided by AWS API Gateway and Lambda, making it the optimal solution.

upvoted 5 times

 **c73bf38** 7 months ago

The requirement is code reuse:

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

Lambda functions packaged as container images do not support adding Lambda layers to the function configuration. However, there are a number of solutions to use the functionality of Lambda layers with container images. You take on the responsibility for packaging your preferred runtimes and dependencies as a part of the container image during the build process.

upvoted 3 times

 **rbm2023** 4 months, 1 week ago

D does not seem a correct option because it suggests packaging everything into a Lambda layer including the Lambda functions. This will break the reusability of the deployment. All you need to package into images are the libraries and the custom classes and then build the layer from there.

the correct option is B, in my view.

upvoted 2 times

 **rtgfdv3** 6 months, 2 weeks ago

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 3 times

 **Untamables** Highly Voted 8 months ago

Selected Answer: D

Option A, B and C are wrong. An AWS Lambda Layer does not support a Docker image or a deployed container as the source.

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

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 7 times

 **dkcloudguru** Most Recent 2 weeks, 2 days ago

Ans is D: <https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/#:~:text=Lambda%20functions%20packaged%20as%20container,Lambda%20layers%20with%20container%20images>.

upvoted 1 times

 **Gabehcoud** 1 month, 2 weeks ago

Answer B.

Previously, Lambda functions were packaged only as .zip archives. This includes functions created in the AWS Management Console. You can now also package and deploy Lambda functions as container images.

You can use familiar container tooling such as the Docker CLI with a Dockerfile to build, test, and tag images locally. Lambda functions built using container images can be up to 10 GB in size. You push images to an Amazon Elastic Container Registry (ECR) repository, a managed AWS container image registry service. You create your Lambda function, specifying the source code as the ECR image URL from the registry.

upvoted 2 times

 **vn_thanhung** 1 month ago

<https://www.youtube.com/watch?v=17R0vN8bt-0>

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct B.

upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

D

layers not supported w container-based lambdas

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: D

Docker images cannot be used in Lambda layers.

upvoted 1 times

 **Jackhemo** 3 months, 1 week ago

Selected Answer: B

From olabiba.ai: Overall, option B provides a streamlined approach to optimize code reuse by centralizing the shared code in a Docker image and using a Lambda layer to share it across multiple functions.

upvoted 1 times

 **Roontha** 3 months, 3 weeks ago

Answer : B

upvoted 1 times

 **rbm2023** 4 months, 1 week ago

Selected Answer: B

"Lambda functions packaged as container images do not support adding Lambda layers to the function configuration. However, there are a number of solutions to use the functionality of Lambda layers with container images. You take on the responsibility for packaging your preferred runtimes and dependencies as a part of the container image during the build process."

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 4 times

 **AMEJack** 4 months, 3 weeks ago

Selected Answer: D

Although the following URL says that you can deploy Lambda layers as container but this can't be used when the Lambda function is zip. The function will be created as another layer in the container image and it should use Lambda runtime environment.

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 3 times

 **dev112233xx** 5 months, 2 weeks ago

Selected Answer: D

B is incorrect.. Docker images uses Layers refer to other Docker images, You can refer to a Docker layer ONLY if you choose to run your code in a Docker container (not a ZIP)

read this article:

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 4 times

 **dev112233xx** 5 months, 2 weeks ago

Also read this article:

"You can use layers only with Lambda functions deployed as a .zip file archive. For functions defined as a container image, you package your preferred runtime and all code dependencies when you create the container image. For more information, see Working with Lambda layers and extensions in container images on the AWS Compute Blog."

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

upvoted 2 times

✉ **dev112233xx** 5 months, 2 weeks ago

and

"Lambda functions packaged as container images do not support adding Lambda layers to the function configuration. However, there are a number of solutions to use the functionality of Lambda layers with container images. You take on the responsibility for packaging your preferred runtimes and dependencies as a part of the container image during the build process."

So it's clearly not B

upvoted 2 times

✉ **Asagumo** 5 months, 4 weeks ago

Selected Answer: B

This page is in Japanese.

<https://michimani.net/post/aws-create-lambda-layers-with-docker/>

upvoted 2 times

✉ **fabu** 6 months ago

Selected Answer: D

B is correct.

upvoted 2 times

✉ **mfsec** 6 months ago

Selected Answer: D

D seems a better choice. Docker images can be used to package and deploy Lambda functions directly, but not for Lambda layers.

upvoted 3 times

✉ **taer** 6 months, 1 week ago

Selected Answer: B

B. Deploy the shared libraries and custom classes to a Docker image. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Create a Lambda layer that uses the Docker image as the source. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the Lambda layer.

upvoted 2 times

✉ **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: B

Lambda layers to package the common code and save it in ECR as a docker image and refer it from actual lambda function.

By using Lambda Layers, the shared libraries and custom classes can be reused across multiple Lambda functions, simplifying the deployment and management of the serverless API. The Lambda Layer can also be versioned, making it easy to update and manage changes to the shared code.

Additionally, the use of Lambda Layers can help reduce the size of the Lambda function packages, which can result in faster deployment times and lower costs.

upvoted 4 times

Question #157

Topic 1

A manufacturing company is building an inspection solution for its factory. The company has IP cameras at the end of each assembly line. The company has used Amazon SageMaker to train a machine learning (ML) model to identify common defects from still images.

The company wants to provide local feedback to factory workers when a defect is detected. The company must be able to provide this feedback even if the factory's internet connectivity is down. The company has a local Linux server that hosts an API that provides local feedback to the workers.

How should the company deploy the ML model to meet these requirements?

- A. Set up an Amazon Kinesis video stream from each IP camera to AWS. Use Amazon EC2 instances to take still images of the streams. Upload the images to an Amazon S3 bucket. Deploy a SageMaker endpoint with the ML model. Invoke an AWS Lambda function to call the inference endpoint when new images are uploaded. Configure the Lambda function to call the local API when a defect is detected.
- B. Deploy AWS IoT Greengrass on the local server. Deploy the ML model to the Greengrass server. Create a Greengrass component to take still images from the cameras and run inference. Configure the component to call the local API when a defect is detected.
- C. Order an AWS Snowball device. Deploy a SageMaker endpoint the ML model and an Amazon EC2 instance on the Snowball device. Take still images from the cameras. Run inference from the EC2 instance. Configure the instance to call the local API when a defect is detected.
- D. Deploy Amazon Monitron devices on each IP camera. Deploy an Amazon Monitron Gateway on premises. Deploy the ML model to the Amazon Monitron devices. Use Amazon Monitron health state alarms to call the local API from an AWS Lambda function when a defect is detected.

 **God_Is_Love** Highly Voted  6 months, 2 weeks ago

Selected Answer: B

Offline operation: AWS IoT Greengrass supports offline operation by enabling devices to continue processing data even when they are disconnected from the internet.

upvoted 11 times

 **dkcloudguru** Most Recent  2 weeks ago

Option B: Greengrass supports offline operation

upvoted 1 times

 **SK_Tyagi** 1 month, 1 week ago

Selected Answer: B

Offline = IoT Greengrass

upvoted 1 times

 **SK_Tyagi** 1 month, 1 week ago

If you can't commission your sensors
Consider the following questions.

Does the mobile phone running the Amazon Monitron App have a stable internet connection?

<https://docs.aws.amazon.com/Monitron/latest/user-guide/troubleshooting.html>

For commissioning a sensor, the mobile phone running the Amazon Monitron App should have internet connectivity.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B for offline

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

keyword = WS IoT Greengrass

upvoted 1 times

 **consultornetwork** 4 months ago

Selected Answer: B

Can't be D.

Amazon Monitron requires Internet connection.Q: Can I use Amazon Monitron when it is not connected to the AWS Region or in a disconnected environment?

A: Amazon Monitron Sensors and Gateways, and their use with the Amazon Monitron service, rely on connectivity over internet to the AWS

Region.

<https://aws.amazon.com/monitron/faqs/>

Amazon Monitron Sensors and Gateways are not designed for disconnected operations or environments with no connectivity. We recommend that customers have highly available internet connectivity.

upvoted 2 times

✉ **Diego1414** 4 months, 2 weeks ago

Selected Answer: B

AWS IoT Greengrass is software that extends cloud capabilities to local devices. This enables devices to collect and analyze data closer to the source of information, react autonomously to local events, and communicate securely with each other on local networks. Local devices can also communicate securely with AWS IoT Core and export IoT data to the AWS Cloud. AWS IoT Greengrass developers can use AWS Lambda functions and prebuilt connectors to create serverless applications that are deployed to devices for local execution.

upvoted 1 times

✉ **mfsec** 6 months ago

Selected Answer: B

The ML model is run locally, so it can still provide feedback when the internet is down.

upvoted 3 times

✉ **hobokabobo** 6 months, 2 weeks ago

Selected Answer: D

Quote "The company must be able to provide this feedback even if the factory's internet connectivity is down"

So everything that needs internet can be ignored. Leaves D.

While there is a lot of garbage text about how they process date with SargeMaker, the question only asks for a solution to detect failures in the equipment. Amazon Monitron does this plus it can work even when internet is down.

All other options provide solutions for things, the question didn't ask for and/or already in place and need internet.

upvoted 1 times

✉ **Appon** 7 months, 2 weeks ago

Selected Answer: B

<https://aws.amazon.com/blogs/machine-learning/anomaly-detection-with-amazon-sagemaker-edge-manager-using-aws-iot-greengrass-v2/>

upvoted 3 times

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

Selected Answer: B

The point is how to offload ML workloads to the local.

upvoted 2 times

✉ **Musk** 7 months, 2 weeks ago

Selected Answer: B

Monitron is something different

upvoted 1 times

✉ **bititan** 7 months, 3 weeks ago

Selected Answer: B

this is taking about detecting defects from an image that is taken from a camera. I would go for running a ML model on IoT greengras pc and transfer it to IoT core, then store it in s3 bucket, which can be called by api function via lambda to send it to users.
option D would monitor only sensor data of machines.

upvoted 4 times

✉ **schalke04** 7 months, 3 weeks ago

Selected Answer: D

Amazon Monitron is a machine-learning based end-to-end condition monitoring system that detects potential failures within equipment. You can use it to implement a predictive maintenance program and reduce lost productivity from unplanned machine downtime. Amazon Monitron includes purpose-built sensors to capture vibration and temperature data, as well as gateways to automatically transfer data to the AWS Cloud. It also comes with an application in two versions. The mobile application handles system setup, analytics, and notification when tracking equipment conditions. The web application provides all the same functions as the mobile app except setup. Reliability managers can quickly deploy Amazon Monitron to track the machine health of industrial equipment, such as such as bearings, motors, gearboxes, and pumps, without any development work or specialized training.

upvoted 2 times

✉ **schalke04** 7 months, 3 weeks ago

B is wrong, D is correct.

upvoted 2 times

✉ **schalke04** 7 months, 3 weeks ago

B is correct.

AWS IoT Greengrass enables ML inference locally using models that are created, trained, and optimized in the cloud using Amazon SageMaker, AWS Deep Learning AMI, or AWS Deep Learning Containers, and deployed on the edge devices

upvoted 2 times

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

when do you take the exam man i would like to see if everything is still valid after you test

upvoted 1 times

Question #158

Topic 1

A solutions architect must create a business case for migration of a company's on-premises data center to the AWS Cloud. The solutions architect will use a configuration management database (CMDB) export of all the company's servers to create the case.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Well-Architected Tool to import the CMDB data to perform an analysis and generate recommendations.
- B. Use Migration Evaluator to perform an analysis. Use the data import template to upload the data from the CMDB export.
- C. Implement resource matching rules. Use the CMDB export and the AWS Price List Bulk API to query CMDB data against AWS services in bulk.
- D. Use AWS Application Discovery Service to import the CMDB data to perform an analysis.

 **ZZ5** Highly Voted 7 months, 3 weeks ago

B

<https://aws.amazon.com/blogs/architecture/accelerating-your-migration-to-aws/>

Build a business case with AWS Migration Evaluator

The foundation for a successful migration starts with a defined business objective (for example, growth or new offerings). In order to enable the business drivers, the established business case must then be aligned to a technical capability (increased security and elasticity). AWS Migration Evaluator (formerly known as TSO Logic) can help you meet these objectives.

To get started, you can choose to upload exports from third-party tools such as Configuration Management Database (CMDB) or install a collector agent to monitor. You will receive an assessment after data collection, which includes a projected cost estimate and savings of running your on-premises workloads in the AWS Cloud. This estimate will provide a summary of the projected costs to re-host on AWS based on usage patterns. It will show the breakdown of costs by infrastructure and software licenses. With this information, you can make the business case and plan next steps.

upvoted 10 times

 **God_Is_Love** Highly Voted 6 months, 2 weeks ago

Selected Answer: B

The AWS Migration Evaluator works by analyzing data about your current on-premises environment, including servers, storage, networking, and applications. It then provides a report that outlines the recommended AWS services and configurations that best match your existing infrastructure and applications. This report includes a detailed cost analysis that estimates the total cost of running your applications in the AWS cloud.

upvoted 6 times

 **duriselvan** Most Recent 1 week, 1 day ago

<https://www.youtube.com/watch?v=2qautbhuJC8>

upvoted 1 times

 **Jonalb** 2 months, 2 weeks ago

Selected Answer: D

D

This tools for Analytics data : <https://aws.amazon.com/pt/migration-evaluator/>
Migration data or vm : <https://aws.amazon.com/pt/application-discovery/faqs/>

upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B - use case for ME

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

Question say : Migration

then Answer is : Migration Evaluator and other respond in this comments

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: B

B is the best fit

upvoted 3 times

 **kiran15789** 7 months ago

Selected Answer: B

Migration Evaluator is a complimentary service to create data-driven assessments and business cases for AWS cloud planning and migration.

upvoted 2 times

✉  **saurabh1805** 7 months ago

Selected Answer: B

B is right answer

upvoted 2 times

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

Selected Answer: B

B

Free service, focus on cost of migration

upvoted 2 times

✉  **spd** 7 months, 2 weeks ago

Selected Answer: B

B - Evaluator

upvoted 2 times

✉  **moota** 7 months, 2 weeks ago

Selected Answer: B

The big hint is business case. So Migration Evaluator.

upvoted 2 times

✉  **Musk** 7 months, 2 weeks ago

Selected Answer: B

I think it's B, which is free, while D requires servers.

upvoted 2 times

✉  **schalke04** 7 months, 3 weeks ago

Selected Answer: D

D

<https://aws.amazon.com/application-discovery/>

upvoted 2 times

✉  **schalke04** 7 months, 3 weeks ago

B is correct.

upvoted 1 times

Question #159

Topic 1

A company has a website that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB is associated with an AWS WAF web ACL.

The website often encounters attacks in the application layer. The attacks produce sudden and significant increases in traffic on the application server. The access logs show that each attack originates from different IP addresses. A solutions architect needs to implement a solution to mitigate these attacks.

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

- A. Create an Amazon CloudWatch alarm that monitors server access. Set a threshold based on access by IP address. Configure an alarm action that adds the IP address to the web ACL's deny list.
- B. Deploy AWS Shield Advanced in addition to AWS WAF. Add the ALB as a protected resource.
- C. Create an Amazon CloudWatch alarm that monitors user IP addresses. Set a threshold based on access by IP address. Configure the alarm to invoke an AWS Lambda function to add a deny rule in the application server's subnet route table for any IP addresses that activate the alarm.
- D. Inspect access logs to find a pattern of IP addresses that launched the attacks. Use an Amazon Route 53 geolocation routing policy to deny traffic from the countries that host those IP addresses.

 **God_Is_Love** Highly Voted  6 months, 2 weeks ago

Selected Answer: B

AWS Shield Advanced is focused on protecting against DDoS attacks, while AWS WAF is focused on protecting against web exploits. However, both services can be used together to provide comprehensive protection for your applications.

upvoted 7 times

 **SK_Tyagi** Most Recent  1 month, 1 week ago

Selected Answer: B

"Least" Operational Overhead - B

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B 100%

upvoted 1 times

 **SkyZeroZx** 3 months, 2 weeks ago

Selected Answer: B

Research more information and correct my answer

Letter B with this information

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-app-layer-protections.html>

upvoted 1 times

 **SkyZeroZx** 4 months ago

Selected Answer: A

For me it would be the letter A

Because AWS Shield Advanced is for DDOS attacks that happen at layer 3.

However, in the question they say attacks in the application layer

"The website often encounters attacks in the application layer."

For this reason, I would consider that it cannot be B and A would be a more feasible solution.

If anyone has more data, welcome to improve the community

Attached answer from Bard from Google

Here are some additional details about each solution:

upvoted 2 times

 **SkyZeroZx** 4 months ago

Solution C: This solution would require creating an AWS Lambda function, which is a paid service. AWS Lambda is a serverless compute service that allows you to run code without provisioning or managing servers. The Lambda function would be used to inspect access logs and identify IP addresses that are launching attacks. The function would then add those IP addresses to the application server's subnet route table, which would prevent traffic from those IP addresses from reaching the application server.

upvoted 1 times

 **SkyZeroZx** 4 months ago

Solution A: This solution is the most efficient because it uses existing AWS services and does not require any additional infrastructure. The CloudWatch alarm will monitor server access and trigger an action when the threshold is reached. The action can be configured to add the IP address to the web ACL's deny list, which will prevent traffic from that IP address from reaching the application server.

Solution B: This solution would require deploying AWS Shield Advanced, which is a paid service. AWS Shield Advanced provides additional protection against DDoS attacks, including application layer attacks. However, it is more expensive than AWS WAF.

upvoted 1 times

 **SkyZeroZx** 4 months ago

Solution D: This solution would require inspecting access logs, which can be a time-consuming process. The access logs would be used to find a pattern of IP addresses that launched the attacks. The IP addresses could then be used to create a geolocation routing policy in Amazon Route 53. The geolocation routing policy would deny traffic from the countries that host those IP addresses.

Overall, solution A is the most efficient solution because it uses existing AWS services and does not require any additional infrastructure.

upvoted 1 times

 **dev112233xx** 5 months, 2 weeks ago

Selected Answer: B

"with the LEAST operational overhead" is AWS SHIELD Advanced without doubts 

upvoted 2 times

 **hpipt** 5 months, 4 weeks ago

Selected Answer: B

B 100% AWS SHIELD

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: B

Deploy AWS Shield Advanced in addition to AWS WAF.

upvoted 2 times

 **rtgfdv3** 7 months ago

as long as i know or think to know, shield advanced, does nothing by default and needs to be configured.

<https://docs.aws.amazon.com/waf/latest/developerguide/enable-ddos-prem.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/getting-started-ddos.html>

Note

Shield Advanced doesn't automatically protect your resources after you subscribe. You must specify the resources you want Shield Advanced to protect configure the protections.

upvoted 2 times

 **moota** 7 months, 2 weeks ago

Selected Answer: B

According to ChatGPT, the ff are what you get with Advanced over Basic.

AWS Shield Advanced is a paid version of the service that provides additional protection against large scale and sophisticated DDoS attacks. This version includes all the features of the Basic version, but with additional capabilities such as 24/7 availability, a dedicated DDoS response team, and advanced attack analytics and reporting. Additionally, AWS Shield Advanced provides access to advanced DDoS protection and mitigation capabilities, such as the ability to customize protections for specific application requirements, and to mitigate attacks more quickly and effectively.

upvoted 3 times

 **Musk** 7 months, 2 weeks ago

Selected Answer: B

Reading more about option B, I pick B

upvoted 4 times

 **Musk** 7 months, 2 weeks ago

Not sure. With WAF you get Shield, which hs DDoS. Not sure the the Shield dvnced gives you much more.

upvoted 1 times

 **schalke04** 7 months, 3 weeks ago

Selected Answer: B

AWS Shield is a managed distributed denial of service (DDoS) protection service that safeguards applications running on AWS. It provides dynamic detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield: Standard and Advanced.

upvoted 4 times

Question #160

Topic 1

A company has a critical application in which the data tier is deployed in a single AWS Region. The data tier uses an Amazon DynamoDB table and an Amazon Aurora MySQL DB cluster. The current Aurora MySQL engine version supports a global database. The application tier is already deployed in two Regions.

Company policy states that critical applications must have application tier components and data tier components deployed across two Regions. The RTO and RPO must be no more than a few minutes each. A solutions architect must recommend a solution to make the data tier compliant with company policy.

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

- A. Add another Region to the Aurora MySQL DB cluster
- B. Add another Region to each table in the Aurora MySQL DB cluster
- C. Set up scheduled cross-Region backups for the DynamoDB table and the Aurora MySQL DB cluster
- D. Convert the existing DynamoDB table to a global table by adding another Region to its configuration
- E. Use Amazon Route 53 Application Recovery Controller to automate database backup and recovery to the secondary Region

 **SK_Tyagi** 1 month, 1 week ago

Selected Answer: AD

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

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: AD

its AD

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: AD

For DynamoDB use global table, for Aurora use cross-region read-replicas.

upvoted 1 times

 **easytoo** 3 months, 1 week ago

a-d-a-d-a-d-a-d-a-d

upvoted 1 times

 **Roontha** 3 months, 3 weeks ago

Answer : A, D

<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html>

upvoted 1 times

 **taer** 6 months, 1 week ago

Selected Answer: AD

A. Add another Region to the Aurora MySQL DB cluster

D. Convert the existing DynamoDB table to a global table by adding another Region to its configuration

upvoted 4 times

 **testingaws123** 6 months, 1 week ago

Badly written question:

"The RTO and RPO must be no more than a few minutes each."

What is few minutes mean? May be it is 2-3 min for me, may be it is 9-10 min for you.

upvoted 4 times

 **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: AC

A solves multi region for DB layer. but question also asks for minimum RPO and RTO which means quick uptime of application in case of failure which is possible with backups.

<https://aws.amazon.com/blogs/database/cost-effective-disaster-recovery-for-amazon-aurora-databases-using-aws-backup/>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/CrossRegionAccountCopyAWS.html>

upvoted 3 times

 **SK_Tyagi** 1 month, 1 week ago

Why use C and do replication with multiple steps when Global Tables support it

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

upvoted 1 times

 **God_Is_Love** 6 months, 2 weeks ago

Hint given is - Aurora MySQL engine version supports a global database which makes this possible -

<https://d2908q01vomqb2.cloudfront.net/887309d048beef83ad3eabf2a79a64a389ab1c9f/2021/03/08/Aurora-Global-database-2.jpg>

upvoted 3 times

 **schalke04** 7 months, 3 weeks ago

Selected Answer: AD

A and D

upvoted 4 times

 **bititan** 7 months, 3 weeks ago

Selected Answer: AD

you can create only db's not global tables, hence A and D

upvoted 4 times

Question #161

Topic 1

A telecommunications company is running an application on AWS. The company has set up an AWS Direct Connect connection between the company's on-premises data center and AWS. The company deployed the application on Amazon EC2 instances in multiple Availability Zones behind an internal Application Load Balancer (ALB). The company's clients connect from the on-premises network by using HTTPS. The TLS terminates in the ALB. The company has multiple target groups and uses path-based routing to forward requests based on the URL path.

The company is planning to deploy an on-premises firewall appliance with an allow list that is based on IP address. A solutions architect must develop a solution to allow traffic flow to AWS from the on-premises network so that the clients can continue to access the application.

Which solution will meet these requirements?

- A. Configure the existing ALB to use static IP addresses. Assign IP addresses in multiple Availability Zones to the ALB. Add the ALB IP addresses to the firewall appliance.
- B. Create a Network Load Balancer (NLB). Associate the NLB with one static IP address in multiple Availability Zones. Create an ALB-type target group for the NLB and add the existing ALB IP addresses to the firewall appliance. Update the clients to connect to the NLB.
- C. Create a Network Load Balancer (NLB). Associate the NLB with one static IP address in multiple Availability Zones. Add the existing target groups to the NLB. Update the clients to connect to the NLB. Delete the ALB. Add the NLB IP addresses to the firewall appliance.
- D. Create a Gateway Load Balancer (GWLB). Assign static IP addresses to the GWLB in multiple Availability Zones. Create an ALB-type target group for the GWLB and add the existing ALB. Add the GWLB IP addresses to the firewall appliance. Update the clients to connect to the GWLB.

 **Untamables** Highly Voted  7 months, 2 weeks ago

Selected Answer: B

The background is the below.

- The company is using ALB features and must keep them.
 - The new on-premise firewall needs a static IP address of the ALB as the next hop.
 - However, ALB cannot have a static IP address.
- So the point is how ALB can have a static IP address endpoint.

Solution

<https://aws.amazon.com/premiumsupport/knowledge-center/alb-static-ip/>

upvoted 10 times

 **jojom19980** Highly Voted  7 months, 3 weeks ago

Selected Answer: B

it uses path-based routing to forward requests based on the URL path

upvoted 6 times

 **Gabehcoud** Most Recent  1 month, 2 weeks ago

Option B says "ALAdd" what is AL add? I see this very often. Can someone help to explain?

Create an ALB-type target group for the NLB and add the existing ALB IP addresses to the firewall appliance. Update the clients to connect to the NLB.

upvoted 1 times

 **khksoma** 2 months, 1 week ago

A Gateway Load Balancer endpoint is a VPC endpoint that provides private connectivity between virtual appliances in the service provider VPC, and application servers in the service consumer VPC. The Gateway Load Balancer is deployed in the same VPC as that of the virtual appliances. These appliances are registered as a target group of the Gateway Load Balancer.

Since the firewall is deployed on-prem I dont think D is a viable option

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B

need to keep ALB behind NLB for path routing

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: B

Since ALB does not support static IP addresses by design then we need to use NLB before the ALB or instead. However, since we are heavily utilizing the application layer of the OSI then we cannot use NLB directly. Hence B remains the only choice

upvoted 1 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

ALB's cannot use static IP's. NLB's have static IP's , addicinally need based on the URL path use ALB then B is more apropiate

upvoted 1 times

 **rbm2023** 4 months, 1 week ago

Selected Answer: B

I agree with B. since clients need access to the ALB using a private connection between on premises and AWS. The firewall which is inside company data center operates at network level but we cannot lose ALB due to many path based routing. So we need something like this:

<https://www.scalefactory.com/blog/2021/12/13/aws-network-load-balancers-new-features/>

<https://www.scalefactory.com/blog/2021/12/13/aws-network-load-balancers-new-features/img/now-firewall-egress.png>

and this:

<https://aws.amazon.com/blogs/networking-and-content-delivery/application-load-balancer-type-target-group-for-network-load-balancer/>

upvoted 2 times

 **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/>

Gateway Load Balancer helps you easily deploy, scale, and manage your third-party virtual appliances. It gives you one gateway for distributing traffic across multiple virtual appliances while scaling them up or down, based on demand. This decreases potential points of failure in your network and increases availability.

upvoted 1 times

 **God_Is_Love** 6 months, 2 weeks ago

https://youtu.be/-j2smz_VCH4?t=1270

ALB (L7)- HTTP, HTTPS

NLB (L4)- TCP, UDP, TLS traffic

GWLB(L3)- IP traffic and 3rd party Appliances

upvoted 2 times

 **God_Is_Love** 6 months, 2 weeks ago

AWS Gateway Load Balancer (GWLB) can terminate TLS traffic. GWLB supports SSL/TLS offloading, which means that it can terminate SSL/TLS connections from clients and then forward the decrypted traffic to backend servers over HTTP or HTTPS.

upvoted 1 times

 **Mickey321** 6 months ago

I think main question is can it support static IP address which is needed by the firmware to waitlist it?

upvoted 1 times

 **Sarutobi** 6 months, 3 weeks ago

Selected Answer: B

The question is confusing. If I understood this question correctly, I do this almost every day, and I don't use those terms. Basically, the solution is inserting an NLB in front of the existing ALB, so traffic is Client->FW->NLB->ALB->EC2. Another point is that fixing the public IP address makes a lot of sense, but not the private one, like in this case. Every time you create an ALB 2 or more ENI are created and you have the IP addresses there.

upvoted 4 times

 **dummy1777** 7 months ago

B. Create a Network Load Balancer (NLB). Associate the NLB with one static IP address in multiple Availability Zones. Create an ALB-type target group for the NLB and add the existing ALB. Add the NLB IP address to the firewall appliance. Update the clients to connect to the NLB.

In this solution, the company would create a new Network Load Balancer (NLB) and associate it with a single static IP address in multiple Availability Zones. The NLB would then be configured with an ALB-type target group and the existing ALB would be added to this target group. The IP address of the NLB would be added to the on-premises firewall appliance, and the clients would be updated to connect to the NLB.

This solution allows the on-premises firewall to whitelist the IP address of the NLB, which is a fixed, predictable address that can be easily identified and managed by the firewall appliance. Additionally, the NLB provides higher network throughput and lower latency than an ALB, which may be beneficial for the application's performance.

upvoted 2 times

 **Musk** 7 months, 2 weeks ago

Selected Answer: B

Sure about this one.

upvoted 2 times

 **masssa** 7 months, 3 weeks ago

<https://aws.amazon.com/jp/premiumsupport/knowledge-center/alb-static-ip/>

ALB cannnot use static ip, so it must be set NLB in front of ALB.

Correct answer is C.

upvoted 2 times

 **masssa** 7 months ago

miss type.

correct answer is B.

There is no need to delete ALB.

upvoted 1 times

 **bititan** 7 months, 3 weeks ago

Selected Answer: C

ALB's cannot use static IP's. NLB's have static IP's

upvoted 1 times

 **jojom19980** 7 months, 3 weeks ago

No should be B cause it uses path-based routing to forward requests based on the URL path

upvoted 3 times

Question #162

Topic 1

A company runs an application on a fleet of Amazon EC2 instances that are in private subnets behind an internet-facing Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. An AWS WAF web ACL that contains various AWS managed rules is associated with the CloudFront distribution.

The company needs a solution that will prevent internet traffic from directly accessing the ALB.

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

- A. Create a new web ACL that contains the same rules that the existing web ACL contains. Associate the new web ACL with the ALB.
- B. Associate the existing web ACL with the ALB.
- C. Add a security group rule to the ALB to allow traffic from the AWS managed prefix list for CloudFront only.
- D. Add a security group rule to the ALB to allow only the various CloudFront IP address ranges.

 **masssa**  7 months, 3 weeks ago

Selected Answer: C

https://docs.amazonaws.cn/en_us/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html
AWS managed prefix list is more recommended.

upvoted 6 times

 **NikkyDicky**  2 months, 3 weeks ago

Selected Answer: C

C for sure

upvoted 1 times

 **rbm2023** 4 months, 1 week ago

Selected Answer: C

https://docs.amazonaws.cn/en_us/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html
If your origin is hosted on Amazon and protected by an Amazon VPC security group, you can use the CloudFront managed prefix list to allow inbound traffic to your origin only from CloudFront's origin-facing servers, preventing any non-CloudFront traffic from reaching your origin , imagine that your origin is an Amazon EC2 instance in the Europe (London) Region (eu-west-2). If the instance is in a VPC, you can create a security group rule that allows inbound HTTPS access from the CloudFront managed prefix list. This allows all of CloudFront's global origin-facing servers to reach the instance. If you remove all other inbound rules from the security group, you prevent any non-CloudFront traffic from reaching the instance

upvoted 2 times

 **mfsec** 6 months ago

C. Add a security group rule to the ALB to allow traffic from the AWS managed prefix list for CloudFront only.

upvoted 1 times

 **ExamTopix01** 7 months, 3 weeks ago

C <https://aws.amazon.com/blogs/news/limit-access-to-your-origins-using-the-aws-managed-prefix-list-for-amazon-cloudfront/>

upvoted 2 times

 **jojom19980** 7 months, 3 weeks ago

Selected Answer: C

<https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-cloudfront-managed-prefix-list/>

upvoted 2 times

Question #163

Topic 1

A company is running an application that uses an Amazon ElastiCache for Redis cluster as a caching layer. A recent security audit revealed that the company has configured encryption at rest for ElastiCache. However, the company did not configure ElastiCache to use encryption in transit. Additionally, users can access the cache without authentication.

A solutions architect must make changes to require user authentication and to ensure that the company is using end-to-end encryption.

Which solution will meet these requirements?

- A. Create an AUTH token. Store the token in AWS System Manager Parameter Store, as an encrypted parameter. Create a new cluster with AUTH, and configure encryption in transit. Update the application to retrieve the AUTH token from Parameter Store when necessary and to use the AUTH token for authentication.
- B. Create an AUTH token. Store the token in AWS Secrets Manager. Configure the existing cluster to use the AUTH token, and configure encryption in transit. Update the application to retrieve the AUTH token from Secrets Manager when necessary and to use the AUTH token for authentication.
- C. Create an SSL certificate. Store the certificate in AWS Secrets Manager. Create a new cluster, and configure encryption in transit. Update the application to retrieve the SSL certificate from Secrets Manager when necessary and to use the certificate for authentication.
- D. Create an SSL certificate. Store the certificate in AWS Systems Manager Parameter Store, as an encrypted advanced parameter. Update the existing cluster to configure encryption in transit. Update the application to retrieve the SSL certificate from Parameter Store when necessary and to use the certificate for authentication.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B, per redis docs.
EC encr in transit is a config option
upvoted 1 times

 **easytoo** 3 months, 1 week ago

b-b-b-b-b-b-b

Creating an AUTH token provides a form of authentication for accessing the ElastiCache cluster.
Storing the AUTH token in AWS Secrets Manager ensures secure and centralized management of the token.
Configuring the existing ElastiCache cluster to use the AUTH token enables authentication for accessing the cache.
Enabling encryption in transit ensures that data is encrypted when it is transferred between the client and the ElastiCache cluster.
Updating the application to retrieve the AUTH token from Secrets Manager and use it for authentication ensures that only authorized users can access the cache.
upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: B

Create an AUTH token. Store the token in AWS Secrets Manager.
upvoted 1 times

 **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: B

Redis CLI has AUTH command as a feature to SET/ROTATE strategies
<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>
upvoted 2 times

 **Zek** 6 months, 3 weeks ago

B seems right.
To enable authentication on an existing Redis server, call the ModifyReplicationGroup API operation. Call ModifyReplicationGroup with the --auth-token parameter as the new token and the --auth-token-update-strategy with the value ROTATE.

After the modification is complete, the cluster supports the AUTH token specified in the auth-token parameter in addition to supporting connecting without authentication. Enabling authentication is only supported on Redis servers with encryption in transit (TLS) enabled.

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>
upvoted 2 times

 **spd** 7 months, 2 weeks ago

Selected Answer: B

As per <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/in-transit-encryption.html>
upvoted 2 times

 **harleydog** 7 months, 3 weeks ago

You have to create a new cluster, otherwise the the cluster supports the AUTH token specified and supports connecting without authentication.
upvoted 1 times

 **jojom19980** 7 months, 3 weeks ago

Selected Answer: B

Previously, you needed to set up authentication for ElastiCache for Redis clusters using Redis user passwords or store the password in AWS Secrets Manager or on a third-party secrets management tool. However, in large organizations that host many applications, passwords can often become out of sync when it comes time to rotate the password. IAM authentication provides a streamlined security posture by allowing access management from a centralized service. With IAM authentication, ElastiCache users can use their IAM identities when connecting to their Redis clusters

upvoted 1 times

 **bititan** 7 months, 3 weeks ago

Selected Answer: B

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

upvoted 1 times

Question #164

Topic 1

A company is running a compute workload by using Amazon EC2 Spot Instances that are in an Auto Scaling group. The launch template uses two placement groups and a single instance type.

Recently, a monitoring system reported Auto Scaling instance launch failures that correlated with longer wait times for system users. The company needs to improve the overall reliability of the workload.

Which solution will meet this requirement?

- A. Replace the launch template with a launch configuration to use an Auto Scaling group that uses attribute-based instance type selection.
- B. Create a new launch template version that uses attribute-based instance type selection. Configure the Auto Scaling group to use the new launch template version.
- C. Update the launch template Auto Scaling group to increase the number of placement groups.
- D. Update the launch template to use a larger instance type.

 **bititan** Highly Voted 7 months, 3 weeks ago

Selected Answer: B

launch config is replaced by launch template hence is not advisable, option A ruled out. C is wrong because launch template cannot be updated. D is also wrong for the same reason

upvoted 6 times

 **Simon523** Most Recent 1 month ago

Selected Answer: B

As an alternative to manually specifying the instance types, you can specify the attributes that an instance must have, and Amazon EC2 will identify all the instance types with those attributes.

This is known as attribute-based instance type selection.

For example, you can specify the minimum and maximum number of vCPUs required for your instances, and EC2 Fleet will launch the instances using any available instance types that meet those vCPU requirements.

upvoted 1 times

 **rl97** 2 months ago

B

Amazon EC2 Auto Scaling can select from a wide range of instance types for launching Spot Instances. This meets the Spot best practice of being flexible about instance types, which gives the Amazon EC2 Spot service a better chance of finding and allocating your required amount of compute capacity.

upvoted 1 times

 **Christina666** 2 months, 2 weeks ago

Selected Answer: B

key word "spot instance launch failure"-> attribute based selection

upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

its a b

upvoted 1 times

 **easystoo** 3 months, 1 week ago

b-b-b-b-bb-b-

Creating a new launch template version allows for making changes to the template without disrupting the existing instances.

Using attribute-based instance type selection enables the Auto Scaling group to automatically select the most suitable instance type based on the defined attributes, such as availability zone, instance family, or instance size.

By leveraging attribute-based instance type selection, the Auto Scaling group can adapt to changing Spot Instance availability and launch instances in zones with higher availability, reducing launch failures.

Updating the launch template with this new version ensures that new instances launched by the Auto Scaling group utilize the improved instance selection process, thereby enhancing reliability.

upvoted 4 times

 **mfsec** 6 months ago

Selected Answer: B

B. Create a new launch template version that uses attribute-based instance type selection.

upvoted 2 times

 **Roontha** 4 months ago

Agreed with B

upvoted 1 times

 **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg-instance-type-requirements.html#use-attribute-based-instance-type-selection-prerequisites>

upvoted 1 times

 **kiran15789** 7 months ago

Selected Answer: B

Confused between B and D , will choose B

upvoted 1 times

 **saurabh1805** 7 months ago

Selected Answer: B

b is correct

<https://aws.amazon.com/blogs/aws/new-attribute-based-instance-type-selection-for-ec2-auto-scaling-and-ec2-fleet/>

upvoted 2 times

 **etechsystem_ts** 7 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

Question #165

Topic 1

A company is migrating a document processing workload to AWS. The company has updated many applications to natively use the Amazon S3 API to store, retrieve, and modify documents that a processing server generates at a rate of approximately 5 documents every second. After the document processing is finished, customers can download the documents directly from Amazon S3.

During the migration, the company discovered that it could not immediately update the processing server that generates many documents to support the S3 API. The server runs on Linux and requires fast local access to the files that the server generates and modifies. When the server finishes processing, the files must be available to the public for download within 30 minutes.

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

- A. Migrate the application to an AWS Lambda function. Use the AWS SDK for Java to generate, modify, and access the files that the company stores directly in Amazon S3.
- B. Set up an Amazon S3 File Gateway and configure a file share that is linked to the document store. Mount the file share on an Amazon EC2 instance by using NFS. When changes occur in Amazon S3, initiate a RefreshCache API call to update the S3 File Gateway.
- C. Configure Amazon FSx for Lustre with an import and export policy. Link the new file system to an S3 bucket. Install the Lustre client and mount the document store to an Amazon EC2 instance by using NFS.
- D. Configure AWS DataSync to connect to an Amazon EC2 instance. Configure a task to synchronize the generated files to and from Amazon S3.

 **schalke04** Highly Voted 7 months, 3 weeks ago

Selected Answer: C

C:

Amazon FSx for Lustre is a fully managed service that provides cost-effective, high-performance, scalable storage for compute workloads. Powered by Lustre, the world's most popular high-performance file system, FSx for Lustre offers shared storage with sub-ms latencies, up to terabytes per second of throughput, and millions of IOPS. FSx for Lustre file systems can also be linked to Amazon Simple Storage Service (S3) buckets, allowing you to access and process data concurrently from both a high-performance file system and from the S3 API.

upvoted 19 times

 **rbm2023** 4 months ago

I disagree with option C. This is an example of how to mount a Lustre from an EC2 Linux system. It does not use NFS
`sudo mount -t lustre <fsx-dns-name>@tcp:<mount-point>`

Amazon FSx for Lustre provides its own Lustre-specific mount command and protocol for mounting the file system on Linux instances. The lustre file system type in the mount command indicates that it is specifically for mounting Lustre-based file systems, such as Amazon FSx for Lustre.

I would still go for option B

upvoted 5 times

 **lxrdm** 2 months, 3 weeks ago

I wouldnt choose Lustre.. would only pick it if its related to HPC (high performance computing), the amount of files generated here is nothing..
 upvoted 2 times

 **dev112233xx** Highly Voted 5 months, 2 weeks ago

Selected Answer: B

B is correct imo

C is incorrect, FSx for Lustre doesn't support NFS protocol

It actually support only POSIX protocol:

Custom (POSIX-compliant) protocol optimized for performance

upvoted 15 times

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

Selected Answer: B

The server is running Linux, How can we use Fsx?

upvoted 3 times

 **chikorita** 3 weeks, 2 days ago

FSX for Lustre is for Linux and does not support Windows

upvoted 2 times

 **CloudHandsOn** 3 weeks, 6 days ago

Selected Answer: B

I believe that B is correct, given that Lustre does not support NFS (it supports POSIX)

upvoted 2 times

 **xav1er** 1 month, 1 week ago

Selected Answer: B

B as file gateway seems simple working solution for this. Lustre does not support NFS and might be an overkill for this solution - its primary used for HPC clusters. DataSync is rather for batch daad migrations and periodic data migration jobs, isn't it?

upvoted 3 times

 **softarts** 1 month, 3 weeks ago

Selected Answer: B

don't understand the question and answer, include B&C. how does it mount to EC2 by using NFS? I think the processing server is running on Premise??

upvoted 1 times

 **ggrodskiy** 2 months ago

Correct D.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B works

C would be better if not for NFS mention

upvoted 1 times

 **PhuocT** 3 months ago

Selected Answer: C

C

<https://docs.aws.amazon.com/fsx/latest/LustreGuide/mount-fs-auto-mount-onreboot.html>

upvoted 1 times

 **PhuocT** 3 months ago

change to B, Lustre does not support NFS mount.

upvoted 1 times

 **easytoo** 3 months, 1 week ago

d-d-d-d-d-d-d-d-d-d

AWS DataSync is a fully-managed service that can be used to synchronize data between on-premises storage and AWS storage services. In this case, AWS DataSync could be used to synchronize the files that the processing server generates and modifies to Amazon S3. Once the files are in Amazon S3, they can be made available to the public for download within 30 minutes.

Therefore, the best solution is to configure AWS DataSync to connect to an Amazon EC2 instance and configure a task to synchronize the generated files to and from Amazon S3. This option would require the least amount of effort and would still meet the company's requirements.

upvoted 2 times

 **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

B. Least amount of effort and it supports NFS which Lustre does not.

upvoted 1 times

 **Bwutch** 4 months ago

he correct answer would be D. Configure AWS DataSync to connect to an Amazon EC2 instance. Configure a task to synchronize the generated files to and from Amazon S3.

This is because AWS DataSync automates and accelerates moving and synchronizing data between on-premises storage and AWS, including S3. The use case described involves a situation where the server generating the documents can't yet support the S3 API directly, and DataSync can bridge that gap by synchronizing the files between the EC2 instance (where the server can have fast local access) and S3.

The other solutions require more changes and more setup than option D, which simply requires setting up the DataSync task. The requirement is to fulfill the needs with the least amount of effort, making option D the best answer.

upvoted 2 times

 **rbm2023** 4 months ago

Selected Answer: B

Although the solution described in C is possible, there is an error at the end mentioning that you would mount the FSX using NFS which is not supported.

<https://aws.amazon.com/blogs/storage/persistent-storage-for-high-performance-workloads-using-amazon-fsx-for-lustre/>

<https://d2908q01vomqb2.cloudfront.net/e1822db470e60d090affd0956d743cb0e7cdf113/2020/04/24/FSx-for-Lustre-persistent-storage-diagram.png>

Mount the file system you created as shown below:

```
$ sudo mount -t lustre -o noatime,flock file_system_dns_name@tcp:/mountname /fsx
```

upvoted 1 times

 **Jesuisleon** 4 months, 1 week ago

Selected Answer: B

C is wrong, amazon FSx for luster does NOT suport nfs file system!

upvoted 3 times

 **intp75** 4 months, 1 week ago

Selected Answer: B

Amazon FSx for Lustre cannot be mounted using NFS so the only choice is B

upvoted 3 times

 **SVGoogle89** 4 months, 1 week ago

C

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/supported-clients-fsx.html>

upvoted 1 times

 **momo3321** 4 months, 2 weeks ago

Selected Answer: D

Guys, the question is "with the LEAST amount of effort" and the AWS DataSync is designed for data transfer and synchronization between different storage services, including EC2 instances and S3, and would provide more efficient and automated data movement for this use case, ensuring the files are available on S3 within the required 30 minutes with less operational overhead.

Is it doesn't least effort than the others?

I'll go with D

upvoted 3 times

Question #166

Topic 1

A delivery company is running a serverless solution in the AWS Cloud. The solution manages user data, delivery information, and past purchase details. The solution consists of several microservices. The central user service stores sensitive data in an Amazon DynamoDB table. Several of the other microservices store a copy of parts of the sensitive data in different storage services.

The company needs the ability to delete user information upon request. As soon as the central user service deletes a user, every other microservice must also delete its copy of the data immediately.

Which solution will meet these requirements?

- A. Activate DynamoDB Streams on the DynamoDB table. Create an AWS Lambda trigger for the DynamoDB stream that will post events about user deletion in an Amazon Simple Queue Service (Amazon SQS) queue. Configure each microservice to poll the queue and delete the user from the DynamoDB table.
- B. Set up DynamoDB event notifications on the DynamoDB table. Create an Amazon Simple Notification Service (Amazon SNS) topic as a target for the DynamoDB event notification. Configure each microservice to subscribe to the SNS topic and to delete the user from the DynamoDB table.
- C. Configure the central user service to post an event on a custom Amazon EventBridge event bus when the company deletes a user. Create an EventBridge rule for each microservice to match the user deletion event pattern and invoke logic in the microservice to delete the user from the DynamoDB table.
- D. Configure the central user service to post a message on an Amazon Simple Queue Service (Amazon SQS) queue when the company deletes a user. Configure each microservice to create an event filter on the SQS queue and to delete the user from the DynamoDB table.

 **CloudFloater** Highly Voted  7 months, 1 week ago

Selected Answer: C

C seems correct; SQS is one queue to one microservice, could not find anything on dynamodb event notifications.

upvoted 12 times

 **Untamables** Highly Voted  7 months, 2 weeks ago

Selected Answer: A

The trigger is that the central user service deletes a user in the DynamoDB table. The DynamoDB Streams meets the requirement.

<https://aws.amazon.com/blogs/database/how-to-perform-ordered-data-replication-between-applications-by-using-amazon-dynamodb-streams/>
Option B is wrong. There is no feature named DynamoDB event notifications.

upvoted 8 times

 **kjcncjek** 3 weeks, 6 days ago

how can you use 1 sqs queue for all microservices?

upvoted 1 times

 **Amac1979** 6 months ago

Correct, the point they want to make is central user service is system of record. You should not be deleting from other services until you delete from DynamoDB.

upvoted 1 times

 **vjp_training** Most Recent  1 week, 2 days ago

Selected Answer: A

https://aws.amazon.com/vi/getting-started/hands-on/send-fanout-event-notifications/?nc1=f_ls

upvoted 1 times

 **Ganshank** 1 month ago

A real-world use case utterly destroyed with some of the worst possible options for solutions.

Simplest solution is to have the interested parties consume events off the DynamoDB streams and delete the user information in their respective datastores. Too many red herrings in the options given, and the only relatively sane one of the lot is Option C.

The bar for coming up with questions with SA professional keeps getting lowered.

upvoted 1 times

 **SK_Tyagi** 1 month, 1 week ago

Selected Answer: A

Event trigger from DynamoDb -- Choose DynamoDb Streams

upvoted 1 times

 **xav1er** 1 month, 1 week ago

Where the hell is fan-out pattern? stupid answers ...

upvoted 2 times

 **aviathor** 1 month, 1 week ago

- * The central user service stores sensitive data in an Amazon DynamoDB table.
- * Several of the other microservices store a copy of parts of the sensitive data in different storage services.

Apparently only the central user service stores user data in DynamoDB. The others use "different storage services". Yet, all of the answers focus on DynamoDB...

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C

A would be preferable with SNS instead of SQS

upvoted 2 times

 **aviathor** 1 month, 1 week ago

Can you seriously mean one should "Create an EventBridge rule for each microservice to match the user deletion event pattern and invoke logic in the microservice to delete the user from the DynamoDB table."???

Why not SQS?

upvoted 1 times

 **kjcncjek** 3 weeks, 6 days ago

it should be SQSs but all answers indicates only 1 queue

upvoted 1 times

 **aviathor** 1 month, 1 week ago

Instead of configuring multiple EventBridge rules, there could be multiple SQS streams :)

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: C

No matter how I would like to use the native DynamoDB services, option A and B have some major issues - A and D expects SQS to be used by several microservices, which is not really what the service is supposed to do. B seems like a nice scenario, however, there isn't something like "DynamoDB event notifications". So we leave with option C

upvoted 2 times

 **Alabi** 3 months ago

Selected Answer: C

The solution that will meet the requirements of immediately deleting user information across all microservices is:

C. Configure the central user service to post an event on a custom Amazon EventBridge event bus when the company deletes a user. Create an EventBridge rule for each microservice to match the user deletion event pattern and invoke logic in the microservice to delete the user from the DynamoDB table.

In this case, you can create an EventBridge rule for each microservice to match the user deletion event pattern and invoke the logic in the microservice to delete the corresponding user data from their respective storage services, including the DynamoDB table.

upvoted 2 times

 **EricZhang** 3 months, 1 week ago

does DynamoDB event notifications exist?

upvoted 1 times

 **Roontha** 4 months ago

Answer : C

upvoted 1 times

 **rbm2023** 4 months ago

Selected Answer: C

I would work on this solution using streams but option A is incorrect since the stream would only occur after the deletion of the user and the option states at the end that the user would be deleted from Dynamo table, so this is in an incorrect order.

This is also a nice article using event bridge with a real world case.

<https://medium.com/aws-serverless-microservices-with-patterns-best/aws-event-driven-serverless-microservices-using-aws-lambda-api-gateway-eventbridge-sqs-dynamodb-a7f46220b738>

upvoted 1 times

 **aviathor** 1 month, 1 week ago

It also does not talk about deleting the sensitive information stored elsewhere than in DynamoDB, which I assume from the question also pertains to users

upvoted 1 times

 **DWsk** 5 months, 1 week ago

Selected Answer: C

This is a tricky one because you could definitely do this using DynamoDB Streams, as that would be the right tool for the job. But the question is trying to trick you because the second half of that answer is to use SQS which would not work when you have multiple consumers, each message can only be consumed once.

Therefore the answer has to be C

upvoted 7 times

✉ **rbm2023** 4 months ago

I agree, with the addition to the fact that every single option states that the final step is to delete the record from Dynamo, by using streams, the deletion would already occur, making option A incorrect.

upvoted 1 times

✉ **birbyne** 5 months, 3 weeks ago

Selected Answer: C

The recommended solution is to configure the central user service to post an event on a custom Amazon EventBridge event bus when the company deletes a user. Each microservice can then create an EventBridge rule that matches the user deletion event pattern and invokes logic in the microservice to delete the user from the DynamoDB table. This solution provides an easy way to coordinate between microservices and ensures that every microservice deletes its copy of the data immediately upon user deletion from the central user service. It also requires minimal effort as there is no need to set up additional services or infrastructure.

upvoted 3 times

✉ **Asagumo** 5 months, 3 weeks ago

Selected Answer: C

Sensitive user information must be deleted immediately. There is no assumption that the time required to poll the SQS queue is acceptable for this mechanism.

upvoted 2 times

✉ **mfsec** 6 months ago

Selected Answer: A

I think A is the best fit here due to the phrasing of the question around who is deleting users.

upvoted 1 times

Question #167

A company is running a web application in a VPC. The web application runs on a group of Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is using AWS WAF.

An external customer needs to connect to the web application. The company must provide IP addresses to all external customers.

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

- A. Replace the ALB with a Network Load Balancer (NLB). Assign an Elastic IP address to the NLB.
- B. Allocate an Elastic IP address. Assign the Elastic IP address to the ALB. Provide the Elastic IP address to the customer.
- C. Create an AWS Global Accelerator standard accelerator. Specify the ALB as the accelerator's endpoint. Provide the accelerator's IP addresses to the customer.
- D. Configure an Amazon CloudFront distribution. Set the ALB as the origin. Ping the distribution's DNS name to determine the distribution's public IP address. Provide the IP address to the customer.

 **Untamables** Highly Voted  7 months, 2 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.alb-accelerator.html>
Option A is wrong. AWS WAF does not support associating with NLB.

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html>
Option B is wrong. An ALB does not support an Elastic IP address.

<https://aws.amazon.com/elasticloadbalancing/features/>

upvoted 12 times

 **masssa** Highly Voted  7 months, 3 weeks ago

static IP can be made below method.

- NLB (replace NLB from ALB)
- NLB + ALB
- global accelerator + ALB
- original load balancer (ex. made by EC2 + nginx)

upvoted 8 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: C

C - basic use case for GA

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

C. Create an AWS Global Accelerator standard accelerator.

upvoted 1 times

 **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: C

An Application Load Balancer cannot be assigned an Elastic IP address (static IP address).

<https://stackoverflow.com/questions/55236806/how-to-assign-elastic-ip-to-application-load-balancer-in-aws>

upvoted 1 times

 **God_Is_Love** 6 months, 2 weeks ago

This feature allows you to migrate your applications to AWS without requiring your partners and customers to change their IP address whitelists. (which could be used in WAF)

BYOIP - Bring your own IP <https://aws.amazon.com/blogs/networking-and-content-delivery/using-bring-your-own-ip-addresses-byoip-with-global-accelerator/>

upvoted 2 times

 **kiran15789** 7 months ago

Selected Answer: C

<https://aws.amazon.com/premiumsupport/knowledge-center/alb-static-ip/>

Can assign Static IP to ALB

upvoted 1 times

 **jojom19980** 7 months, 3 weeks ago

Selected Answer: A

.....

upvoted 2 times

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

C

WAF cannot be associated with NLB

upvoted 1 times

✉ **massa** 7 months, 3 weeks ago

NLB cannot be used when WAF is used

upvoted 1 times

✉ **ExamTopix01** 7 months, 3 weeks ago

A

<https://aws.amazon.com/jp/premiumsupport/knowledge-center/alb-static-ip/>

upvoted 1 times

✉ **ExamTopix01** 7 months, 3 weeks ago

Sorry C

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.alb-accelerator.html>

upvoted 1 times

✉ **schalke04** 7 months, 3 weeks ago

This solution meets the requirement with the least operational overhead, as it only requires the allocation of an Elastic IP address, assignment to the ALB, and providing the address to the customer. The other options involve configuring additional services, which can increase operational overhead.

upvoted 1 times

✉ **bititan** 7 months, 3 weeks ago

Selected Answer: C

this option has the least admin effort. A has more admin effort, B is not possible, D will not give static IP address

upvoted 4 times

✉ **schalke04** 7 months, 3 weeks ago

Selected Answer: B

B will work

upvoted 1 times

Question #168

Topic 1

A company has a few AWS accounts for development and wants to move its production application to AWS. The company needs to enforce Amazon Elastic Block Store (Amazon EBS) encryption at rest current production accounts and future production accounts only. The company needs a solution that includes built-in blueprints and guardrails.

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

- A. Use AWS CloudFormation StackSets to deploy AWS Config rules on production accounts.
- B. Create a new AWS Control Tower landing zone in an existing developer account. Create OUs for accounts. Add production and development accounts to production and development OUs, respectively.
- C. Create a new AWS Control Tower landing zone in the company's management account. Add production and development accounts to production and development OUs, respectively.
- D. Invite existing accounts to join the organization in AWS Organizations. Create SCPs to ensure compliance.
- E. Create a guardrail from the management account to detect EBS encryption.
- F. Create a guardrail for the production OU to detect EBS encryption.

 **God_Is_Love** Highly Voted 6 months, 2 weeks ago

Selected Answer: CDF

When you enable controls on an organizational unit (OU) that is registered with AWS Control Tower, preventive controls apply to all member accounts under the OU, enrolled and unenrolled. Detective controls apply to enrolled accounts only.

<https://docs.aws.amazon.com/controlltower/latest/userguide/controls.html>

upvoted 9 times

 **bur4an** Most Recent 1 week, 6 days ago

Basically order is DCF of the setup

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: CDF

CDF for sure

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: BCF

CEF

- A) AWS Config not enforce rule
- B) Why developer account ? is incorrect is management account
- C) Sounds good
- D) SCP for enforce sounds good
- E) EBS encryption in managament account ? not only required in production
- F) encryption in production OU sounds great

upvoted 1 times

 **SkyZeroZx** 3 months ago

CDF is correct

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: BCF

<https://www.examtopics.com/discussions/amazon/view/97939-exam-aws-certified-solutions-architect-professional-sap-c02/>

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: BCF

<https://www.examtopics.com/discussions/amazon/view/97939-exam-aws-certified-solutions-architect-professional-sap-c02/>

upvoted 1 times

 **Windows98** 3 months, 3 weeks ago

Selected Answer: ACF

C because we want to use Control Tower

A and C because we're going to use Controls and Config

Not D because Control Tower is a parallel product to Organisations and it doesn't use SCPs although it can import existing OUs.

upvoted 1 times

 **Windows98** 3 months, 3 weeks ago

I meant to say A and F because we're going to use Controls and Config

upvoted 1 times

 **Roontha** 4 months ago

Answer : C,D,F

upvoted 1 times

 **DWsk** 5 months ago

Selected Answer: ACF

I think the answer is ACF.

I don't think you need D once you have C. Also, control tower uses config rules to set up guardrails. See the link below:

<https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#:~:text=isn%27t%20enabled%20on%20any%20OUs.-,The%20artifact%20for%20this%20control%20is%20the%20following%20AWS%20Config%20rule.,-AWSTemplateFormatVersion%3A%202010%2D09%2D09>

upvoted 1 times

 **xenodamus** 4 months, 2 weeks ago

You still need to invite accounts before you can organize them in OUs. All steps are needed. I don't like the way they scatter between answers though.

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: CDF

CDF seems the best choice

upvoted 1 times

 **dummy1777** 7 months ago

B. Create a new AWS Control Tower landing zone in an existing developer account. Create OUs for accounts. Add production and development accounts to production and development OUs, respectively.

D. Invite existing accounts to join the organization in AWS Organizations. Create SCPs to ensure compliance.

F. Create a control for the production OU to detect EBS encryption.

By creating a new AWS Control Tower landing zone, the company can create OUs for accounts and add them to the appropriate production and development OUs. This will enable centralized governance and enforce consistent policies and best practices. The company can then invite existing accounts to join the organization in AWS Organizations and create SCPs to ensure compliance. Finally, the company can create a control for the production OU to detect EBS encryption, ensuring that encryption at rest is enforced in production accounts.

upvoted 2 times

 **spd** 7 months, 2 weeks ago

Selected Answer: CDF

Answer is CDF

<https://docs.aws.amazon.com/controltower/latest/userguide/controls.html>

<https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>

upvoted 1 times

 **c73bf38** 7 months, 1 week ago

The artifact for this control is AWS Config rule and AWS Config rules cannot be deployed using AWS CloudFormation StackSets.

upvoted 1 times

 **c73bf38** 7 months, 1 week ago

moderator, delete above as the statement is incorrect that I posted, don't approve post.

upvoted 1 times

 **Musk** 7 months, 2 weeks ago

Selected Answer: ABD

In F, guardrails are proposed to detect. Guardrails don't detect but prevent.

upvoted 1 times

 **Musk** 7 months, 1 week ago

I found this, and after further reading I vote for CDF: <https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>

upvoted 1 times

 **oatif** 7 months, 2 weeks ago

Selected Answer: CDF

CloudTower and guard rails are custom built for this kind of situation

upvoted 1 times

 **Untamables** 7 months, 2 weeks ago

Selected Answer: CDF

<https://docs.aws.amazon.com/controltower/latest/userguide/controls.html>

<https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>

AWS is now transitioning the previous term 'guardrail' new term 'control'.

upvoted 4 times

 **ExamTopix01** 7 months, 3 weeks ago

CDF

<https://docs.aws.amazon.com/controlltower/latest/userguide/guardrails.html>

upvoted 4 times

Question #169

Topic 1

A company is running a critical stateful web application on two Linux Amazon EC2 instances behind an Application Load Balancer (ALB) with an Amazon RDS for MySQL database. The company hosts the DNS records for the application in Amazon Route 53. A solutions architect must recommend a solution to improve the resiliency of the application.

The solution must meet the following objectives:

- Application tier: RPO of 2 minutes. RTO of 30 minutes
- Database tier: RPO of 5 minutes. RTO of 30 minutes

The company does not want to make significant changes to the existing application architecture. The company must ensure optimal latency after a failover.

Which solution will meet these requirements?

- Configure the EC2 instances to use AWS Elastic Disaster Recovery. Create a cross-Region read replica for the RDS DB instance. Create an ALB in a second AWS Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs. Update DNS records to point to the Global Accelerator endpoint.
- Configure the EC2 instances to use Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes. Configure RDS automated backups. Configure backup replication to a second AWS Region. Create an ALB in the second Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs. Update DNS records to point to the Global Accelerator endpoint.
- Create a backup plan in AWS Backup for the EC2 instances and RDS DB instance. Configure backup replication to a second AWS Region. Create an ALB in the second Region. Configure an Amazon CloudFront distribution in front of the ALB. Update DNS records to point to CloudFront.
- Configure the EC2 instances to use Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes. Create a cross-Region read replica for the RDS DB instance. Create an ALB in a second AWS Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs.

 **God_Is_Love** Highly Voted 6 months, 2 weeks ago

Selected Answer: A

DRS includes EC2 instances as well not just data related as offered by DLM or Backup

Q: What operating systems and applications are supported by AWS DRS?

A: You can use AWS DRS to recover all of your applications and databases that run on supported Windows and Linux operating system versions. This includes critical databases such as Oracle, MySQL, and SQL Server, and enterprise applications such as SAP.

AWS Elastic Disaster Recovery (DRS) vs AWS DLM vs AWS Backup

You should use DLM when you want to automate the creation, retention, and deletion of EBS snapshots. You should use AWS Backup to manage and monitor backups across the AWS services you use, including EBS volumes, from a single place.

upvoted 14 times

 **bititan** Highly Voted 7 months, 3 weeks ago

Selected Answer: A

its understood that others cannot meet the RTO and RPO requirements, because restore from back can take time based on the size of the data
upvoted 7 times

 **nharaz** Most Recent 1 week, 3 days ago

Selected Answer: A

DRS is faster to recover than Backups > https://youtu.be/07EHsPuKXc0?si=w_dZQKOAynE2T4JY
upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A for low RPO
upvoted 1 times

 **Jesuisleon** 4 months, 2 weeks ago

I don't understand the sentence "Update DNS records to point to the Global Accelerator endpoint" in A and B. It doesn't make sense. I think it should "update DNS records to point to the GA two static IP addresses or GA's DNS name"

upvoted 1 times

✉️  **dev112233xx** 5 months, 2 weeks ago

Selected Answer: A

RDS Cross-region replication has the best RPO and RTO:

<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html>

AWS Elastic Disaster Recovery also provide the best RTO/RPO (with Warm standby and active-active)

https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_disaster_recovery.html

upvoted 4 times

✉️  **OCHT** 5 months, 3 weeks ago

Selected Answer: D

You are correct that AWS Elastic Disaster Recovery (DRS) can be used to recover both data and EC2 instances. However, in the scenario described in the question, the specified RPO and RTO objectives for the application tier can be met using Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes attached to the EC2 instances.

While restoring from a backup can take time depending on the size of the data, using Amazon DLM to take snapshots of the EBS volumes provides a way to recover data within the specified RPO of 2 minutes and RTO of 30 minutes for the application tier.

In addition, creating a cross-Region read replica for the RDS DB instance provides a way to recover data within the specified RPO of 5 minutes and RTO of 30 minutes for the database tier.

upvoted 1 times

✉️  **OCHT** 5 months, 3 weeks ago

Option A is not the best solution because it involves using AWS Elastic Disaster Recovery, which is not necessary to meet the specified RPO and RTO objectives for the application and database tiers.

AWS Elastic Disaster Recovery is a service that helps customers prepare for and recover from disasters by providing a cost-effective, fully managed, and scalable solution for disaster recovery. While it can be useful in certain scenarios, it is not necessary in this case because the specified RPO and RTO objectives can be met using other AWS services such as Amazon Data Lifecycle Manager (Amazon DLM) and cross-Region read replicas for the RDS DB instance.

Therefore, Option D is a better solution because it meets the specified requirements without introducing unnecessary complexity or cost.

upvoted 1 times

✉️  **OCHT** 5 months, 3 weeks ago

Overall, while AWS Elastic Disaster Recovery (DRS) can be a useful service in certain scenarios, it is not necessary in this case because the specified RPO and RTO objectives can be met using other AWS services such as Amazon Data Lifecycle Manager (Amazon DLM) and cross-Region read replicas for the RDS DB instance.

upvoted 1 times

✉️  **OCHT** 5 months, 3 weeks ago

Overall, while AWS Elastic Disaster Recovery (DRS) can be a useful service in certain scenarios, it is not necessary in this case because the specified RPO and RTO objectives can be met using other AWS services such as Amazon Data Lifecycle Manager (Amazon DLM) and cross-Region read replicas for the RDS DB instance.

upvoted 1 times

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

The process of starting up new instances and mount the EBS volumes to them will absolutely take more than 30 minutes.

upvoted 1 times

✉️  **Musk** 7 months, 2 weeks ago

Selected Answer: A

I agree it's A

upvoted 2 times

✉️  **schalke04** 7 months, 3 weeks ago

Selected Answer: A

DRS should fulfill the requirements

upvoted 3 times

Question #170

Topic 1

A solutions architect wants to cost-optimize and appropriately size Amazon EC2 instances in a single AWS account. The solutions architect wants to ensure that the instances are optimized based on CPU, memory, and network metrics.

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

- A. Purchase AWS Business Support or AWS Enterprise Support for the account.
- B. Turn on AWS Trusted Advisor and review any “Low Utilization Amazon EC2 Instances” recommendations.
- C. Install the Amazon CloudWatch agent and configure memory metric collection on the EC2 instances.
- D. Configure AWS Compute Optimizer in the AWS account to receive findings and optimization recommendations.
- E. Create an EC2 Instance Savings Plan for the AWS Regions, instance families, and operating systems of interest.

 **God_Is_Love** Highly Voted  6 months, 2 weeks ago

Selected Answer: CD

Not B because, Trusted Advisor is available for Enterprise support only which is not cheap and the SA needs to cost optimize here. CPU, memory, and network relate to Compute so D for sure. C will enable to know how much actual memory/CPU is needed for instances and SA can provision based on cw logs

upvoted 6 times

 **Simon523** Most Recent  1 month ago

Selected Answer: CD

AWS Compute Optimizer recommends optimal AWS resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics.

upvoted 1 times

 **SK_Tyagi** 1 month, 1 week ago

Selected Answer: CD

Cloud Watch Agent for memory metric & Compute Optimizer for recommendations

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: CD

cd for sure

upvoted 1 times

 **iamunstopable** 5 months ago

A & B will incur more cost. CD are correct

upvoted 2 times

 **Roontha** 4 months ago

Agreed. Answers are C,D

<https://docs.aws.amazon.com/compute-optimizer/latest/ug/metrics.html>

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: CD

CD is right

upvoted 1 times

 **saurabh1805** 7 months ago

Selected Answer: CD

trusted advisor does not take memory in consideration hence CD is right answer.

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html>

upvoted 1 times

 **CloudFloater** 7 months, 1 week ago

D,OK.. but, why not B trusted advisor rather than C cloudwatch ?

upvoted 1 times

 **rtgfdv3** 7 months ago

seems like you need cloud watch agent installed in order to check memory parameter

Note:

To have Compute Optimizer analyze the memory utilization of your instances, install the CloudWatch agent on your instances. Enabling Compute Optimizer to analyze memory utilization data for your instances provides an additional measurement of data that further improves

Compute Optimizer's recommendations

<https://docs.aws.amazon.com/compute-optimizer/latest/ug/metrics.html>

upvoted 2 times

✉ **hobokabobo** 6 months, 2 weeks ago

Memory taken by the os is almost always 100% - but most of it caches, buffers. To get you need the actually used memory by applications. This number is os specific(need to ask the os how the memory is used: only caches or actual use?) and as such can't be gathered from the virtualizer. So you need an agent for that.

upvoted 1 times

✉ **Musk** 7 months, 1 week ago

Selected Answer: CD

CD according to <https://docs.aws.amazon.com/compute-optimizer/latest/ug/metrics.html>

upvoted 2 times

✉ **spd** 7 months, 2 weeks ago

Selected Answer: CD

For Memory - CloudWatch and Compute Optimizer

upvoted 3 times

✉ **c73bf38** 7 months, 1 week ago

What about the other metrics?

CPU and network metrics.

upvoted 1 times

✉ **c73bf38** 7 months, 1 week ago

CD is correct, CloudWatch agents supports the metrics mentioned.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html>

upvoted 1 times

Question #171

Topic 1

A company uses an AWS CodeCommit repository. The company must store a backup copy of the data that is in the repository in a second AWS Region.

Which solution will meet these requirements?

- A. Configure AWS Elastic Disaster Recovery to replicate the CodeCommit repository data to the second Region.
- B. Use AWS Backup to back up the CodeCommit repository on an hourly schedule. Create a cross-Region copy in the second Region.
- C. Create an Amazon EventBridge rule to invoke AWS CodeBuild when the company pushes code to the repository. Use CodeBuild to clone the repository. Create a .zip file of the content. Copy the file to an S3 bucket in the second Region.
- D. Create an AWS Step Functions workflow on an hourly schedule to take a snapshot of the CodeCommit repository. Configure the workflow to copy the snapshot to an S3 bucket in the second Region

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

its a C

upvoted 1 times

 **easytoo** 3 months, 1 week ago

b-b-b-b-b-b-b-b

upvoted 1 times

 **easytoo** 3 months, 1 week ago

C-C-C-C-CC-C-C-C-C-C-C

upvoted 1 times

 **easytoo** 3 months, 1 week ago

b in incorrect as AWS Backup does not backup code commit as a source.

upvoted 1 times

 **Roontha** 4 months ago

Answer : C

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-event-driven-backups-from-codecommit-to-amazon-s3-using-codebuild-and-cloudwatch-events.html>

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

C for sure

upvoted 2 times

 **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-event-driven-backups-from-codecommit-to-amazon-s3-using-codebuild-and-cloudwatch-events.html>

upvoted 1 times

 **kiran15789** 7 months ago

Selected Answer: C

<https://www.automat-it.com/post/backup-aws-codecommit>

upvoted 2 times

 **c73bf38** 7 months, 1 week ago

Selected Answer: C

C is correct, AWS Backup does not backup code commit as a source.

upvoted 1 times

 **Iunt** 7 months, 1 week ago

Selected Answer: C

B is wrong > AWS Backup does not support CodeCommit as source.

A is out.

C is right.

upvoted 1 times

 **Musk** 7 months, 1 week ago

Selected Answer: C

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-event-driven-backups-from-codecommit-to-amazon-s3-using-codebuild-and-cloudwatch-events.html>

upvoted 2 times

✉ **c73bf38** 7 months, 1 week ago

Selected Answer: B

It says backup so I think B is the answer:

B. Use AWS Backup to back up the CodeCommit repository on an hourly schedule. Create a cross-Region copy in the second Region.

upvoted 1 times

✉ **c73bf38** 7 months, 1 week ago

Changing to C, thanks.

upvoted 2 times

✉ **spd** 7 months, 2 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/deploy-code-in-multiple-aws-regions-using-aws-codepipeline-aws-codecommit-and-aws-codebuild.html>

<https://medium.com/geekculture/replicate-aws-codecommit-repositories-between-regions-using-codebuild-and-codepipeline-39f6b8fcfd2>

upvoted 4 times

Question #172

Topic 1

A company has multiple business units that each have separate accounts on AWS. Each business unit manages its own network with several VPCs that have CIDR ranges that overlap. The company's marketing team has created a new internal application and wants to make the application accessible to all the other business units. The solution must use private IP addresses only.

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

- A. Instruct each business unit to add a unique secondary CIDR range to the business unit's VPC. Peer the VPCs and use a private NAT gateway in the secondary range to route traffic to the marketing team.
- B. Create an Amazon EC2 instance to serve as a virtual appliance in the marketing account's VPC. Create an AWS Site-to-Site VPN connection between the marketing team and each business unit's VPC. Perform NAT where necessary.
- C. Create an AWS PrivateLink endpoint service to share the marketing application. Grant permission to specific AWS accounts to connect to the service. Create interface VPC endpoints in other accounts to access the application by using private IP addresses.
- D. Create a Network Load Balancer (NLB) in front of the marketing application in a private subnet. Create an API Gateway API. Use the Amazon API Gateway private integration to connect the API to the NLB. Activate IAM authorization for the API. Grant access to the accounts of the other business units.

 **spd** Highly Voted  7 months, 2 weeks ago

Selected Answer: C

Private link is the solution for IP Overlapping and Securely access the app between accounts

upvoted 8 times

 **c73bf38** Highly Voted  7 months, 1 week ago

Selected Answer: C

With AWS PrivateLink, the marketing team can create an endpoint service to share their internal application with other accounts securely using private IP addresses. They can grant permission to specific AWS accounts to connect to the service and create interface VPC endpoints in the other accounts to access the application by using private IP addresses. This option does not require any changes to the network of the other business units, and it does not require peering or NATing. This solution is both scalable and secure.

upvoted 7 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: C

C for sure

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: C

The solution that will meet the requirements with the least operational overhead is:

C. Create an AWS PrivateLink endpoint service to share the marketing application. Grant permission to specific AWS accounts to connect to the service. Create interface VPC endpoints in other accounts to access the application using private IP addresses.

AWS PrivateLink provides secure and scalable private connectivity between VPCs, AWS services, and on-premises applications, without using public IP addresses. In this case, you can create an AWS PrivateLink endpoint service for the marketing application, which allows other business units to access the application using private IP addresses.

By granting permission to specific AWS accounts to connect to the PrivateLink endpoint service, you can control access to the marketing application. Then, in each business unit's VPC, you can create interface VPC endpoints to connect to the PrivateLink service, allowing them to access the marketing application privately.

upvoted 2 times

 **mfsec** 6 months ago

Selected Answer: C

Private link

upvoted 1 times

 **God_Is_Love** 6 months, 2 weeks ago

Selected Answer: C

Networking & Content Delivery blog -

<https://aws.amazon.com/blogs/networking-and-content-delivery/connecting-networks-with-overlapping-ip-ranges/>

upvoted 4 times

Question #173

Topic 1

A company needs to audit the security posture of a newly acquired AWS account. The company's data security team requires a notification only when an Amazon S3 bucket becomes publicly exposed. The company has already established an Amazon Simple Notification Service (Amazon SNS) topic that has the data security team's email address subscribed.

Which solution will meet these requirements?

- A. Create an S3 event notification on all S3 buckets for the isPublic event. Select the SNS topic as the target for the event notifications.
- B. Create an analyzer in AWS Identity and Access Management Access Analyzer. Create an Amazon EventBridge rule for the event type "Access Analyzer Finding" with a filter for "isPublic: true." Select the SNS topic as the EventBridge rule target.
- C. Create an Amazon EventBridge rule for the event type "Bucket-Level API Call via CloudTrail" with a filter for "PutBucketPolicy." Select the SNS topic as the EventBridge rule target.
- D. Activate AWS Config and add the cloudtrail-s3-dataevents-enabled rule. Create an Amazon EventBridge rule for the event type "Config Rules Re-evaluation Status" with a filter for "NON_COMPLIANT." Select the SNS topic as the EventBridge rule target.

 **God_Is_Love** Highly Voted  6 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-analyzer.html>

upvoted 7 times

 **God_Is_Love** 6 months, 1 week ago

Click on the "Create rule" button.

Enter a name for the rule and a brief description, if desired.

Under "Define pattern", select "Event pattern".

Select "Custom pattern".

In the "Event pattern" field, enter the following code:

```
{
  "source": ["aws.securityhub"],
  "detail-type": ["Access Analyzer Finding"],
  "detail": {
    "findings": [
      {
        "isPublic": [
          true
        ]
      }
    ]
  }
}
```

This code will match all Access Analyzer Finding events where the "isPublic" field is set to "true".

upvoted 7 times

 **c73bf38** Highly Voted  7 months, 1 week ago

Selected Answer: B

B is the correct solution because it uses AWS Identity and Access Management Access Analyzer to continuously monitor access control configurations and detect whether any S3 buckets have been configured to be publicly accessible. When a publicly accessible bucket is detected, an Amazon EventBridge rule is triggered, and the SNS topic is notified with the finding.

upvoted 6 times

 **dkcloudguru** Most Recent  1 week, 6 days ago

Option B

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

it's B

upvoted 1 times

 **dkx** 2 months, 3 weeks ago

A. No, because Amazon S3 can NOT currently publish notifications for isPublic events.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/EventNotifications.html>

- B. Yes, because IAM Access Analyzer for S3 alerts you to S3 buckets that are configured to allow access to anyone on the internet or other AWS accounts
<https://aws.amazon.com/blogs/security/how-to-prioritize-iam-access-analyzer-findings/>
- C. No, because PutBucketPolicy notifies us of an Amazon S3 bucket policy event to an Amazon S3 bucket, and we are looking for a SPECIFIC event to the bucket permissions, not ALL events.
- D. No, because cloudtrail-s3-dataevents-enabled checks if at least one AWS CloudTrail trail is logging Amazon Simple Storage Service (Amazon S3) data events for all S3 buckets.

<https://docs.aws.amazon.com/config/latest/developerguide/cloudtrail-s3-dataevents-enabled.html>
 upvoted 2 times

✉ **Maria2023** 3 months ago

Selected Answer: B

Ideally, I would use config rule, but here, of course, they suggest the wrong rule. The other option remains the access analyzer
 upvoted 1 times

✉ **SkyZeroZx** 3 months, 1 week ago

Selected Answer: B

keyword = AWS Identity and Access Management Access Analyzer
 then B

upvoted 1 times

✉ **leehjworking** 4 months ago

Selected Answer: B

The code by God_is_love did not work for me. I guess something has been changed.
 The following code worked in my environment.

```
{
"source":["aws.access-analyzer"],
"detail-type":["Access Analyzer Finding"],
"detail": {
{
"isPublic":true}
}
}
```

upvoted 1 times

✉ **SkyZeroZx** 4 months ago

Selected Answer: B

Aws is letter B

Previous writing is a error

upvoted 1 times

✉ **SkyZeroZx** 4 months ago

Letter C

upvoted 1 times

✉ **SkyZeroZx** 4 months ago

Solution D will not meet the requirements because it will notify the data security team whenever an S3 bucket is not compliant with the cloudtrail-s3-dataevents-enabled rule, even if the bucket is not publicly exposed. The cloudtrail-s3-dataevents-enabled rule checks if at least one AWS CloudTrail trail is logging Amazon Simple Storage Service (Amazon S3) data events for all S3 buckets. If a bucket is not compliant with this rule, it does not mean that the bucket is publicly exposed. The bucket may simply not be logging S3 data events.

upvoted 1 times

✉ **SkyZeroZx** 4 months ago

Here are some reasons why an S3 bucket may not be logging S3 data events:

The bucket may not have a CloudTrail trail associated with it.

The CloudTrail trail for the bucket may not be enabled.

The CloudTrail trail for the bucket may not be configured to log S3 data events.

If the data security team is only interested in being notified when an S3 bucket becomes publicly exposed, then solution D is not the best solution. Solution B is a better solution because it will only notify the data security team when an S3 bucket becomes publicly exposed.

upvoted 1 times

✉ **y0eri** 4 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-eventbridge.html>

upvoted 1 times

✉ **mfsec** 6 months ago

Selected Answer: B

B eventbridge and access analyser

upvoted 2 times

✉  **massa** 7 months, 1 week ago

Selected Answer: B

Access Analyzer is to assess the access policy.

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/access-control-block-public-access.html

upvoted 2 times

✉  **[Removed]** 7 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/blogs/security/how-to-use-aws-iam-access-analyzer-api-to-automate-detection-of-public-access-to-aws-kms-keys/>

upvoted 2 times

✉  **mdijoux25** 7 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-analyzer.html>

upvoted 2 times

✉  **spd** 7 months, 2 weeks ago

Selected Answer: D

D by elimination rule

upvoted 2 times

✉  **Jay_2pt0_1** 4 months, 3 weeks ago

I thought D, as well, but it seems everyone else thinks Access Analyzer.

upvoted 1 times

Question #174

Topic 1

A solutions architect needs to assess a newly acquired company's portfolio of applications and databases. The solutions architect must create a business case to migrate the portfolio to AWS. The newly acquired company runs applications in an on-premises data center. The data center is not well documented. The solutions architect cannot immediately determine how many applications and databases exist. Traffic for the applications is variable. Some applications are batch processes that run at the end of each month.

The solutions architect must gain a better understanding of the portfolio before a migration to AWS can begin.

Which solution will meet these requirements?

- A. Use AWS Server Migration Service (AWS SMS) and AWS Database Migration Service (AWS DMS) to evaluate migration. Use AWS Service Catalog to understand application and database dependencies.
- B. Use AWS Application Migration Service. Run agents on the on-premises infrastructure. Manage the agents by using AWS Migration Hub. Use AWS Storage Gateway to assess local storage needs and database dependencies.
- C. Use Migration Evaluator to generate a list of servers. Build a report for a business case. Use AWS Migration Hub to view the portfolio. Use AWS Application Discovery Service to gain an understanding of application dependencies.
- D. Use AWS Control Tower in the destination account to generate an application portfolio. Use AWS Server Migration Service (AWS SMS) to generate deeper reports and a business case. Use a landing zone for core accounts and resources.

 **spd** Highly Voted 7 months, 2 weeks ago

Selected Answer: C

First need to evaluate
upvoted 12 times

 **c73bf38** Highly Voted 7 months, 1 week ago

Selected Answer: C

C. Use Migration Evaluator to generate a list of servers. Build a report for a business case. Use AWS Migration Hub to view the portfolio. Use AWS Application Discovery Service to gain an understanding of application dependencies.
upvoted 5 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: C

C for sure
upvoted 1 times

 **Roontha** 4 months ago

Answer : C
<https://aws.amazon.com/migration-evaluator/>
upvoted 1 times

 **F_Eldin** 4 months ago

Selected Answer: B

The emphasis is on applications. "Some applications are batch processes that run at the end of each month"
I do not understand why C is better than B
upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: C

Use migration evaluator
upvoted 3 times

Question #175

Topic 1

A company has an application that runs as a ReplicaSet of multiple pods in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster has nodes in multiple Availability Zones. The application generates many small files that must be accessible across all running instances of the application. The company needs to back up the files and retain the backups for 1 year.

Which solution will meet these requirements while providing the FASTEST storage performance?

- A. Create an Amazon Elastic File System (Amazon EFS) file system and a mount target for each subnet that contains nodes in the EKS cluster. Configure the ReplicaSet to mount the file system. Direct the application to store files in the file system. Configure AWS Backup to back up and retain copies of the data for 1 year.
- B. Create an Amazon Elastic Block Store (Amazon EBS) volume. Enable the EBS Multi-Attach feature. Configure the ReplicaSet to mount the EBS volume. Direct the application to store files in the EBS volume. Configure AWS Backup to back up and retain copies of the data for 1 year.
- C. Create an Amazon S3 bucket. Configure the ReplicaSet to mount the S3 bucket. Direct the application to store files in the S3 bucket. Configure S3 Versioning to retain copies of the data. Configure an S3 Lifecycle policy to delete objects after 1 year.
- D. Configure the ReplicaSet to use the storage available on each of the running application pods to store the files locally. Use a third-party tool to back up the EKS cluster for 1 year.

 **c73bf38** Highly Voted 7 months, 1 week ago

Selected Answer: A

Explanation: Amazon EFS provides shared file storage that is highly available and durable. It is an ideal solution to share files between containers running on multiple instances in a cluster. Mounting an Amazon EFS file system on each subnet provides a shared file system for multiple instances running in different Availability Zones. Additionally, AWS Backup provides automated backup and recovery of Amazon EFS file systems.

upvoted 6 times

 **spd** Highly Voted 7 months, 2 weeks ago

Selected Answer: A

EFS = Fastest storage performance compare to S3/EBS

upvoted 6 times

 **masssa** 7 months, 1 week ago

I vote B.

I think EBS is faster than S3/EBS.

<https://www.msp360.com/resources/blog/amazon-s3-vs-ebs-vs-efs/>

upvoted 1 times

 **masssa** 7 months, 1 week ago

typo.

EBS faster than S3/EFS.

upvoted 2 times

 **Musk** 7 months, 1 week ago

I just read the question refers to multiple AZs, so B is not an option.

upvoted 6 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: A

A - EFS for multi-AZ

upvoted 2 times

 **dkx** 2 months, 3 weeks ago

A. Yes, because Amazon EFS offers you the choice of creating file systems using Standard or One Zone storage classes. Standard storage classes store data with and across multiple AZs.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/run-stateful-workloads-with-persistent-data-storage-by-using-amazon-efs-on-amazon-eks-with-aws-fargate.html>

B. No, because Amazon EBS Multi-Attach enabled volumes can be attached to up to 16 Linux instances built on the Nitro System that are in the same Availability Zone. We need to solve for "nodes in multiple Availability Zones"

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html>

C. No, because if you're looking to run file-based applications that need to collaborate or coordinate on shared data across instances or users, AWS recommends fully managed file services, such as Amazon FSx or Amazon Elastic File System (EFS).

D. No, because the company needs to back up the files, not backup the EKS Cluster.

upvoted 2 times

✉  **mfsec** 6 months ago

Selected Answer: A

A for sure

upvoted 2 times

✉  **ramyaram** 6 months ago

Selected Answer: A

Keyword here is multiple small files and shared between multiple clusters

upvoted 3 times

✉  **God_Is_Love** 6 months, 1 week ago

Selected Answer: A

In the past, EBS can be attached only to one ec2 instance but not anymore but there are limitations like - it works only on io1/io2 instance types and many others as described here. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html>
EFS has shareable storage

In terms of performance, Amazon EFS is optimized for workloads that require high levels of aggregate throughput and IOPS, whereas EBS is optimized for low-latency, random access I/O operations. Amazon EFS is designed to scale throughput and capacity automatically as your storage needs grow, while EBS volumes can be resized on demand.

upvoted 3 times

✉  **Zek** 6 months, 3 weeks ago

I support A since their is a multi-AZ requirement.

<https://repost.aws/questions/QUK2RANw1QTKCwpDUwCCI72A/efs-vs-ebs-mult-attach>

EFS is also designed for high availability and high durability. To achieve these levels of availability and durability, EFS automatically replicates data within and across 3 Availability Zones, with no single points of failure. EBS multi-attach volumes can be used for clients within a single Availability Zone.

upvoted 1 times

✉  **Sarutobi** 6 months, 3 weeks ago

Selected Answer: A

When you have an EKS cluster and use the EBS that is local to the node, only Pods running on that node have access to the storage. If the node starts on any other Pod, it will potentially break. There are ways to fix this, but they are beyond this question. I believe we need shared fast storage here, so it should be S3 vs EFS the decision.

upvoted 3 times

✉  **Musk** 7 months, 1 week ago

I've been reding here and there, and B does not seem that feasible, although if supported it would be faster than A.

upvoted 2 times

Question #176

Topic 1

A company runs a customer service center that accepts calls and automatically sends all customers a managed, interactive, two-way experience survey by text message. The applications that support the customer service center run on machines that the company hosts in an on-premises data center. The hardware that the company uses is old, and the company is experiencing downtime with the system. The company wants to migrate the system to AWS to improve reliability.

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

- A. Use Amazon Connect to replace the old call center hardware. Use Amazon Pinpoint to send text message surveys to customers.
- B. Use Amazon Connect to replace the old call center hardware. Use Amazon Simple Notification Service (Amazon SNS) to send text message surveys to customers.
- C. Migrate the call center software to Amazon EC2 instances that are in an Auto Scaling group. Use the EC2 instances to send text message surveys to customers.
- D. Use Amazon Pinpoint to replace the old call center hardware and to send text message surveys to customers.

 **God_Is_Love** Highly Voted  6 months, 1 week ago

Selected Answer: A

Amazon Connect is a cloud-based contact center service that allows you to set up a virtual call center for your business. It provides an easy-to-use interface for managing customer interactions through voice and chat. Amazon Connect integrates with other AWS services, such as Amazon S3 and Amazon Kinesis, to help you collect, store, and analyze customer data for insights into customer behavior and trends.

On the other hand, Amazon Pinpoint is a marketing automation and analytics service that allows you to engage with your customers across different channels, such as email, SMS, push notifications, and voice. It helps you create personalized campaigns based on user behavior and enables you to track user engagement and retention.

While both services allow you to communicate with your customers, they serve different purposes. Amazon Connect is focused on customer support and service, while Amazon Pinpoint is focused on marketing and engagement.

upvoted 6 times

 **rrrrrrrrr1** Most Recent  2 months, 2 weeks ago

Why not b though? SNS is easy as heck to use.

upvoted 1 times

 **rrrrrrrrr1** 2 months, 2 weeks ago

nvm text message surveys are probably a pinpoint thing. I was thinking like a link to a survey.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A - basic AWS connect use case

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: A

Amazon connect + Pinpoint are the best choice here

upvoted 1 times

 **Roontha** 4 months ago

Answer: A

upvoted 1 times

 **mfsec** 6 months ago

Selected Answer: A

Use Amazon Connect to replace the old call center hardware. Use Amazon Pinpoint to send text message surveys to customers.

upvoted 1 times

 **c73bf38** 7 months, 1 week ago

Selected Answer: A

The solution that will meet the company's requirements with the LEAST ongoing operational overhead and send two-way experience survey is to use Amazon Connect to replace the old call center hardware and use Amazon Pinpoint to send text message surveys to customers. Amazon Connect is a fully managed, cloud-based contact center service that is easy to set up and configure, while Amazon Pinpoint can be used to send text message surveys and gather responses. By using these services, the company can offload the operational overhead of running and maintaining the call center hardware and survey system to AWS.

upvoted 3 times

 **spd** 7 months, 2 weeks ago

Selected Answer: A<https://docs.aws.amazon.com/pinpoint/latest/userguide/channels-sms-two-way.html>

upvoted 2 times

Question #177

Topic 1

A company is building a call center by using Amazon Connect. The company's operations team is defining a disaster recovery (DR) strategy across AWS Regions. The contact center has dozens of contact flows, hundreds of users, and dozens of claimed phone numbers.

Which solution will provide DR with the LOWEST RTO?

- A. Create an AWS Lambda function to check the availability of the Amazon Connect instance and to send a notification to the operations team in case of unavailability. Create an Amazon EventBridge rule to invoke the Lambda function every 5 minutes. After notification, instruct the operations team to use the AWS Management Console to provision a new Amazon Connect instance in a second Region. Deploy the contact flows, users, and claimed phone numbers by using an AWS CloudFormation template.
- B. Provision a new Amazon Connect instance with all existing users in a second Region. Create an AWS Lambda function to check the availability of the Amazon Connect instance. Create an Amazon EventBridge rule to invoke the Lambda function every 5 minutes. In the event of an issue, configure the Lambda function to deploy an AWS CloudFormation template that provisions contact flows and claimed numbers in the second Region.
- C. Provision a new Amazon Connect instance with all existing contact flows and claimed phone numbers in a second Region. Create an Amazon Route 53 health check for the URL of the Amazon Connect instance. Create an Amazon CloudWatch alarm for failed health checks. Create an AWS Lambda function to deploy an AWS CloudFormation template that provisions all users. Configure the alarm to invoke the Lambda function.
- D. Provision a new Amazon Connect instance with all existing users and contact flows in a second Region. Create an Amazon Route 53 health check for the URL of the Amazon Connect instance. Create an Amazon CloudWatch alarm for failed health checks. Create an AWS Lambda function to deploy an AWS CloudFormation template that provisions claimed phone numbers. Configure the alarm to invoke the Lambda function.

 **spd** Highly Voted 7 months, 1 week ago

Selected Answer: D

D looks most appropriate

upvoted 9 times

 **nyxs_19** Highly Voted 7 months, 1 week ago

Selected Answer: D

The solution that will provide DR with the LOWEST RTO (Recovery Time Objective) is option D.

Option D provisions a new Amazon Connect instance with all existing users and contact flows in a second Region. It also sets up an Amazon Route 53 health check for the URL of the Amazon Connect instance, an Amazon CloudWatch alarm for failed health checks, and an AWS Lambda function to deploy an AWS CloudFormation template that provisions claimed phone numbers. This option allows for the fastest recovery time because all the necessary components are already provisioned and ready to go in the second Region. In the event of a disaster, the failed health check will trigger the AWS Lambda function to deploy the CloudFormation template to provision the claimed phone numbers, which is the only missing component.

upvoted 6 times

 **SK_Tyagi** Most Recent 1 month ago

Selected Answer: D

D seems to fit all requirements, however C & D seem to be very similar. Only difference is whether to upload users or phone numbers through Cloud Formation. It seems users, routing profiles, queues, and flows get created with ReplicateInstance API
<https://docs.aws.amazon.com/connect/latest/adminguide/create-replica-connect-instance.html>

upvoted 1 times

 **MRL110** 1 month, 4 weeks ago

Selected Answer: B

Apparently Route 53 can't manage Amazon Connect DNS names or health checks.

<https://docs.aws.amazon.com/connect/latest/adminguide/update-your-connect-domain.html#new-domain-custom>

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

D i guess

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: B

I vote for B since I was not able to find a way to make Route53 serve the Amazon connect URL and therefore it cannot perform healthcheck. If someone has more information on this - please share

upvoted 1 times

✉️  **SkyZeroZx** 4 months ago

why not letter C

"CloudFormation template that provisions all users" insted of "CloudFormation template that provisions claimed phone numbers" of letter D

upvoted 2 times

✉️  **dev112233xx** 5 months, 2 weeks ago

Selected Answer: B

I'm voting B because i don't think it's possible to use Amazon Route 53 health check to verify the availability of Amazon Connect

upvoted 1 times

✉️  **Eshu2009** 6 months ago

why not C?

upvoted 1 times

✉️  **mfsec** 6 months ago

Selected Answer: D

D. Provision a new Amazon Connect instance with all existing users and contact flows in a second Region.

upvoted 3 times

✉️  **c73bf38** 7 months, 1 week ago

Selected Answer: D

D is the better solution.

upvoted 3 times

✉️  **c73bf38** 7 months, 1 week ago

Selected Answer: B

B. Provision a new Amazon Connect instance with all existing users in a second Region. Create an AWS Lambda function to check the availability of the Amazon Connect instance. Create an Amazon EventBridge rule to invoke the Lambda function every 5 minutes. In the event of an issue, configure the Lambda function to deploy an AWS CloudFormation template that provisions contact flows and claimed numbers in the second Region will provide disaster recovery with the LOWEST Recovery Time Objective.

upvoted 2 times

✉️  **c73bf38** 7 months, 1 week ago

Thanks for pointing that out, D is the better solution.

upvoted 2 times

✉️  **Musk** 7 months, 1 week ago

With D you can have a quicker reaction if you use high-resolution CloudWatch alarms that alert as soon as 10-second or 30-second periods. Additionally, contact flows are already there so you don't need to deploy when the error occurs.

upvoted 5 times

Question #178

Topic 1

A company runs an application on AWS. The company curates data from several different sources. The company uses proprietary algorithms to perform data transformations and aggregations. After the company performs ETL processes, the company stores the results in Amazon Redshift tables. The company sells this data to other companies. The company downloads the data as files from the Amazon Redshift tables and transmits the files to several data customers by using FTP. The number of data customers has grown significantly. Management of the data customers has become difficult.

The company will use AWS Data Exchange to create a data product that the company can use to share data with customers. The company wants to confirm the identities of the customers before the company shares data. The customers also need access to the most recent data when the company publishes the data.

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

- A. Use AWS Data Exchange for APIs to share data with customers. Configure subscription verification. In the AWS account of the company that produces the data, create an Amazon API Gateway Data API service integration with Amazon Redshift. Require the data customers to subscribe to the data product.
- B. In the AWS account of the company that produces the data, create an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift cluster. Configure subscription verification. Require the data customers to subscribe to the data product.
- C. Download the data from the Amazon Redshift tables to an Amazon S3 bucket periodically. Use AWS Data Exchange for S3 to share data with customers. Configure subscription verification. Require the data customers to subscribe to the data product.
- D. Publish the Amazon Redshift data to an Open Data on AWS Data Exchange. Require the customers to subscribe to the data product in AWS Data Exchange. In the AWS account of the company that produces the data, attach IAM resource-based policies to the Amazon Redshift tables to allow access only to verified AWS accounts.

 **youngmanaws** Highly Voted 5 months ago

Selected Answer: B

The company wants to confirm the identities of the customers before the company shares data. The customers also need access to the most recent data when the company publishes the data. With B, customer can get data from Redshift directly with no time lag and additional operations.

upvoted 5 times

 **NikkyDicky** Most Recent 2 months, 3 weeks ago

Selected Answer: B

it's a B

upvoted 1 times

 **SmileyCloud** 2 months, 3 weeks ago

Selected Answer: B

Keyword is datashare

<https://docs.aws.amazon.com/redshift/latest/dg/adx-getting-started.html>

upvoted 1 times

 **easystoo** 3 months, 1 week ago

b-b-b-b-b-b-b-b-b-b

LEAST operational overhead...

Option (A) uses AWS Data Exchange for APIs, which requires you to create an Amazon API Gateway Data API service integration with Amazon Redshift. This is a more complex solution than using a datashare.

Option (C) uses AWS Data Exchange for S3, which requires you to download the data from Amazon Redshift to Amazon S3 periodically. This is also a more complex solution than using a datashare.

Option (D) publishes the data to an Open Data on AWS Data Exchange, which does not allow you to configure subscription verification. This means that anyone can access the data, which is not ideal for a company that wants to protect its proprietary algorithms.

upvoted 2 times

 **TECHNOWARRIOR** 3 months, 1 week ago

AWS Data Exchange for APIs enables customers to discover and utilize third-party APIs in the cloud, with authentication using AWS IAM credentials and SDKs. It simplifies access permissions and governance. Users can access data APIs from numerous providers. On the other hand, AWS Data Exchange Datashare focuses on licensing access to Amazon Redshift data. It utilizes AWS-native authentication and automatically adds customers as data consumers. With read-only access, customers can retrieve objects from datashares. While both services integrate with AWS, Data Exchange for APIs is geared towards API usage, while Data Exchange Datashare is centered around licensing access to Amazon Redshift data.

upvoted 3 times

Roontha 4 months ago

Answer : B

<https://www.youtube.com/watch?v=BeloTSql4IM>

(AWS Data Exchange for Amazon Redshift demo | Amazon Web Services)

upvoted 2 times

Sarutobi 4 months, 1 week ago

Selected Answer: B

B is the closest one but is not correct either.

https://docs.amazonaws.cn/en_us/redshift/latest/dg/adx-getting-started-producer.html, like every thing else in AWS you need policy to grant access and that is missing in B.

upvoted 2 times

renegadedme 5 months ago

Selected Answer: B

I think it's B.

According to <https://aws.amazon.com/data-exchange/why-aws-data-exchange/redshift-data-tables/>

Customers can find and subscribe to third-party data in AWS Data Exchange and directly query the data in minutes in Amazon Redshift without extracting, transforming, or loading it.

In B, customers can query Redshift directly. No need to use S3 periodically. Minimizes operational overhead.

upvoted 4 times

nqg54118 5 months ago

Selected Answer: C

データの顧客数は大幅に増加した対策にS3

upvoted 1 times

easytoo 3 months, 1 week ago

yup! was about to say the same.

upvoted 2 times

OCHT 5 months ago

Selected Answer: C

The correct answer is C. Download the data from the Amazon Redshift tables to an Amazon S3 bucket periodically. Use AWS Data Exchange for S3 to share data with customers. Configure subscription verification. Require the data customers to subscribe to the data product.

Exporting the data to an Amazon S3 bucket periodically ensures that customers have access to the most recent data when the company publishes it.

AWS Data Exchange for S3 allows you to share data with customers easily and manage their subscriptions.

Subscription verification helps confirm the identity of customers before sharing data with them.

This solution minimizes operational overhead as it leverages AWS Data Exchange and Amazon S3, which are managed services.

The unique keywords combination in this option that makes it easier to remember is Amazon S3, AWS Data Exchange, and subscription verification.

upvoted 2 times

Yowie351 5 months ago

Selected Answer: B

Answer is B. <https://aws.amazon.com/data-exchange/?adx-cards2.sort-by=item.additionalFields.eventDate&adx-cards2.sort-order=desc>

upvoted 2 times

Question #179

Topic 1

A solutions architect is designing a solution to process events. The solution must have the ability to scale in and out based on the number of events that the solution receives. If a processing error occurs, the event must move into a separate queue for review.

Which solution will meet these requirements?

- A. Send event details to an Amazon Simple Notification Service (Amazon SNS) topic. Configure an AWS Lambda function as a subscriber to the SNS topic to process the events. Add an on-failure destination to the function. Set an Amazon Simple Queue Service (Amazon SQS) queue as the target.
- B. Publish events to an Amazon Simple Queue Service (Amazon SQS) queue. Create an Amazon EC2 Auto Scaling group. Configure the Auto Scaling group to scale in and out based on the ApproximateAgeOfOldestMessage metric of the queue. Configure the application to write failed messages to a dead-letter queue.
- C. Write events to an Amazon DynamoDB table. Configure a DynamoDB stream for the table. Configure the stream to invoke an AWS Lambda function. Configure the Lambda function to process the events.
- D. Publish events to an Amazon EventBridge event bus. Create and run an application on an Amazon EC2 instance with an Auto Scaling group that is behind an Application Load Balancer (ALB). Set the ALB as the event bus target. Configure the event bus to retry events. Write messages to a dead-letter queue if the application cannot process the messages.

 **Sarutobi** Highly Voted  5 months ago

Selected Answer: B

I would go with B just because of the wording. I believe A should work just fine, but the question asks for "scale in and out based on the number of events." In my opinion, that is what SNS->Lambda->SQS(DLQ) would do, too; I think the SNS->Lambda scale in/out behavior is more implicit. So I will go with B here because it is more explicit.

upvoted 13 times

 **Yowie351** Highly Voted  5 months ago

Selected Answer: B

SQS with DLQ

upvoted 6 times

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

Selected Answer: B

The question asks to "process events", which should be going to SQS. If the wording was more around messages, then yeah, i would say SNS.
upvoted 1 times

 **Sweetedadad** 3 weeks, 6 days ago

Selected Answer: A

It's A. Can't be B due to this link. It would work, except the parameter should be based on backlog and not Approximate age of old message.
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

upvoted 2 times

 **SK_Tyagi** 1 month ago

Selected Answer: A

My initial reaction was going with B, but then did some research on the scaling parameter. It should be NumberOfMessagesReceived rather than ApproximateAgeOfOldestMessage

upvoted 1 times

 **MRL110** 1 month, 4 weeks ago

Selected Answer: B

A would work just fine. But watch out for the wording here: "the event must move into a separate queue for review."
This indicates that the primary solution is also a queue in the first place which sends failed events to a "separate queue".
upvoted 1 times

 **MRL110** 1 month, 4 weeks ago

EDIT: This indicates that the primary solution is also a queue in the first place and failed events will be moved to a "separate queue".
upvoted 1 times

 **breadops** 2 months ago

Selected Answer: A

A is the answer.
B will not work because 'ApproximateAgeOfOldestMessage' is the wrong thing to scale on, should be 'ApproximateNumberOfMessagesVisible'.
C/D nope.

upvoted 2 times

 **ggrodskiy** 2 months ago

Correct A.

upvoted 1 times

 **nicecurls** 2 months, 2 weeks ago

Selected Answer: A

select A

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A seems like a good option

upvoted 1 times

 **dkx** 2 months, 3 weeks ago

A. Yes, because this uses the concept of Lambda Destinations. Destinations gives you the ability to handle the Failure of function invocations along with their Success. When a function invocation fails, such as when retries are exhausted or the event age has been exceeded (hitting its TTL), Destinations routes the record to the destination resource for every failed invocation for further investigation or processing.
<https://aws.amazon.com/blogs/compute/introducing-aws-lambda-destinations/>

B. No, because the Amazon SQS metric 'ApproximateAgeOfOldestMessage' is the approximate age of the oldest non-deleted message in the queue. Our requirement is to scale on the 'number of events' and not the 'age' of a message.

C. No, because this option fails to clearly mention how to process errors

D. No, because an ALB is not currently available as an EventBridge target. See: <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-targets.html>

upvoted 3 times

 **dkx** 2 months, 3 weeks ago

Additionally, Dead Letter Queues (DLQ) have been available since 2016 and are a great way to handle asynchronous failure situations. Destinations provide more useful capabilities by passing additional function execution information, including code exception stack traces, to more destination services.

upvoted 1 times

 **Piccaso** 2 months, 4 weeks ago

Selected Answer: A

B uses EC2. Lambda function is better.

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: A

Lambda will automatically scale on number of events received.

Scaling of auto-scaling group should not be done based on "ApproximateAgeOfOldestMessage" metric, instead "ApproximateNumberOfMessages" should be used. Further more, question asks to scale based on number of messages received, and "ApproximateAgeOfOldestMessage" doesn't provide that indication.

Ref: <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

upvoted 2 times

 **Maria2023** 3 months ago

Selected Answer: A

I vote for A only because of the metric, used in B - ApproximateAgeOfOldestMessage. This is not how you set up autoscaling for SQS.

upvoted 3 times

 **easystoo** 3 months, 1 week ago

b-b-b-b-b-b-b-b

upvoted 1 times

 **Roontha** 3 months, 3 weeks ago

Answer : A

SNS -> SQS -> Lambda

<https://stackoverflow.com/questions/42656485/sns-to-lambda-vs-sns-to-sqs-to-lambda>

upvoted 3 times

 **y0eri** 4 months, 1 week ago

Selected Answer: A

No age metric for B: <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/sqs/get-queue-attributes.html>

upvoted 2 times

 **clownfishman** 3 months, 2 weeks ago

there is such a cloudwatch metrics - the question is whether AutoScaling group can read that to scale in/out

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-available-cloudwatch-metrics.html>

upvoted 1 times

Question #180

Topic 1

A company runs a processing engine in the AWS Cloud. The engine processes environmental data from logistics centers to calculate a sustainability index. The company has millions of devices in logistics centers that are spread across Europe. The devices send information to the processing engine through a RESTful API.

The API experiences unpredictable bursts of traffic. The company must implement a solution to process all data that the devices send to the processing engine. Data loss is unacceptable.

Which solution will meet these requirements?

- A. Create an Application Load Balancer (ALB) for the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create a listener and a target group for the ALB Add the SQS queue as the target. Use a container that runs in Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to process messages in the queue.
- B. Create an Amazon API Gateway HTTP API that implements the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create an API Gateway service integration with the SQS queue. Create an AWS Lambda function to process messages in the SQS queue.
- C. Create an Amazon API Gateway REST API that implements the RESTful API. Create a fleet of Amazon EC2 instances in an Auto Scaling group. Create an API Gateway Auto Scaling group proxy integration. Use the EC2 instances to process incoming data.
- D. Create an Amazon CloudFront distribution for the RESTful API. Create a data stream in Amazon Kinesis Data Streams. Set the data stream as the origin for the distribution. Create an AWS Lambda function to consume and process data in the data stream.

 **momo3321** Highly Voted 4 months, 2 weeks ago

Selected Answer: B

Option A is incorrect because Application Load Balancer (ALB) can't directly target an Amazon SQS queue.

Option C is incorrect because while Amazon API Gateway and EC2 Auto Scaling can handle high loads, they don't provide a built-in mechanism to ensure that all messages are processed without loss.

Option D is incorrect because Amazon CloudFront is a content delivery network (CDN), and it is not typically used to handle incoming API requests. It is primarily used to cache and deliver content to users.

upvoted 9 times

 **SK_Tyagi** Most Recent 1 month ago

Selected Answer: B

KDS need to implement Sharding for unpredictable bursts

upvoted 1 times

 **rxhan** 2 months ago

Similar to #179

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B is right

upvoted 1 times

 **Roontha** 4 months ago

Answer : B

upvoted 1 times

 **rbm2023** 4 months ago

Selected Answer: B

I agree with B

<https://aws.amazon.com/blogs/architecture/things-to-consider-when-you-build-rest-apis-with-amazon-api-gateway/>

This pattern can decouple the data ingestion from the data processing.

"you should look for opportunities to design an asynchronous, loosely coupled architecture. A decoupled architecture separates the data ingestion from the data processing and allows you to scale each system separately"

upvoted 1 times

 **AMEJack** 4 months, 3 weeks ago

Selected Answer: B

Kinesis DataStreams can't be the origin for the CloudFront

upvoted 2 times

 **mrfretz** 5 months ago

Selected Answer: D

Kinesis retention
upvoted 1 times

 **mrfretz** 5 months ago

Selected Answer: B

Kinesis retention
upvoted 1 times

 **mrfretz** 5 months ago
Answer D, sorry typo
upvoted 1 times

 **Sarutobi** 5 months ago
B is the best option.
upvoted 1 times

 **Littleboy95** 5 months ago

Selected Answer: B

B is correct, you can integrate SQS with API Gateway HTTP. I have checked it in AWS API Gateway Console
<https://repost.aws/knowledge-center/api-gateway-rest-api-sqs-errors>

A is incorrect because you can not set SQS queue as the target of ALB
C is incorrect because a fleet of EC2 instances and ASG can lead instances to terminated unexpectedly → data loss
D is incorrect because Kinesis Data Streams is a provisioned service, It can not handle unpredictable bursts
upvoted 2 times

 **youngmanaws** 5 months ago

KDS has on-demand mode.
<https://docs.aws.amazon.comstreams/latest/dev/how-do-i-size-a-stream.html>
upvoted 1 times

 **Littleboy95** 5 months ago

Yes, KDS has on-demand mode, my wrong. But according to the above link, KDS on-demand can only accommodate up to double the peak write throughput observed in the previous 30 days. While SQS standard Queue has Unlimited Throughput
<https://aws.amazon.com/sqs/features/>
upvoted 1 times

 **OCHT** 5 months ago

Selected Answer: A

The unique keywords combination for the right answer is: Create an Application Load Balancer (ALB) for the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create a listener and a target group for the ALB. Add the SQS queue as the target. Use a container that runs in Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to process messages in the queue.

upvoted 1 times

 **renegadedme** 5 months ago

It's not A.
SQS queue is not a supported target type for ALB target group - <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#target-type>
upvoted 1 times

 **[Removed]** 5 months ago

Selected Answer: B

You can integrate API Gateway with an SQS queue using the AWS SDK, you can write code within your API Gateway implementation to send messages directly to an SQS queue.

upvoted 4 times

 **Yowie351** 5 months ago

Selected Answer: D

Kinesis Data Stream use case. <https://aws.amazon.com/kinesis/data-streams/>
upvoted 2 times

 **Yowie351** 5 months ago

Changing my answer to B
upvoted 2 times

Question #181

Topic 1

A company is designing its network configuration in the AWS Cloud. The company uses AWS Organizations to manage a multi-account setup. The company has three OUs. Each OU contains more than 100 AWS accounts. Each account has a single VPC, and all the VPCs in each OU are in the same AWS Region.

The CIDR ranges for all the AWS accounts do not overlap. The company needs to implement a solution in which VPCs in the same OU can communicate with each other but cannot communicate with VPCs in other OUs.

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

- A. Create an AWS CloudFormation stack set that establishes VPC peering between accounts in each OU. Provision the stack set in each OU.
- B. In each OU, create a dedicated networking account that has a single VPC. Share this VPC with all the other accounts in the OU by using AWS Resource Access Manager (AWS RAM). Create a VPC peering connection between the networking account and each account in the OU.
- C. Provision a transit gateway in an account in each OU. Share the transit gateway across the organization by using AWS Resource Access Manager (AWS RAM). Create transit gateway VPC attachments for each VPC.
- D. In each OU, create a dedicated networking account that has a single VPC. Establish a VPN connection between the networking account and the other accounts in the OU. Use third-party routing software to route transitive traffic between the VPCs.

 **SK_Tyagi** 1 month ago

Selected Answer: C

Fits the use case

<https://aws.amazon.com/transit-gateway/>

upvoted 1 times

 **SK_Tyagi** 1 month ago

<https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-isolated.html>

upvoted 1 times

 **MRL110** 1 month, 4 weeks ago

Selected Answer: A

A for two reasons:

1. Sharing the TGW with the entire organization (C) will make every VPC in every account propagate its subnet in the default TGW route table which will enable organization-wide communication which is categorically prohibited by the question.
2. The question only says more than 100 accounts and 1 VPC per account. It does not mention anything about 125+ VPCs. Plus the peerings are being created by stack sets so there's automation involved. So I believe A is the only solution here.

upvoted 1 times

 **MRL110** 1 month, 4 weeks ago

Disabling default route table association/propagation could be a solution for TGW, but creating 100s of VPC attachments manually is too much operational overhead.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

I think C

upvoted 1 times

 **dkx** 2 months, 3 weeks ago

C. Yes, because, Transit Gateway is a managed service from AWS that acts as a hub interconnecting VPCs and VPN connections within a single region. It allows you to build more complex networks without the need for VPC peering.

Similar to: <https://aws.amazon.com/blogs/networking-and-content-delivery/automating-aws-transit-gateway-attachments-to-a-transit-gateway-in-a-central-account/>

A,B. No, because a VPC peering connection has a limit of 125 Active VPC peering connections per VPC. In this case, each OU contains MORE THAN 100 AWS accounts -- this could mean 101 accounts or 10001 accounts.

D. No, because this is not the answer choice with the LEAST operational overhead. Third-party routing software is not required to route transitive traffic between the VPCs.

upvoted 2 times

 **xflare** 1 month, 2 weeks ago

I believe in this context the organization is the OU, not the entire company. The company is referred to as "the company".

Therefore it's C.

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: C

A separate transit GW for each OU.

upvoted 1 times

Maria2023 3 months ago

Selected Answer: C

The answer should be C. Since VPC peering is not transitive then for 100+ accounts in OU then we'll breach the limit of 125. As for VPN - I wouldn't use VPN to connect AWS resources - I don't know even if that's possible

upvoted 1 times

Jackhemo 3 months ago

Olabiba.ai says C.

upvoted 2 times

Ashas 3 months ago

I have an exam on 27th june, what question set should I prepare? I have only done from Question#1 to Question#181 yet. Please help

upvoted 1 times

Rootha 4 months ago

Answer : C

Reference : <https://catalog.workshops.aws/networking/en-US/intermediate/6-vpc-peering/10-vpc-peering-overview>

upvoted 1 times

Jonalb 4 months ago

Selected Answer: C

D wrong, shared network with transit gateway

upvoted 1 times

SkyZeroZx 4 months ago

Selected Answer: C

Transit Gateway

C

upvoted 1 times

100fold 4 months ago

Selected Answer: C

Changing to answer C. TGW should suffice w route tables.

B: Each OU contains more than 100 AWS accounts. (Could be 126+)

D: Don't think D because best practices is to use AWS services.

upvoted 1 times

dev112233xx 4 months ago

Selected Answer: D

D: I have no other choice

A, B: Peering solution is wrong, because there is a limit of 125 active peering for each VPC (and for 100 VPC full mesh you need at least 4k peering)

C: the solution is incomplete, if you attach all the VPCs in the organization to the TGW then all the VPCs will communicate with each other. better solution is to create separate TGW for each OU! at the beginning i thought the answer is correct until i read this "Share the transit gateway across the organization"

upvoted 1 times

nexus2020 3 months, 3 weeks ago

creating TGW attachment does not enable the flow rightaway, you still need to update the routing table to say reach org B, send to TGW B, etc.

upvoted 2 times

F_Eldin 4 months ago

across the organization not across the organizationS

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: B

Active VPC peering connections per VPC (up to 125). Does not communicate with VPCs in other OUs.

Selecting answer B

upvoted 3 times

AMEJack 4 months, 3 weeks ago

Selected Answer: C

A: CloudFormation StackSets is provision per account not per OU.

B: Maximum VPC peering is 125 (Hard Limit)

C (Correct): Sharing Transit Gateway, yes sharing the TGW will be shared per OU put routing between VPC can be handled through the route

tables.

D: No sense as using third party solution, which can be done by AWS services.

upvoted 3 times

 **MikelH93** 5 months ago

Selected Answer: A

A is the answer

B impossible to share VPC with RAM

C does not meet the requirements because sharing transit gateway with all organizations will allow other OUs to access to all vpc.

D no sense

upvoted 2 times

 **rxhan** 2 months ago

vpc peering for 100s of account?

upvoted 1 times

 **Jay_2pt0_1** 4 months, 3 weeks ago

Peering more than 100 accounts just doesn't seem right.

upvoted 3 times

 **Yowie351** 5 months ago

You can share the VPC with RAM

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

upvoted 2 times

 **DWsk** 5 months ago

Why can't the answer be A?

upvoted 2 times

 **iamunstopable** 5 months ago

B is the correct answer

C will allow inter account vpc communications which the question prohibited

upvoted 2 times

Question #182

Topic 1

A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large important documents within the application with the following requirements:

1. The data must be highly durable and available
2. The data must always be encrypted at rest and in transit
3. The encryption key must be managed by the company and rotated periodically

Which of the following solutions should the solutions architect recommend?

- A. Deploy the storage gateway to AWS in file gateway mode. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.
- B. Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.
- C. Use Amazon DynamoDB with SSL to connect to DynamoDB. Use an AWS KMS key to encrypt DynamoDB objects at rest.
- D. Deploy instances with Amazon EBS volumes attached to store this data. Use EBS volume encryption using an AWS KMS key to encrypt the data.

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

if you have come far it means that you are persistent, good luck in your exam
upvoted 9 times

 **easytoo** 3 months, 1 week ago

My man. Respect, we are all cloud brothers here.
upvoted 6 times

 **SK_Tyagi** Most Recent 1 month ago

Selected Answer: B

Easy breezy
upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

its a b
upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: B

At least an easy one - the provided configuration for S3 in B satisfies the requirements for encryption, durability and availability
upvoted 1 times

 **Alabi** 3 months, 1 week ago

Selected Answer: B

B for sure
upvoted 1 times

 **erhard** 3 months, 1 week ago

Not C because _large_ documents and
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/ServiceQuotas.html#limits-items>
upvoted 1 times

 **Alabi** 3 months, 2 weeks ago

Selected Answer: B

Definitely B
upvoted 1 times

 **kfrum4** 3 months, 2 weeks ago

Selected Answer: B

Answer: B
upvoted 1 times

 **AMEJack** 4 months ago

Selected Answer: B

Answer is B

upvoted 2 times

 **Roontha** 4 months ago

Answer : B

upvoted 2 times

Question #183

Topic 1

A company's public API runs as tasks on Amazon Elastic Container Service (Amazon ECS). The tasks run on AWS Fargate behind an Application Load Balancer (ALB) and are configured with Service Auto Scaling for the tasks based on CPU utilization. This service has been running well for several months.

Recently, API performance slowed down and made the application unusable. The company discovered that a significant number of SQL injection attacks had occurred against the API and that the API service had scaled to its maximum amount.

A solutions architect needs to implement a solution that prevents SQL injection attacks from reaching the ECS API service. The solution must allow legitimate traffic through and must maximize operational efficiency.

Which solution meets these requirements?

- A. Create a new AWS WAF web ACL to monitor the HTTP requests and HTTPS requests that are forwarded to the ALB in front of the ECS tasks.
- B. Create a new AWS WAF Bot Control implementation. Add a rule in the AWS WAF Bot Control managed rule group to monitor traffic and allow only legitimate traffic to the ALB in front of the ECS tasks.
- C. Create a new AWS WAF web ACL. Add a new rule that blocks requests that match the SQL database rule group. Set the web ACL to allow all other traffic that does not match those rules. Attach the web ACL to the ALB in front of the ECS tasks.
- D. Create a new AWS WAF web ACL. Create a new empty IP set in AWS WAF. Add a new rule to the web ACL to block requests that originate from IP addresses in the new IP set. Create an AWS Lambda function that scrapes the API logs for IP addresses that send SQL injection attacks, and add those IP addresses to the IP set. Attach the web ACL to the ALB in front of the ECS tasks.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C 100%

upvoted 1 times

 **dkx** 2 months, 3 weeks ago

C. Yes, because The SQL database rule group contains rules to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. Evaluate this rule group for use if your application interfaces with an SQL database.

<https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-use-case.html>

A. No, because this does not prevent SQL injection attacks from reaching the ECS API service

B. No, because with Bot Control, you can easily monitor, block, or rate limit bots such as scrapers, scanners, crawlers, status monitors, and search engines.

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-bot-control.html>

D. No, because because this is a reactive response after a SQL injection attack has occurred for new IP addresses

upvoted 2 times

 **pupsik** 3 months ago

Selected Answer: C

C for sure

upvoted 1 times

 **Alabi** 3 months, 1 week ago

Selected Answer: C

C for sure

upvoted 1 times

 **nexus2020** 3 months, 3 weeks ago

Selected Answer: C

C; the wording is bad. rule is block, and then set the acl to allow everything else that is not matching the block rule?

B: if attacker knows what to attach, coming from a legitment IP, B will not be able to block it, but C can.

D is crazy

upvoted 1 times

 **Snape** 3 months, 4 weeks ago

Selected Answer: C

Adding new rule for blocking requests which matches SQL database rule group is more 'operationally efficient' than manually scraping API logs and IP based blocking.

upvoted 3 times

 **ShinLi** 3 months, 4 weeks ago

why not B?

upvoted 1 times

 **AMEJack** 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

 **Roontha** 4 months ago

Answer : C

<https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-use-case.html>

upvoted 3 times

 **deegadaze1** 4 months ago

B- is correct---> AWS WAF Bot Control

upvoted 1 times

Question #184

Topic 1

An environmental company is deploying sensors in major cities throughout a country to measure air quality. The sensors connect to AWS IoT Core to ingest timeseries data readings. The company stores the data in Amazon DynamoDB.

For business continuity, the company must have the ability to ingest and store data in two AWS Regions.

Which solution will meet these requirements?

- A. Create an Amazon Route 53 alias failover routing policy with values for AWS IoT Core data endpoints in both Regions. Migrate data to Amazon Aurora global tables.
- B. Create a domain configuration for AWS IoT Core in each Region. Create an Amazon Route 53 latency-based routing policy. Use AWS IoT Core data endpoints in both Regions as values. Migrate the data to Amazon MemoryDB for Redis and configure cross-Region replication.
- C. Create a domain configuration for AWS IoT Core in each Region. Create an Amazon Route 53 health check that evaluates domain configuration health. Create a failover routing policy with values for the domain name from the AWS IoT Core domain configurations. Update the DynamoDB table to a global table.
- D. Create an Amazon Route 53 latency-based routing policy. Use AWS IoT Core data endpoints in both Regions as values. Configure DynamoDB streams and cross-Region data replication.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

its a C

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: C

The only answer which configures DynamoDB properly for multi-region is C

upvoted 1 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: C

Removed B because is replacing Dynamo, unnecessary

upvoted 1 times

 **F_Eldin** 3 months, 4 weeks ago

Selected Answer: C

<https://aws.amazon.com/solutions/implementations/disaster-recovery-for-aws-iot/>

A, B Wrong. No need to replace DynamoDB with any other DB. DynamoDB Global Table is enough

D- Wrong, Not a use-case for Change Data Capture through Streams

upvoted 3 times

 **andreitugui** 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

 **Roontha** 4 months ago

Answer: C

upvoted 1 times

Question #185

Topic 1

A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company's finance team has a data processing application that uses AWS Lambda and Amazon DynamoDB. The company's marketing team wants to access the data that is stored in the DynamoDB table.

The DynamoDB table contains confidential data. The marketing team can have access to only specific attributes of data in the DynamoDB table. The finance team and the marketing team have separate AWS accounts.

What should a solutions architect do to provide the marketing team with the appropriate access to the DynamoDB table?

- A. Create an SCP to grant the marketing team's AWS account access to the specific attributes of the DynamoDB table. Attach the SCP to the OU of the finance team.
- B. Create an IAM role in the finance team's account by using IAM policy conditions for specific DynamoDB attributes (fine-grained access control). Establish trust with the marketing team's account. In the marketing team's account, create an IAM role that has permissions to assume the IAM role in the finance team's account.
- C. Create a resource-based IAM policy that includes conditions for specific DynamoDB attributes (fine-grained access control). Attach the policy to the DynamoDB table. In the marketing team's account, create an IAM role that has permissions to access the DynamoDB table in the finance team's account.
- D. Create an IAM role in the finance team's account to access the DynamoDB table. Use an IAM permissions boundary to limit the access to the specific attributes. In the marketing team's account, create an IAM role that has permissions to assume the IAM role in the finance team's account.

 **andreitugui**  4 months ago

Selected Answer: B

Answer is B

upvoted 5 times

 **AMohanty**  4 weeks, 1 day ago

For Cross Account permission we attach Resource Policy with Principal identified as incoming Request Account ARN + IAM permissions to query the Finance Account.

C seems more of a resonable answer.

upvoted 1 times

 **chikorita** 3 weeks, 1 day ago

i dont think C can address the requirement of "he marketing team can have access to only specific attributes of data in the DynamoDB table" hence, B

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct C.

upvoted 1 times

 **Gmail78** 1 month ago

While resource-based policies can provide granular access control, they are typically used for controlling access within the same AWS account. Cross-account access control is typically achieved using IAM roles with trust relationships. It is B.

upvoted 1 times

 **AMohanty** 4 weeks, 1 day ago

No, Resource based policies can specify which Principals to give access to Cross Account.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B. DynamoDB fine-grained access using IAM

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: B

B for sure.

Key word: trust

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: B

D would be the perfect choice, since the boundaries are the "new fancy thing" but it's lacking the trust to the marketing account which is a requirement to assume role from one account to another. So it should be B

upvoted 2 times

 **Alabi** 3 months, 1 week ago

Selected Answer: B

B for sure.

Key word: trust

upvoted 1 times

 **kfrum4** 3 months, 2 weeks ago

Selected Answer: B

Answer: B

DynamoDB doesn't support resource based policy

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/using-identity-based-policies.html>

upvoted 1 times

 **ggrodsckiy** 2 months ago

That is not correct. DynamoDB does support resource-based policies for tables and indexes. You can attach a resource-based policy to a DynamoDB table or index to specify who can access that resource and under what conditions. You can also use resource-based policies to grant cross-account access or fine-grained access control for specific DynamoDB attributes. For more information, please refer to this documentation: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/using-identity-based-policies.html>

upvoted 1 times

 **Rajivjain** 3 months, 3 weeks ago

Selected Answer: C

Resource-based IAM policy

upvoted 1 times

 **Roontha** 4 months ago

Answer : B

upvoted 2 times

Question #186

Topic 1

A solutions architect is creating an application that stores objects in an Amazon S3 bucket. The solutions architect must deploy the application in two AWS Regions that will be used simultaneously. The objects in the two S3 buckets must remain synchronized with each other.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

- A. Create an S3 Multi-Region Access Point Change the application to refer to the Multi-Region Access Point
- B. Configure two-way S3 Cross-Region Replication (CRR) between the two S3 buckets
- C. Modify the application to store objects in each S3 bucket
- D. Create an S3 Lifecycle rule for each S3 bucket to copy objects from one S3 bucket to the other S3 bucket
- E. Enable S3 Versioning for each S3 bucket
- F. Configure an event notification for each S3 bucket to invoke an AWS Lambda function to copy objects from one S3 bucket to the other S3 bucket

 **SK_Tyagi** 1 month ago

Selected Answer: ABE

Reason as explained by everyone

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: ABE

ABE for sure

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: ABE

Cross Region Replication(CRR) requires versioning to be activated due to the way that data is replicated between S3 buckets.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiRegionAccessPointRequestRouting.html>

<https://stackoverflow.com/questions/60947157/aws-s3-replication-without-versioning#:~:text=The%20automated%20Same%20Region%20Replication,is%20replicated%20between%20S3%20buckets.>
upvoted 2 times

 **chathur** 3 months, 3 weeks ago

Selected Answer: ABE

A - Multi Region Access points are like a proxy. It can dynamically request traffic to the nearest S3 bucket (latency based). [1]

B - Two way replication must be enabled to have data in sync. [1]

E - Versioning must be enabled for Replication. [3]

[1] <https://aws.amazon.com/s3/features/multi-region-access-points/>

[2] <https://aws.amazon.com/about-aws/whats-new/2020/12/amazon-s3-replication-adds-support-two-way-replication/>

[3] <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html#two-way-replication-scenario#:~:text=Both%20source%20and%20destination%20buckets%20must%20have%20versioning%20enabled.%20For%20more%20information%20about%20versioning%2C%20see%20Using%20versioning%20in%20S3%20buckets.>
upvoted 4 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: ABE

I only chosen E because the other options were not making much sense. I guess we need versioning in order to use two-way replication.

upvoted 3 times

 **Jesuisleon** 3 months, 3 weeks ago

yes, Cross Region Replication can be implemented only when the versioning of both the buckets is enabled.

upvoted 1 times

 **Snape** 3 months, 4 weeks ago

Selected Answer: ABE

A. Create an S3 Multi-Region Access Point. - this gives you Single Endpoint for accessing S3 into multiple regions

B. Configure CRR between the two S3 - For automatic replication to different region

E. Enable S3 Versioning on both S3 - Will give you an ability to track and recover from previous versions if needed

C, D and F doesn't meet the criteria from LEAST operation overhead perspective.

upvoted 3 times

✉ **F_Eldin** 3 months, 4 weeks ago

Selected Answer: ABE

If the reason for E is not obvious then read this:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html>

Both source and destination buckets must have versioning enabled.

upvoted 3 times

✉ **Bobbyyy** 4 months ago

Cross Region Replication(CRR) requires versioning to be activated due to the way that data is replicated between S3 buckets.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiRegionAccessPointRequestRouting.html>

<https://stackoverflow.com/questions/60947157/aws-s3-replication-without-versioning#:~:text=The%20automated%20Same%20Region%20Replication,is%20replicated%20between%20S3%20buckets.>

upvoted 1 times

✉ **AMEJack** 4 months ago

Selected Answer: ABE

Answer is A B E

upvoted 1 times

✉ **Roontha** 4 months ago

Answer : A,B,E

upvoted 2 times

Question #187

Topic 1

A company has an IoT platform that runs in an on-premises environment. The platform consists of a server that connects to IoT devices by using the MQTT protocol. The platform collects telemetry data from the devices at least once every 5 minutes. The platform also stores device metadata in a MongoDB cluster.

An application that is installed on an on-premises machine runs periodic jobs to aggregate and transform the telemetry and device metadata. The application creates reports that users view by using another web application that runs on the same on-premises machine. The periodic jobs take 120-600 seconds to run. However, the web application is always running.

The company is moving the platform to AWS and must reduce the operational overhead of the stack.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

- A. Use AWS Lambda functions to connect to the IoT devices
- B. Configure the IoT devices to publish to AWS IoT Core
- C. Write the metadata to a self-managed MongoDB database on an Amazon EC2 instance
- D. Write the metadata to Amazon DocumentDB (with MongoDB compatibility)
- E. Use AWS Step Functions state machines with AWS Lambda tasks to prepare the reports and to write the reports to Amazon S3. Use Amazon CloudFront with an S3 origin to serve the reports
- F. Use an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with Amazon EC2 instances to prepare the reports. Use an ingress controller in the EKS cluster to serve the reports

 **SK_Tyagi** 1 month ago

Selected Answer: BDE

F is EKS on EC2 and question is Least Operational overhead

upvoted 1 times

 **softarts** 1 month, 2 weeks ago

E=> how does step function run periodic jobs?

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct BDE.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: BDE

BDE for sure

upvoted 1 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: BDE

Not A - lambda to connect to IoT is no good

Not C - ec2 instance to run MongoDB

E or F - the job should be short 600 seconds top and serve the reports using Cloud Front - E

upvoted 3 times

 **andreitugui** 4 months ago

Selected Answer: BDE

Answer is B D E

upvoted 1 times

 **AMEJack** 4 months ago

Selected Answer: BDE

Support B D E

upvoted 3 times

 **Roontha** 4 months ago

Answer : B,D,E

<https://aws.amazon.com/step-functions/use-cases/>

upvoted 3 times

✉  **deegadaze1** 4 months ago

Correct is ABD

upvoted 1 times

✉  **ShinLi** 4 months ago

why E is wrong?

upvoted 1 times

Question #188

Topic 1

A global manufacturing company plans to migrate the majority of its applications to AWS. However, the company is concerned about applications that need to remain within a specific country or in the company's central on-premises data center because of data regulatory requirements or requirements for latency of single-digit milliseconds. The company also is concerned about the applications that it hosts in some of its factory sites, where limited network infrastructure exists.

The company wants a consistent developer experience so that its developers can build applications once and deploy on premises, in the cloud, or in a hybrid architecture. The developers must be able to use the same tools, APIs, and services that are familiar to them.

Which solution will provide a consistent hybrid experience to meet these requirements?

- A. Migrate all applications to the closest AWS Region that is compliant. Set up an AWS Direct Connect connection between the central on-premises data center and AWS. Deploy a Direct Connect gateway.
- B. Use AWS Snowball Edge Storage Optimized devices for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds. Retain the devices on premises. Deploy AWS Wavelength to host the workloads in the factory sites.
- C. Install AWS Outposts for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds. Use AWS Snowball Edge Compute Optimized devices to host the workloads in the factory sites.
- D. Migrate the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds to an AWS Local Zone. Deploy AWS Wavelength to host the workloads in the factory sites.

 **geoakes** Highly Voted 4 months ago

Selected Answer: C

Key comment: "specific country or in the company's central on-premises data center because of data regulatory requirements or requirements for latency of single-digit milliseconds."

A - No - Region doesn't assure you have in country presence for data sovereignty

B - No - Snowball part is correct. However, Wavelength access is only via mobile networks, and not in every country, so this is not possible unless all developers are connecting over the mobile network that will have speed variations

D - No - Local Zones can be fast with a DX connection, but this option like Wavelength is not in every country

Correct answer is C. 100% of the time you are on premise providing single-digit milliseconds latency as Outposts (rack or server) and Snowball will be in the country for the requirements

upvoted 7 times

 **SK_Tyagi** Most Recent 1 month ago

Selected Answer: C

Wavelength doesn't make sense here

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C works

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: C

Wasn't sure about Snowball Edge compute optimized to run workloads, but it appears to be quite capable option.

Ref: <https://docs.aws.amazon.com/snowball/latest/developer-guide/whatisedge.html#edge-related>

upvoted 2 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: C

short decision based on brief search

Not B nor D - <https://aws.amazon.com/wavelength/>

A will not meet the millisecond requirement

upvoted 1 times

 **Nash101** 4 months ago

Answer C

Installing AWS Outposts for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds will provide a fully managed service that extends AWS infrastructure, services, APIs, and tools to customer premises¹. AWS Outposts allows customers to run some AWS services locally and connect to a broad range of services available in the local AWS Region¹. Using AWS Snowball Edge Compute Optimized devices to host the workloads in the factory sites will provide local compute and storage resources for locations with limited network infrastructure². AWS Snowball Edge devices can run Amazon EC2 instances and AWS Lambda functions locally and sync data with AWS when network connectivity is available².

upvoted 3 times

✉ **Roontha** 4 months ago

Answer : C

Reference : <https://aws.amazon.com/blogs/compute/aws-local-zones-and-aws-outposts-choosing-the-right-technology-for-your-edge-workload/#:~:text=Unlike%20Outposts%2C%20which%20you%20deploy,using%20for%20an%20AWS%20Region>

Local Zones and Outposts can both help you achieve low latency for their latency sensitive workloads. With Direct Connect available in Local Zones, you can achieve low single-digit millisecond latencies, required for applications in online gaming, Media and Entertainment, some SaaS services, AR and VR content delivery etc.

Because Outposts are installed on premises of customers or their data centers, you can achieve under 1 millisecond latencies for workloads that require it.

upvoted 2 times

✉ **Masonryeh** 4 months ago

Selected Answer: D

Local Zone reduce the latency issue

upvoted 2 times

✉ **geoakes** 4 months ago

Yes, a local zone reduces latency, but local zones are not in every country. The closest thing to an every country option is Snowball and Outpost

upvoted 1 times

✉ **Roontha** 4 months ago

@Masonryeh, can you review this AWS information page on local zones and outposts, confirm your answer again.

<https://aws.amazon.com/blogs/compute/aws-local-zones-and-aws-outposts-choosing-the-right-technology-for-your-edge-workload/#:~:text=Unlike%20Outposts%2C%20which%20you%20deploy,using%20for%20an%20AWS%20Region>.

upvoted 1 times

✉ **ShinLi** 4 months ago

<https://docs.aws.amazon.com/wavelength/latest/developerguide/what-is-wavelength.html>

upvoted 1 times

✉ **Roontha** 3 months, 3 weeks ago

Answer : C

<https://aws.amazon.com/blogs/compute/aws-local-zones-and-aws-outposts-choosing-the-right-technology-for-your-edge-workload/#:~:text=Unlike%20Outposts%2C%20which%20you%20deploy,using%20for%20an%20AWS%20Region>.

What is Outposts?

Outposts is a family of fully managed solutions delivering AWS infrastructure and services to virtually any on-premises or edge location for a truly consistent hybrid experience.

upvoted 1 times

✉ **geoakes** 4 months ago

Wavelength is not present in every country with a datacenter, so B and D options are automatically wrong

upvoted 1 times

Question #189

Topic 1

A company is updating an application that customers use to make online orders. The number of attacks on the application by bad actors has increased recently.

The company will host the updated application on an Amazon Elastic Container Service (Amazon ECS) cluster. The company will use Amazon DynamoDB to store application data. A public Application Load Balancer (ALB) will provide end users with access to the application. The company must prevent attacks and ensure business continuity with minimal service interruptions during an ongoing attack.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Create an Amazon CloudFront distribution with the ALB as the origin. Add a custom header and random value on the CloudFront domain. Configure the ALB to conditionally forward traffic if the header and value match.
- B. Deploy the application in two AWS Regions. Configure Amazon Route 53 to route to both Regions with equal weight.
- C. Configure auto scaling for Amazon ECS tasks Create a DynamoDB Accelerator (DAX) cluster.
- D. Configure Amazon ElastiCache to reduce overhead on DynamoDB.
- E. Deploy an AWS WAF web ACL that includes an appropriate rule group. Associate the web ACL with the Amazon CloudFront distribution.

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: AE

its AE

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: AE

The only options that helps to protect are A E

upvoted 1 times

 **Jackhemo** 3 months ago

Selected Answer: AE

From Olabiba.ai:

Option A: By adding a custom header and random value on the CloudFront domain and configuring the ALB to conditionally forward traffic if the header and value match, you can implement a form of request validation. This helps to filter out potentially malicious requests and prevent attacks from reaching the application.

- Option E: Deploying an AWS WAF web ACL that includes an appropriate rule group and associating it with the Amazon CloudFront distribution adds an additional layer of protection. The web ACL can include rules to block common attack patterns and provide protection against various types of attacks, such as SQL injection and cross-site scripting (XSS).

upvoted 1 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: AE

its a combination of steps, only two of them mention cloud front A and E. it would also be the cheapest option to protect against attacks without having to increase unnecessary performance to the infrastructure which would only cost more money (setup additional region - B , configure auto scaling for ECS and add a DAX - C, configure caching , D).

upvoted 3 times

 **andreitugui** 4 months ago

Selected Answer: AE

The only options that helps to protect are A E

upvoted 2 times

 **Roontha** 4 months ago

Answer : A E

upvoted 1 times

Question #190

Topic 1

A company runs a web application on AWS. The web application delivers static content from an Amazon S3 bucket that is behind an Amazon CloudFront distribution. The application serves dynamic content by using an Application Load Balancer (ALB) that distributes requests to a fleet of Amazon EC2 instances in Auto Scaling groups. The application uses a domain name setup in Amazon Route 53.

Some users reported occasional issues when the users attempted to access the website during peak hours. An operations team found that the ALB sometimes returned HTTP 503 Service Unavailable errors. The company wants to display a custom error message page when these errors occur. The page should be displayed immediately for this error code.

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

- A. Set up a Route 53 failover routing policy. Configure a health check to determine the status of the ALB endpoint and to fail over to the failover S3 bucket endpoint.
- B. Create a second CloudFront distribution and an S3 static website to host the custom error page. Set up a Route 53 failover routing policy. Use an active-passive configuration between the two distributions.
- C. Create a CloudFront origin group that has two origins. Set the ALB endpoint as the primary origin. For the secondary origin, set an S3 bucket that is configured to host a static website. Set up origin failover for the CloudFront distribution. Update the S3 static website to incorporate the custom error page.
- D. Create a CloudFront function that validates each HTTP response code that the ALB returns. Create an S3 static website in an S3 bucket. Upload the custom error page to the S3 bucket as a failover. Update the function to read the S3 bucket and to serve the error page to the end users.

 **bur4an** 1 week, 5 days ago

Repeat question?

upvoted 1 times

 **kjcncjek** 3 weeks, 3 days ago

why not A?

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

it's a C

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: C

Origin Groups in CloudFront is what we need here.

upvoted 1 times

 **Jackhemo** 3 months ago

Selected Answer: C

From olabiba.ai:

By using a CloudFront origin group with two origins, you can configure failover between the ALB endpoint and the S3 bucket hosting the static website. This ensures that if the ALB returns HTTP 503 Service Unavailable errors, CloudFront will automatically failover to the S3 bucket and serve the custom error page.

Setting up origin failover for the CloudFront distribution allows for immediate failover to the secondary origin when the primary origin is unavailable. This minimizes the impact of the ALB errors and provides a seamless experience for users by displaying the custom error page.

Updating the S3 static website to incorporate the custom error page ensures that the error page is readily available and can be served to users without any additional processing or delays.

upvoted 2 times

 **rbm2023** 3 months, 4 weeks ago

Almost went for D but this would take too much operational overhead.

upvoted 2 times

 **rbm2023** 3 months, 4 weeks ago

Option C

upvoted 1 times

 **andreitugui** 4 months ago

Selected Answer: C

Answer is C, you can use origin groups and configure error response pages in Cloud Front based on different request response codes (503, 404, 403 etc)

upvoted 2 times

 **Roontha** 4 months ago

Answer : C

<https://repost.aws/knowledge-center/cloudfront-distribution-serve-content>

upvoted 3 times

Question #191

Topic 1

A company is planning to migrate an application to AWS. The application runs as a Docker container and uses an NFS version 4 file share.

A solutions architect must design a secure and scalable containerized solution that does not require provisioning or management of the underlying infrastructure.

Which solution will meet these requirements?

- A. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Use Amazon Elastic File System (Amazon EFS) for shared storage. Reference the EFS file system ID, container mount point, and EFS authorization IAM role in the ECS task definition.
- B. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Use Amazon FSx for Lustre for shared storage. Reference the FSx for Lustre file system ID, container mount point, and FSx for Lustre authorization IAM role in the ECS task definition.
- C. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type and auto scaling turned on. Use Amazon Elastic File System (Amazon EFS) for shared storage. Mount the EFS file system on the ECS container instances. Add the EFS authorization IAM role to the EC2 instance profile.
- D. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type and auto scaling turned on. Use Amazon Elastic Block Store (Amazon EBS) volumes with Multi-Attach enabled for shared storage. Attach the EBS volumes to ECS container instances. Add the EBS authorization IAM role to an EC2 instance profile.

 **Christina666** 2 months, 2 weeks ago

Selected Answer: A

Amazon EFS is a managed NAS filer for EC2 instances based on Network File System (NFS) version 4.

upvoted 3 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A for sure

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: A

A is correct

B Fsx For Lustre is POSIX Compilance not is correct in this question

C and D usage EC2 more overhead administrative is incorrect

upvoted 2 times

 **Gishpi** 2 months, 2 weeks ago

EFS is POSIX Compliant too. A is correct, because EFS file systems can be accessed by Amazon EC2 Linux instances, Amazon ECS, Amazon EKS, AWS Fargate, and AWS Lambda functions via a file system interface such as NFS protocol.

upvoted 2 times

 **Maria2023** 3 months ago

Selected Answer: A

<https://aws.amazon.com/fsx/when-to-choose-fsx/>

upvoted 2 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: A

Must be fargate due to the "not require provisioning or management of the underlying infra"

A or B , tie breaker using EFS and not FSx

Hence option A.

upvoted 1 times

 **andreitugui** 4 months ago

Selected Answer: A

The correct answer is A, fargate(no infra management) & efs for NFSv4

upvoted 1 times

 **deegadaze1** 4 months ago

A is correct due to -- NFS version 4.

upvoted 3 times

 **Roontha** 4 months ago

Answer : A

<https://aws.amazon.com/about-aws/whats-new/2017/03/amazon-elastic-file-system-amazon-efs-now-supports-nfsv4-lock-upgrading-and-downgrading/>

upvoted 1 times

Question #192

Topic 1

A company is running an application in the AWS Cloud. The core business logic is running on a set of Amazon EC2 instances in an Auto Scaling group. An Application Load Balancer (ALB) distributes traffic to the EC2 instances. Amazon Route 53 record api.example.com is pointing to the ALB.

The company's development team makes major updates to the business logic. The company has a rule that when changes are deployed, only 10% of customers can receive the new logic during a testing window. A customer must use the same version of the business logic during the testing window.

How should the company deploy the updates to meet these requirements?

- A. Create a second ALB, and deploy the new logic to a set of EC2 instances in a new Auto Scaling group. Configure the ALB to distribute traffic to the EC2 instances. Update the Route 53 record to use weighted routing, and point the record to both of the ALBs.
- B. Create a second target group that is referenced by the ALB. Deploy the new logic to EC2 instances in this new target group. Update the ALB listener rule to use weighted target groups. Configure ALB target group stickiness.
- C. Create a new launch configuration for the Auto Scaling group. Specify the launch configuration to use the AutoScalingRollingUpdate policy, and set the MaxBatchSize option to 10. Replace the launch configuration on the Auto Scaling group. Deploy the changes.
- D. Create a second Auto Scaling group that is referenced by the ALB. Deploy the new logic on a set of EC2 instances in this new Auto Scaling group. Change the ALB routing algorithm to least outstanding requests (LOR). Configure ALB session stickiness.

 **aviathor** 1 month, 1 week ago

The problem I have with B is that it does not mention stickiness. The problem I have with A is that the stickiness will work only as long as the DNS entry does not time out...

upvoted 1 times

 **aviathor** 1 month, 1 week ago

Oops. It does mention stickiness...

upvoted 1 times

 **ggrodskiy** 2 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B better

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

B) Classic usage of Blue/Green deployment

A is good option but not have a stickiness with Route 53 more appropriate is ALB with stickiness

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: B

<https://docs.aws.amazon.com/prescriptive-guidance/latest/load-balancer-stickiness/target-group-stickiness.html>

upvoted 1 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: B

Agree with B

blue green deployment, using target group

upvoted 3 times

 **rbm2023** 3 months, 4 weeks ago

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/>

upvoted 1 times

 **F_Eldin** 3 months, 4 weeks ago

Selected Answer: B

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/>

upvoted 2 times

 **Roontha** 4 months ago

Answer : B

<https://medium.com/capital-one-tech/deploying-with-confidence-strategies-for-canary-deployments-on-aws-7cab3798823e>

upvoted 2 times

Question #193

Topic 1

A large education company recently introduced Amazon Workspaces to provide access to internal applications across multiple universities. The company is storing user profiles on an Amazon FSx for Windows File Server file system. The file system is configured with a DNS alias and is connected to a self-managed Active Directory. As more users begin to use the Workspaces, login time increases to unacceptable levels.

An investigation reveals a degradation in performance of the file system. The company created the file system on HDD storage with a throughput of 16 MBps. A solutions architect must improve the performance of the file system during a defined maintenance window.

What should the solutions architect do to meet these requirements with the LEAST administrative effort?

- A. Use AWS Backup to create a point-in-time backup of the file system. Restore the backup to a new FSx for Windows File Server file system. Select SSD as the storage type. Select 32 MBps as the throughput capacity. When the backup and restore process is completed, adjust the DNS alias accordingly. Delete the original file system.
- B. Disconnect users from the file system. In the Amazon FSx console, update the throughput capacity to 32 MBps. Update the storage type to SSD. Reconnect users to the file system.
- C. Deploy an AWS DataSync agent onto a new Amazon EC2 instance. Create a task. Configure the existing file system as the source location. Configure a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput as the target location. Schedule the task. When the task is completed, adjust the DNS alias accordingly. Delete the original file system.
- D. Enable shadow copies on the existing file system by using a Windows PowerShell command. Schedule the shadow copy job to create a point-in-time backup of the file system. Choose to restore previous versions. Create a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput. When the copy job is completed, adjust the DNS alias. Delete the original file system.

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

Selected Answer: A

B is wrong :

<https://aws.amazon.com/fsx/windows/faqs/#:~:text=A%3A%20While%20you%20cannot%20change,with%20a%20different%20storage%20type.>

I can modify the capacity, but not the type.

upvoted 7 times

 **Jonalb** Most Recent 2 months, 1 week ago

Selected Answer: A

A or D

Its corret more certain A

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

go with A

upvoted 1 times

 **javitech83** 2 months, 3 weeks ago

Selected Answer: A

correct is A. There is a maintenance windows so there can be service outage

upvoted 1 times

 **TECHNOWARRIOR** 3 months, 1 week ago

Selected answer A: Considering the time constraints of the maintenance window and the requirement for the least administrative effort, it might be more efficient to focus on optimizing the existing file system directly. This could involve adjusting the storage configuration, increasing throughput, or optimizing the file system settings to improve performance.

By concentrating on the file system itself, the administrative effort can be minimized, and the maintenance window can be utilized more effectively to address the degradation in performance. This approach allows for a targeted and streamlined solution without introducing the complexities of deploying and managing DataSync.

upvoted 1 times

 **chathur** 3 months, 3 weeks ago

Selected Answer: A

C is wrong as datasync does need an agent to migrate data between two AWS Services.

upvoted 1 times

 **Jesuisleon** 4 months ago

A is correct.

C "Deploy an aws datasync agent onto a new amazon ec2 instance" is not right, should be

"Deploy an aws datasync agent as an amazon ec2 instance", see

<https://docs.aws.amazon.com/datasync/latest/userguide/deploy-agents.html#ec2-deploy-agent>

"To learn how to transfer files from an existing in-cloud file system to your FSx for Windows File Server, see Deploy your agent as an Amazon EC2 instance in the AWS DataSync User Guide. "

Backup can also do the backups for FSx

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/using-backups.html#aws-backup-and-fsx>

upvoted 1 times

✉ **Jesuisleon** 4 months ago

"We recommend using AWS DataSync to transfer data between FSx for Windows File Server file systems. DataSync is a data transfer service that simplifies, automates, and accelerates moving and replicating data between on-premises storage systems and other AWS storage services over the internet or AWS Direct Connect. " <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html>

here we can see datasync is used between on-premises and aws storage services. the scenario in the question is already in aws. so datasync is not right.

upvoted 1 times

✉ **Jesuisleon** 4 months ago

Q: Can I change the storage type (SSD/HDD) of my file system?

"A: While you cannot change the storage type on your existing file system, you can take a backup and restore that backup to a new file system with a different storage type."

from <https://aws.amazon.com/fsx/windows/faqs/>

here " take a backup and restore" also proves aws backup is the right answer.

upvoted 3 times

✉ **ShinLi** 4 months ago

Selected Answer: B

I am thinking is B. Refer <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-throughput-capacity.html>

upvoted 3 times

✉ **ShinLi** 3 months, 4 weeks ago

my bad, change answer to A, as it needs change disk type as well

Q: Can I change the storage type (SSD/HDD) of my file system?

A: While you cannot change the storage type on your existing file system, you can take a backup and restore that backup to a new file system with a different storage type.

upvoted 1 times

✉ **Roontha** 4 months ago

Answer : C

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html>

upvoted 2 times

✉ **Roontha** 4 months ago

Agree with Answer : A

<https://www.youtube.com/watch?v=pGZhlg6-gqY>

(AWS re:Invent 2020: Deep dive on Amazon FSx for Windows File Server)

C option is valid only when end user want to perform individual files/folders (i.e self service).

But question is asking about entire system

upvoted 1 times

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

Still sticking with C as per <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html#migrating-between-two-systems>

upvoted 1 times

✉ **geoakes** 3 months, 3 weeks ago

Not C. Why I would go with A is that the question states "during a defined maintenance window." - DataSync tends to be more than just a maintenance window that the service is operating. So 'A' makes the most sense. Maintenance window also implies any clients that need disconnecting / reconnecting as well plus your not adding to operational overhead of new services and instances

upvoted 1 times

Question #194

Topic 1

A company hosts an application on AWS. The application reads and writes objects that are stored in a single Amazon S3 bucket. The company must modify the application to deploy the application in two AWS Regions.

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

- A. Set up an Amazon CloudFront distribution with the S3 bucket as an origin. Deploy the application to a second Region. Modify the application to use the CloudFront distribution. Use AWS Global Accelerator to access the data in the S3 bucket.
- B. Create a new S3 bucket in a second Region. Set up bidirectional S3 Cross-Region Replication (CRR) between the original S3 bucket and the new S3 bucket. Configure an S3 Multi-Region Access Point that uses both S3 buckets. Deploy a modified application to both Regions.
- C. Create a new S3 bucket in a second Region. Deploy the application in the second Region. Configure the application to use the new S3 bucket. Set up S3 Cross-Region Replication (CRR) from the original S3 bucket to the new S3 bucket.
- D. Set up an S3 gateway endpoint with the S3 bucket as an origin. Deploy the application to a second Region. Modify the application to use the new S3 gateway endpoint. Use S3 Intelligent-Tiering on the S3 bucket.

 **MasterP007** 1 month, 2 weeks ago

Selected Answer: B

Option B creates a new S3 bucket in a second Region and sets up bidirectional S3 Cross-Region Replication (CRR) between the original S3 bucket and the new S3 bucket. S3 CRR is a feature that enables automatic, asynchronous copying of objects across S3 buckets in different AWS Regions. You can use S3 CRR to keep your data synchronized across Regions for lower latency, compliance, security, disaster recovery, and regional efficiency.

upvoted 1 times

 **azizmo** 1 month, 4 weeks ago

Selected Answer: B

The answer is B

upvoted 1 times

 **nicecurls** 2 months, 2 weeks ago

Selected Answer: B

it's a B

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

its a B

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

the "stored in a single Amazon S3 bucket" comment is confusing though. have to assume new versionn will have buckets in each region
upvoted 2 times

 **phattran** 2 months, 3 weeks ago

Selected Answer: B

S3 CRR prefer S3 Multi-Region Access Point

upvoted 1 times

 **YodaMaster** 2 months, 3 weeks ago

B sounds right for deploying in 2 different regions though.

upvoted 1 times

 **YodaMaster** 2 months, 3 weeks ago

this question seems incomplete?

upvoted 1 times

 **Masonryeh** 4 months ago

B, enable the S3 sync

upvoted 3 times

 **Roontha** 4 months ago

Answer : B

<https://aws.amazon.com/s3/features/multi-region-access-points/>

upvoted 2 times

Question #195

Topic 1

An online gaming company needs to rehost its gaming platform on AWS. The company's gaming application requires high performance computing (HPC) processing and has a leaderboard that changes frequently. An Ubuntu instance that is optimized for compute generation hosts a Node.js application for game display. Game state is tracked in an on-premises Redis instance.

The company needs a migration strategy that optimizes application performance.

Which solution will meet these requirements?

- A. Create an Auto Scaling group of m5.large Amazon EC2 Spot Instances behind an Application Load Balancer. Use an Amazon ElastiCache for Redis cluster to maintain the leaderboard.
- B. Create an Auto Scaling group of c5.large Amazon EC2 Spot Instances behind an Application Load Balancer. Use an Amazon OpenSearch Service cluster to maintain the leaderboard.
- C. Create an Auto Scaling group of c5.large Amazon EC2 On-Demand Instances behind an Application Load Balancer. Use an Amazon ElastiCache for Redis cluster to maintain the leaderboard.
- D. Create an Auto Scaling group of m5.large Amazon EC2 On-Demand Instances behind an Application Load Balancer. Use an Amazon DynamoDB table to maintain the leaderboard.

 **Roontha** Highly Voted 4 months ago

Answer : C

<https://aws.amazon.com/blogs/database/building-a-real-time-gaming-leaderboard-with-amazon-elasticsearch-for-redis/>
upvoted 5 times

 **dkcloudguru** Most Recent 1 week, 6 days ago

Agree with option C

upvoted 1 times

 **SK_Tyagi** 1 month ago

Selected Answer: C

Agree with C.

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C for sure

upvoted 1 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: C

C is the way

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: C

C for sure

upvoted 1 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: C

Elastic Cache for Redis, C or D.

Both are on demand, we can't use spot

Tie breaker is the instance type c5.

upvoted 2 times

 **F_Eldin** 3 months, 4 weeks ago

Selected Answer: C

A, B : Wrong. Spot instances. B: OpenSearch instead of Redis

D: Wrong, DynamoDB instead of Redis

upvoted 1 times

andreitugui 3 months, 4 weeks ago

Selected Answer: C

The answer is C as compute optimized instance is required c5, and ElastiCache is the for Redis.

upvoted 1 times

Masonryeho 4 months ago

Agree with C

upvoted 2 times

Question #196

Topic 1

A solutions architect is designing an application to accept timesheet entries from employees on their mobile devices. Timesheets will be submitted weekly, with most of the submissions occurring on Friday. The data must be stored in a format that allows payroll administrators to run monthly reports. The infrastructure must be highly available and scale to match the rate of incoming data and reporting requests.

Which combination of steps meets these requirements while minimizing operational overhead? (Choose two.)

- A. Deploy the application to Amazon EC2 On-Demand Instances with load balancing across multiple Availability Zones. Use scheduled Amazon EC2 Auto Scaling to add capacity before the high volume of submissions on Fridays.
- B. Deploy the application in a container using Amazon Elastic Container Service (Amazon ECS) with load balancing across multiple Availability Zones. Use scheduled Service Auto Scaling to add capacity before the high volume of submissions on Fridays.
- C. Deploy the application front end to an Amazon S3 bucket served by Amazon CloudFront. Deploy the application backend using Amazon API Gateway with an AWS Lambda proxy integration.
- D. Store the timesheet submission data in Amazon Redshift. Use Amazon QuickSight to generate the reports using Amazon Redshift as the data source.
- E. Store the timesheet submission data in Amazon S3. Use Amazon Athena and Amazon QuickSight to generate the reports using Amazon S3 as the data source.

 **CloudHandsOn** 3 weeks, 2 days ago

C & E. "minimizing operational overhead" is the deciding factor between C and B. operating and managing ECS and ALB would be more cumbersome versus a more serverless approach like APIGW, Lambda, and S3.

upvoted 1 times

 **SK_Tyagi** 1 month ago

Selected Answer: CE

Least Operational overhead

upvoted 1 times

 **easystoo** 1 month, 4 weeks ago

b-e-b-e-b-e-b-e

upvoted 2 times

 **ggrodsckiy** 2 months ago

Correct CE.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: CE

CE. front-end app like angular can be hosted inn s3 and CF

upvoted 1 times

 **YodaMaster** 2 months, 3 weeks ago

oh and this from AWS which seems familiar to the question. <https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/>

upvoted 2 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: CE

- A. EC2 on-demand instances don't make sense to accept timesheet entries
 - B. ECS can be done but they want to minimise operational overhead where option C sounds better/simple
 - C. Sounds simple enough to use s3. I choose this.
 - D. I already chose s3 so this doesn't apply + redshift seems overkill
 - E. This goes with Option C
- So answer C and E

upvoted 4 times

 **Jackhemo** 3 months ago

Selected Answer: BE

Olabiba.ai said:

Option B suggests deploying the application in a container using Amazon ECS with load balancing across multiple Availability Zones. This ensures high availability and scalability by distributing the workload across multiple instances and zones. Using scheduled Service Auto Scaling allows for adding capacity before the high volume of submissions on Fridays, ensuring the application can handle the increased load.

Option E suggests storing the timesheet submission data in Amazon S3, which provides a highly durable and scalable storage solution. Amazon

Athena can be used to query the data directly from S3, and Amazon QuickSight can be used to generate the monthly reports using S3 as the data source. This combination allows for efficient data storage and reporting without the need for additional infrastructure or operational overhead.

By implementing these steps, you can achieve a highly available and scalable infrastructure while minimizing operational overhead.

upvoted 2 times

 **emiliocb4** 3 months, 1 week ago

Selected Answer: BE

i'm going with BE.

A not correct with EC2 instances to mantain.

C is not correct because we cannot host webapplication on S3 (only static contents)

D too much effort for Redshift

upvoted 2 times

 **Gmail78** 1 month ago

It looks like BE are the best options. While deploying the frontend to S3 and using API Gateway with Lambda for the backend is a good architectural approach, it might not directly address the requirement for load scaling and scheduling.

upvoted 1 times

 **hitesh24** 3 months, 3 weeks ago

Selected Answer: CE

C and E will require least operational overhead.

upvoted 2 times

 **Jesuisleon** 3 months, 3 weeks ago

Selected Answer: AE

I prefer A to C, as I didn't see why Cloudfront is necesary in C.

the mainstream is from mobile to AWS environment while cloudfront is used to cache files for a user to the nearest edge location. The question emphasize the Friday burst, but C doesn't address this scenario purposely. I think A is better than C.

upvoted 2 times

 **Darkhorse_79** 3 months, 3 weeks ago

Selected Answer: CE

Submitting timesheets is likely a pretty static site setup,, javascript based, why would you deploy a full EC2 or ECS platform when you can host it on S3 easily

upvoted 3 times

 **Jesuisleon** 3 months, 3 weeks ago

May be there are consistent verifications there for example job number check, number of projects check or completion check(some fields must be filled), when all checks passed, the forms can be saved in S3.

upvoted 1 times

 **nexus2020** 3 months, 3 weeks ago

Selected Answer: CE

minimizing operational overhead, then No EC2, NO ECS. a lot of operational work to maintain it.

upvoted 2 times

 **andreitugui** 3 months, 4 weeks ago

Selected Answer: CE

C. By deploying the application front end to an Amazon S3 bucket served by Amazon CloudFront, you can benefit from the scalability, high availability, and low latency of the S3 and CloudFront services. This combination allows for efficient content delivery and a smooth user experience on mobile devices.

Using Amazon API Gateway with an AWS Lambda proxy integration for the backend enables serverless execution and eliminates the need for managing and scaling infrastructure. It provides an efficient way to handle the timesheet submissions and i

upvoted 4 times

 **AMEJack** 4 months ago

Selected Answer: AE

Answer should be A E.

B (Wrong): Why I need to auto scale EC2 instances while scaling is managed by ECS.

D (Wrong): Why I need to run a complete Redshift environment to generate a report. Athena can do the job.

upvoted 3 times

 **nexus2020** 3 months, 3 weeks ago

For "minimizing operational overhead", For A: EC2 is not a good way as you need to maintain the OS etc. whats wrong with C?

upvoted 1 times

 **Jesuisleon** 3 months, 3 weeks ago

CloudFront is not necessary in this scenario. I didn't see the necessity to cache forms in Cloudfront.

upvoted 1 times

 **rxhan** 2 months ago

not forms but reports

upvoted 1 times

 **ShinLi** 4 months ago

Selected Answer: AD

I am thinking AD

A is less operation overhead than B. as B is not using Fargate deployment, so you need deploy EC2 anyway. and they you need manage ECS on top EC2. more layers and more operation overhead.

D: we should use redshift for report, not from S3 bucket

upvoted 1 times

 **Nash101** 4 months ago

Answer A & E

upvoted 1 times

Question #197

Topic 1

A company is storing sensitive data in an Amazon S3 bucket. The company must log all activities for objects in the S3 bucket and must keep the logs for 5 years. The company's security team also must receive an email notification every time there is an attempt to delete data in the S3 bucket.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

- A. Configure AWS CloudTrail to log S3 data events.
- B. Configure S3 server access logging for the S3 bucket.
- C. Configure Amazon S3 to send object deletion events to Amazon Simple Email Service (Amazon SES).
- D. Configure Amazon S3 to send object deletion events to an Amazon EventBridge event bus that publishes to an Amazon Simple Notification Service (Amazon SNS) topic.
- E. Configure Amazon S3 to send the logs to Amazon Timestream with data storage tiering.
- F. Configure a new S3 bucket to store the logs with an S3 Lifecycle policy.

 **cmoreira** 3 weeks, 1 day ago

Selected Answer: ADF

ADF

A or B work, but docs recommend cloud trail:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 1 times

 **study_aws1** 3 weeks, 4 days ago

A, D, F

You can record the actions that are taken by users, roles, or AWS services on Amazon S3 resources and maintain log records for auditing and compliance purposes. To do this, you can use server-access logging, AWS CloudTrail logging, or a combination of both. We recommend that you use CloudTrail for logging bucket-level and object-level actions for your Amazon S3 resources.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 1 times

 **Sweetedad** 3 weeks, 6 days ago

Selected Answer: ADF

ADF. Please read this "We recommend that you use CloudTrail for logging bucket-level and object-level actions for your Amazon S3 resources." <https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 2 times

 **vn_thanh tung** 3 weeks, 4 days ago

<https://repost.aws/knowledge-center/s3-audit-deleted-missing-objects>

agree with ADF

upvoted 1 times

 **SK_Tyagi** 1 month ago

Selected Answer: BDF

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-logging.html>

AWS CloudTrail logs provide a record of actions taken by a user, role, or an AWS service in Amazon S3, while Amazon S3 server access logs provide detailed records for the requests that are made to an S3 bucket.

upvoted 2 times

 **xav1er** 1 month ago

Selected Answer: BDF

I would go with BDF, B because server access logging can be sufficient for logging all activities on objects (not bucket itself) and is more cost-effective than cloud-trail. Close one tho :)

upvoted 3 times

 **chico2023** 1 month, 1 week ago

Selected Answer: BDF

Question says "The company must log all activities for objects in the S3 bucket." Special attention to "the S3 bucket." Now, add to the requirement "MOST cost-effectively."

This only should make you choose B instead of A. But we can go a bit further if we look here "The company must log all activities". You can check the documentation, but Olabiba can save you time with this question:

- Me: What S3 activities are logged using CloudTrail?
- Olabiba: By default, CloudTrail logs S3 bucket-level API calls that were made in the last 90 days. These bucket-level calls include events such

as CreateBucket, DeleteBucket, PutBucketLifecycle, PutBucketPolicy, and more.

However, CloudTrail does not log requests made to objects within the S3 bucket. If you need more detailed logging for object-level activities, you can enable S3 server access logging.

upvoted 3 times

easytoo 1 month, 4 weeks ago

b-d-f----b-d-f----b-d-f

upvoted 2 times

ggrodskiy 2 months ago

Correct ADF.

upvoted 1 times

totozero 2 months ago

Selected Answer: BDF

A and B have both the capability to log events for objects. But B is definitely more cost effective and sticks better with other options (like A would miss something like "and send trails to S3").

upvoted 3 times

lxrdm 2 months, 1 week ago

Selected Answer: BDF

Track all object activities is to use S3 access logs and store the log into another bucket

upvoted 2 times

Christina666 2 months, 2 weeks ago

Selected Answer: ADF

key words:

log all data events-> cloudtrail

send email for "delete events"-> event bridge rule-> ses

retain for 5 yrs-> lifecycle

upvoted 2 times

NikkyDicky 2 months, 3 weeks ago

Selected Answer: ADF

Its ADF

upvoted 1 times

YodaMaster 2 months, 3 weeks ago

Selected Answer: BDF

B makes more sense than A (for MOST cost-effective). They both track object deletions.

By default, CloudTrail records bucket-level events. To get logs for object-level operations like GetObject, DeleteObject, and PutObject, you must configure object-level logging. Object-level logging incurs additional charges, so be sure to review the pricing for CloudTrail data events.

<https://repost.aws/knowledge-center/s3-audit-deleted-missing-objects>

upvoted 2 times

SkyZeroZx 2 months, 3 weeks ago

Selected Answer: ADF

B : Wrong. Server logging has limited features compared to cloudtrail

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

CloudTrail data events can be set for all the S3 buckets for the AWS account or just for some folder in S3 bucket. Whereas, S3 server access logs would be set at individual bucket level

C: Wrong. You need Lambda to connect events to SES . SNS and eventbridge

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html#supported-notification-event-types>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/EventBridge.html>

<https://medium.com/@anirsom2012/send-email-notification-on-aws-s3-events-186acd25a401>

E: Wrong, Timestreams is an overkill.

upvoted 2 times

dkx 2 months, 3 weeks ago

Both AWS CloudTrail and Amazon S3 Server Logs capture Object operations and Bucket operations, however, for CloudTrail, data events incur a fee, in addition to storage of logs. For Amazon S3 Server Logs, no other cost in addition to storage of logs.

Thus, given this question asks how to solve MOST cost-effectively, we must conclude B, not A.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 1 times

javitech83 2 months, 4 weeks ago

Selected Answer: ADF

It must be A and not B. With B will send logs about object access. But in order to send notifications to evenbridge the delete event needs to be published in Cloudtrail, so option A is needed

upvoted 2 times

✉️  **Maria2023** 3 months ago

Selected Answer: ADF

Awful wording here. You do not actually set up S3 to send events - you create a rule in EventBridge that responds to a trigger that is "detail-type": "Object Deleted". I personally couldn't find any way to make Server access logging trigger anything.

upvoted 1 times

✉️  **Maria2023** 3 months ago

I've accidentally triggered wrong choices - it's BDF

upvoted 2 times

Question #198

A company is building a hybrid environment that includes servers in an on-premises data center and in the AWS Cloud. The company has deployed Amazon EC2 instances in three VPCs. Each VPC is in a different AWS Region. The company has established an AWS Direct Connect connection to the data center from the Region that is closest to the data center.

The company needs the servers in the on-premises data center to have access to the EC2 instances in all three VPCs. The servers in the on-premises data center also must have access to AWS public services.

Which combination of steps will meet these requirements with the LEAST cost? (Choose two.)

- A. Create a Direct Connect gateway in the Region that is closest to the data center. Attach the Direct Connect connection to the Direct Connect gateway. Use the Direct Connect gateway to connect the VPCs in the other two Regions.
- B. Set up additional Direct Connect connections from the on-premises data center to the other two Regions.
- C. Create a private VIF. Establish an AWS Site-to-Site VPN connection over the private VIF to the VPCs in the other two Regions.
- D. Create a public VIF. Establish an AWS Site-to-Site VPN connection over the public VIF to the VPCs in the other two Regions.
- E. Use VPC peering to establish a connection between the VPCs across the Regions. Create a private VIF with the existing Direct Connect connection to connect to the peered VPCs.

 **Roontha** Highly Voted 4 months ago

Answer : A, D

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-site-to-site-vpn.html>

upvoted 8 times

 **cmoreira** Most Recent 3 weeks, 1 day ago

Selected Answer: AD

There is no correct answer. NONE.

- A. Direct Connect gateway are global. You don't create them in a "region"
- B. Not needed, since you have DX-GW.
- C. Can't establish site-to-site VPN over private VIF. You do it over public or transit (recommended).
- D. Yes, should use private VIF, but for access to AWS public resources, not the other VPCs.
- E. VPC peering won't allow OnPrem to access other VPCs via peering.

Best Answer is DX-Gateway AND Public VIF (A and D). However they're both wrong.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

upvoted 3 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: AD

its AD

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: AD

Answer : A, D

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-site-to-site-vpn.html>

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: AD

got to use Public VIF in order to connect to AWS Services via Direct Connect.

upvoted 1 times

 **easytoo** 3 months ago

a-d-a-d-a-d-a-d

upvoted 1 times

 **Jesuisleon** 3 months, 3 weeks ago

Agree Roontha.

For E, "Create a private VIF with the existing Direct Connect connection to connect to the peered VPCs" is wrong. private VIF can only connect to the VPC which is in the same region with direct connection, you can't extend private VIF to the VPCs in other 2 regions.

upvoted 2 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: AD

agree with A and D tks to Roontha

upvoted 3 times

 **andreitugui** 3 months, 4 weeks ago

Selected Answer: AD

Answer is A,D

upvoted 1 times

Question #199

Topic 1

A company is using an organization in AWS Organizations to manage hundreds of AWS accounts. A solutions architect is working on a solution to provide baseline protection for the Open Web Application Security Project (OWASP) top 10 web application vulnerabilities. The solutions architect is using AWS WAF for all existing and new Amazon CloudFront distributions that are deployed within the organization.

Which combination of steps should the solutions architect take to provide the baseline protection? (Choose three.)

- A. Enable AWS Config in all accounts
- B. Enable Amazon GuardDuty in all accounts
- C. Enable all features for the organization
- D. Use AWS Firewall Manager to deploy AWS WAF rules in all accounts for all CloudFront distributions
- E. Use AWS Shield Advanced to deploy AWS WAF rules in all accounts for all CloudFront distributions
- F. Use AWS Security Hub to deploy AWS WAF rules in all accounts for all CloudFront distributions

 **Roontha** Highly Voted 4 months ago

My Answer A,C,D

<https://aws.amazon.com/blogs/security/using-aws-firewall-manager-and-waf-to-protect-your-web-applications-with-master-rules-and-application-specific-rules/>

can someone post the link if you feel my answer is incorrect
upvoted 7 times

 **ShinLi** 4 months ago

why you pickup C? why we need enable all the features?
upvoted 1 times

 **Roontha** 3 months, 3 weeks ago

@ShinLi,

C is must requirement in order leverage AWS Firewall Manager according to aws.

Prerequisites

AWS Firewall Manager has the following prerequisites:

AWS Organizations: Your organization must be using AWS Organizations to manage your accounts, and All Features must be enabled. For more information, see [Creating an Organization and Enabling All Features in Your Organization](#).
 A firewall administrator AWS Account: You must designate one of the AWS accounts in your organization as the administrator for AWS Firewall Manager. This gives the account permission to deploy AWS WAF rules across the organization.
 AWS Config: You must enable AWS Config for all of the accounts in your organization so that AWS Firewall Manager can detect newly created resources. To enable AWS Config for all of the accounts in your organization, you can use the [Enable AWS Config template](#) on the StackSets Sample Templates page. For more information, see [Getting Started with AWS Config](#).

upvoted 6 times

 **easystoo** Most Recent 1 month, 4 weeks ago

a-c-d----a-c-d----a-c-d

GuardDuty, Shield Advanced, and Security Hub provide other security capabilities but are not directly related to deploying WAF rules across all accounts and distributions.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: ACD

its ACD

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: ACD

D is clear. A and C are needed for D to work

<https://aws.amazon.com/es/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/#:~:text=Firewall%20Manager%20prerequisites>

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: ACD

ACD

Link reference : <https://aws.amazon.com/es/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/#:~:text=Firewall%20Manager%20prerequisites>

manager/#:~:text=Firewall%20Manager%20prerequisites
upvoted 3 times

easytoo 3 months ago
baseline for OWASP = b-d-f
upvoted 1 times

emilioch4 3 months, 1 week ago

Selected Answer: ACD

baseline protection vconfiguration.
A to evaluate the configurations of AWS resources
C enabling all features required by Firewall manager
D to enable the waf rules
upvoted 3 times

Jonalb 3 months, 2 weeks ago

Selected Answer: ABD

Enable AWS Config in all accounts: AWS Config provides a detailed view of the configuration of AWS resources within an organization. By enabling AWS Config, the solutions architect can track and monitor the configuration of CloudFront distributions and ensure that they adhere to the desired baseline configuration, including AWS WAF settings.

Enable Amazon GuardDuty in all accounts: Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior within AWS accounts. Enabling GuardDuty in all accounts allows for real-time threat detection and alerts related to potential web application vulnerabilities.

upvoted 1 times

SVGoogle89 3 months, 3 weeks ago

Prerequisites for using AWS Firewall Manager
Your account must be a member of AWS Organizations
Your AWS account must be a member of an organization in the AWS Organizations service, and the organization must have all features enabled.

Your account must be the AWS Firewall Manager administrator
To configure Firewall Manager policies, your account must be set as the AWS Firewall Manager administrator account, in the Settings pane.

You must have AWS Config enabled for your accounts and Regions
You must enable AWS Config for each of your AWS Organizations member accounts and for each AWS Region that contains resources that you want to protect using AWS Firewall Manager.

upvoted 1 times

Jesuisleon 3 months, 3 weeks ago

Selected Answer: ACD

A,C,D is right answer.
Infact My initial choice is B,C,D.
After I rewatch neal Davis' video, GuardDuty is intelligent thread detection service based ML,
it does continuous monitoring for : 1) CloudTrail Management events; 2) CloudTrail S3 Data Events; 3)VPC Flow Logs 4) DNS logs. so guardduty is not right in this scenario.

upvoted 3 times

chathur 3 months, 3 weeks ago

Selected Answer: ACD

The tutorial is here.

<https://aws.amazon.com/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/#:~:text=Firewall%20Manager%20prerequisites>

upvoted 1 times

Gmail78 1 month ago

I assume if you want to secure AWS you need Guard duty enabled, it also interact with AWS WAF:
<https://aws.amazon.com/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/>
upvoted 1 times

Rajivjain 3 months, 3 weeks ago

Selected Answer: BDE

Updating My Vote to BDE
Enabling Amazon GuardDuty will help monitor and detect malicious activity.
Deploying WAF rules via Firewall Manager or Shield Advanced will filter incoming traffic and block common attack patterns. These steps can help protect against many of the most common web application security risks identified by OWASP.
A (Enable AWS Config) is not directly related to providing baseline protection for web applications against OWASP's top 10 vulnerabilities.
C (Enable All Features) is too broad and does not specifically address web application security.
F (Use Security Hub) does not have a native capability to deploy WAF rules at scale.

upvoted 2 times

MnqobiZulu 3 months, 4 weeks ago

ACD.....

upvoted 1 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: CDF

It is a combination of steps, and you need to choose THREE, remember that all options should be related to the Organization wide management, so:

Option C – You need to take advantage of managing security services using Organization, hence enable all features is required in this case we have hundreds of accounts.

Option D – In the same Link above Firewall Manager is one of the listed services, you can centrally configure and manage AWS WAF rules across accounts in your organization.

upvoted 2 times

 **rbm2023** 3 months, 4 weeks ago

Option F – Again, security hub is an organization wide feature, while AWS Security Hub can provide visibility into security findings related to web application vulnerabilities detected by AWS WAF, it is AWS WAF that provides the actual protection by inspecting and filtering web traffic to your applications.

eliminating A – if you enable ALL FEATURES, you do not need this option.

eliminating B – if you enable ALL FEATURES, you do not need this option.

eliminating E - AWS Shield Advanced is a DDoS

upvoted 1 times

 **Urameshi** 3 months, 4 weeks ago

Selected Answer: ABD

A,D are correct, based on this: <https://aws.amazon.com/pt/blogs/security/using-aws-firewall-manager-and-waf-to-protect-your-web-applications-with-master-rules-and-application-specific-rules/>

I'm in doubt about the third option, but I would go with option B because Guarduty integrates with the WAF:

<https://aws.amazon.com/pt/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/>

So A, B, D are my answers.

upvoted 1 times

 **Rajivjain** 4 months ago

Selected Answer: BDF

to provide baseline protection.

upvoted 1 times

 **Rajivjain** 4 months ago

BDF is right, considering taking to provide the baseline protection.

upvoted 1 times

Question #200

Topic 1

A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on-premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal, access to the AWS environment is granted. However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment.

Which items should the solutions architect check to ensure identity federation is properly configured? (Choose three.)

- A. The IAM user's permissions policy has allowed the use of SAML federation for that user.
- B. The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.
- B. Test users are not in the AWSFederatedUsers group in the company's IdP.
- C. The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the IAM role, and the SAML assertion from IdP.
- D. The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs.
- E. The company's IdP defines SAML assertions that properly map users or groups. In the company to IAM roles with appropriate permissions.

 **Rajivjain** Highly Voted 4 months ago

Kindly correct the Answers' sequence. A to F

upvoted 12 times

 **Rajivjain** 4 months ago

Ref: BDF <https://www.examtopics.com/discussions/amazon/view/36355-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 3 times

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

B) The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.

D) The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the IAM role, and the SAML assertion from IdP.

F)The company's IdP defines SAML assertions that properly map users or groups. In the company to IAM roles with appropriate permissions.

upvoted 8 times

 **dkcloudguru** Most Recent 1 week, 6 days ago

BDF is correct

upvoted 1 times

 **CloudHandsOn** 3 weeks, 2 days ago

Selected Answer: BCE

B,C, & E was my first choice

upvoted 1 times

 **Gmail78** 4 weeks ago

C- STS AssumerolewithSAML

B1- Define trust policy for IAM assumed by the principal

E - SAML Assertion

upvoted 1 times

 **SK_Tyagi** 1 month ago

Selected Answer: BD

BDF is correct

upvoted 1 times

 **anttan** 1 month, 2 weeks ago

Should be BEF, right?

D. The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the IAM role, and the SAML assertion from IdP. This is already being done by the federated identity web portal.

So E) The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs. The on-premises IdP's DNS hostname must be reachable from the AWS environment VPCs. This is because the AWS STS AssumeRoleWithSAML API will need to be able to resolve the DNS hostname of the IdP in order to retrieve the SAML assertion.

upvoted 1 times

 **breadops** 2 months ago

Selected Answer: B

BDF is the right answers

upvoted 1 times

✉  **ggrodsckiy** 2 months ago

Correct BCE.

upvoted 1 times

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

Selected Answer: BD

Admin The Order from the Question is not right.. Answer is BDF!

upvoted 1 times

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

Selected Answer: BCE

B (the 1st B, as there are two in this version of question) CE

upvoted 2 times

✉  **easytoo** 3 months ago

it's B-D-F Jeff.

upvoted 1 times

✉  **Roontha** 4 months ago

Answer : B, C, E

upvoted 2 times

✉  **Roontha** 4 months ago

Sorry...it is BDF

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

upvoted 4 times

Question #201

Topic 1

A solutions architect needs to improve an application that is hosted in the AWS Cloud. The application uses an Amazon Aurora MySQL DB instance that is experiencing overloaded connections. Most of the application's operations insert records into the database. The application currently stores credentials in a text-based configuration file.

The solutions architect needs to implement a solution so that the application can handle the current connection load. The solution must keep the credentials secure and must provide the ability to rotate the credentials automatically on a regular basis.

Which solution will meet these requirements?

- A. Deploy an Amazon RDS Proxy layer. In front of the DB instance. Store the connection credentials as a secret in AWS Secrets Manager.
- B. Deploy an Amazon RDS Proxy layer in front of the DB instance. Store the connection credentials in AWS Systems Manager Parameter Store
- C. Create an Aurora Replica. Store the connection credentials as a secret in AWS Secrets Manager
- D. Create an Aurora Replica. Store the connection credentials in AWS Systems Manager Parameter Store.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

easy A

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: A

Agree with other explanations here.

upvoted 1 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: A

Agree with A

Rotate the keys using Secrets Manager, Param store does not cover it.

RDS Proxy is exactly to solve the issues with overloaded connection because is a connection pool component.

upvoted 3 times

 **Masonryeho** 4 months ago

Selected Answer: A

Using RDS Proxy, you can handle unpredictable surges in database traffic. Otherwise, these surges might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool. This approach avoids the memory and CPU overhead of opening a new database connection each time. To protect the database against oversubscription, you can control the number of database connections that are created.

upvoted 4 times

 **Roontha** 4 months ago

Answer : A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 3 times

Question #202

Topic 1

A company needs to build a disaster recovery (DR) solution for its ecommerce website. The web application is hosted on a fleet of t3.large Amazon EC2 instances and uses an Amazon RDS for MySQL DB instance. The EC2 instances are in an Auto Scaling group that extends across multiple Availability Zones.

In the event of a disaster, the web application must fail over to the secondary environment with an RPO of 30 seconds and an RTO of 10 minutes.

Which solution will meet these requirements MOST cost-effectively?

- A. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create a cross-Region read replica for the DB instance. Set up a backup plan in AWS Backup to create cross-Region backups for the EC2 instances and the DB instance. Create a cron expression to back up the EC2 instances and the DB instance every 30 seconds to the DR Region. Recover the EC2 instances from the latest EC2 backup. Use an Amazon Route 53 geolocation routing policy to automatically fail over to the DR Region in the event of a disaster.
- B. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create a cross-Region read replica for the DB instance. Set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. Run the EC2 instances at the minimum capacity in the DR Region. Use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster. Increase the desired capacity of the Auto Scaling group.
- C. Set up a backup plan in AWS Backup to create cross-Region backups for the EC2 instances and the DB instance. Create a cron expression to back up the EC2 instances and the DB instance every 30 seconds to the DR Region. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Manually restore the backed-up data on new instances. Use an Amazon Route 53 simple routing policy to automatically fail over to the DR Region in the event of a disaster.
- D. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create an Amazon Aurora global database. Set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. Run the Auto Scaling group of EC2 instances at full capacity in the DR Region. Use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster.

 **SK_Tyagi** 1 month ago

Selected Answer: B

Close between B & D but Max out ASG is tie-breaker

upvoted 1 times

 **softarts** 1 month, 2 weeks ago

Selected Answer: D

I think (D) only aurora global database can meet RPO 30 seconds? although B is cost-effective

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B for sure

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

A) Not seems for my , possible backup

B) Active Pasive

C) Backup

D) Active Active

Then B is correct in this case

upvoted 2 times

 **Jackhemo** 3 months, 1 week ago

olabiba.ai said B.

upvoted 1 times

 **Jonalb** 3 months, 2 weeks ago

Selected Answer: B

Explanation:

Option B leverages infrastructure as code (IaC) to provision the necessary infrastructure in the DR Region, which allows for automated and repeatable deployments.

Creating a cross-Region read replica for the Amazon RDS DB instance ensures that the database is replicated and available in the DR Region. AWS Elastic Disaster Recovery can be used to continuously replicate the EC2 instances from the primary Region to the DR Region, ensuring up-to-date copies of the application.

Running the EC2 instances at the minimum capacity in the DR Region helps reduce costs, as resources are only utilized when failover occurs. Using an Amazon Route 53 failover routing policy allows for automatic failover to the DR Region in the event of a disaster, minimizing downtime. Increasing the desired capacity of the Auto Scaling group ensures that sufficient resources are available in the DR Region to handle the workload during failover.

upvoted 3 times

Moallal 3 months, 2 weeks ago

Selected Answer: A

Do the math, option A is 5.55 days.

upvoted 1 times

Snapre 3 months, 4 weeks ago

Selected Answer: B

A Wrong - I have stopped reading after 'create cron' , Same goes with C.

D Wrong - Running ASG at full capacity in the DR is not cost efficient

upvoted 4 times

rbm2023 3 months, 4 weeks ago

i think i agree with option B, initially chosen D

the problem is that we need a cost effective solution and based on the following the global database might be more expensive and the fact the RDS cross region replication may cover the RTO of 10 minutes.

quick compare on global database and cross region replication

RDS Cross Region Replication - You will accrue charges for data transfer between Amazon EC2 and Amazon RDS across Regions, charged on both sides of the transfer (\$0.02/GB out)

Aurora Global Database - you pay for replicated write I/O operations between the primary Region and each secondary Region. The number of replicated write I/O operations to each secondary Region is the same as the number of in-Region write I/O operations performed by the primary Region Replicated Write I/Os \$0.20 per million replicated write I/Os

upvoted 2 times

andreitugui 3 months, 4 weeks ago

Selected Answer: B

I would go with B as 10minutes RTO allows for scale up the ASG size. Also read replica is cheaper and can be promoted to primary. Also aurora replication to read replica is usually much less than 100 milliseconds after the primary writes operation which will be enough for the RPO of 30 seconds.

upvoted 1 times

dbaroger 3 months, 4 weeks ago

Selected Answer: B

Cost efective = B

upvoted 2 times

AMEJack 4 months ago

Selected Answer: B

Agree with B

upvoted 1 times

Masonryeho 4 months ago

Selected Answer: C

save the running EC2 cost. Only bring up when needed

upvoted 1 times

Roontha 4 months ago

but the question is saying "web application must fail over to the secondary environment with an RPO of 30 seconds and an RTO of 10 minutes"

How RPO/RTO can be achieved with bare minimum EC2 is up and running in DR site.

Can you paste the link/reading to justify your answer.

Thanks

upvoted 3 times

Roontha 4 months ago

I agree with Answer B

upvoted 3 times

ShinLi 4 months ago

me too. B looks better.

upvoted 1 times

Roontha 4 months ago

<https://aws.amazon.com/disaster-recovery/>

upvoted 1 times

Question #203

Topic 1

A company is planning a one-time migration of an on-premises MySQL database to Amazon Aurora MySQL in the us-east-1 Region. The company's current internet connection has limited bandwidth. The on-premises MySQL database is 60 TB in size. The company estimates that it will take a month to transfer the data to AWS over the current internet connection. The company needs a migration solution that will migrate the database more quickly.

Which solution will migrate the database in the LEAST amount of time?

- A. Request a 1 Gbps AWS Direct Connect connection between the on-premises data center and AWS. Use AWS Database Migration Service (AWS DMS) to migrate the on-premises MySQL database to Aurora MySQL.
- B. Use AWS DataSync with the current internet connection to accelerate the data transfer between the on-premises data center and AWS. Use AWS Application Migration Service to migrate the on-premises MySQL database to Aurora MySQL.
- C. Order an AWS Snowball Edge device. Load the data into an Amazon S3 bucket by using the S3 interface. Use AWS Database Migration Service (AWS DMS) to migrate the data from Amazon S3 to Aurora MySQL.
- D. Order an AWS Snowball device. Load the data into an Amazon S3 bucket by using the S3 Adapter for Snowball. Use AWS Application Migration Service to migrate the data from Amazon S3 to Aurora MySQL.

 **F_Eldin**  3 months, 4 weeks ago

Selected Answer: C

Why Not D:

1- C=SnowBall Edge, D=SnowBall Device.

The basic difference between Snowball and Snowball Edge is the capacity they provide. Snowball provides a total of 50 TB or 80 TB, out of which 42 TB or 72 TB is available, while Amazon Snowball Edge provides 100 TB, out of which 83 TB is available.

2- C=AWS Database Migration . D=Application Migration Service,

Application Migration Service simplifies, expedites, and reduces the cost of migrating and modernizing applications. Not for Database

upvoted 10 times

 **NikkyDicky**  2 months, 3 weeks ago

Selected Answer: C

Basic Snowball edge / DMS use case

upvoted 1 times

 **Moallal** 3 months, 2 weeks ago

Do the math, option A is 5.55 days. It's A

upvoted 1 times

 **breadops** 2 months ago

It can take months to provision a DX connection, its not A.

upvoted 1 times

 **Jackhemo** 3 months, 1 week ago

it takes ages to order a 1G circuit.

upvoted 1 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: C

I agree with option C.

Option D does not seem ideal because mentions Application Migration Service, also the snowball is more required for petabyte scale data migration while edge seems to be a better fit.

upvoted 1 times

 **andreitugui** 3 months, 4 weeks ago

Selected Answer: C

First of all a snowball solution is required for one time migration will focus in C & D.

Now since we are looking to migrate a database, DMS is needed also Snowball edge can accommodate the 60TB of data as the capacity limit is 80TB.

D is wrong by mentioning Application Migration service to migrate a database.

So correct answer is C). Order an AWS Snowball Edge device. Load the data into an Amazon S3 bucket by using the S3 interface. Use AWS Database Migration Service (AWS DMS) to migrate the data from Amazon S3 to Aurora MySQL.

upvoted 3 times

 **dbaroger** 3 months, 4 weeks ago

Selected Answer: D

D better cost than C and it does the same for S3. Need adapter too

upvoted 1 times

 **Roontha** 4 months ago

Answer : C (Key words : Limited bandwidth + DB migration should be done quickly)

if there no DB migration, we can go with B

upvoted 2 times

Question #204

Topic 1

A company has an application in the AWS Cloud. The application runs on a fleet of 20 Amazon EC2 instances. The EC2 instances are persistent and store data on multiple attached Amazon Elastic Block Store (Amazon EBS) volumes.

The company must maintain backups in a separate AWS Region. The company must be able to recover the EC2 instances and their configuration within 1 business day, with loss of no more than 1 day's worth of data. The company has limited staff and needs a backup solution that optimizes operational efficiency and cost. The company already has created an AWS CloudFormation template that can deploy the required network configuration in a secondary Region.

Which solution will meet these requirements?

- A. Create a second CloudFormation template that can recreate the EC2 instances in the secondary Region. Run daily multivolume snapshots by using AWS Systems Manager Automation runbooks. Copy the snapshots to the secondary Region. In the event of a failure launch the CloudFormation templates, restore the EBS volumes from snapshots, and transfer usage to the secondary Region.
- B. Use Amazon Data Lifecycle Manager (Amazon DLM) to create daily multivolume snapshots of the EBS volumes. In the event of a failure, launch the CloudFormation template and use Amazon DLM to restore the EBS volumes and transfer usage to the secondary Region.
- C. Use AWS Backup to create a scheduled daily backup plan for the EC2 instances. Configure the backup task to copy the backups to a vault in the secondary Region. In the event of a failure, launch the CloudFormation template, restore the instance volumes and configurations from the backup vault, and transfer usage to the secondary Region.
- D. Deploy EC2 instances of the same size and configuration to the secondary Region. Configure AWS DataSync daily to copy data from the primary Region to the secondary Region. In the event of a failure, launch the CloudFormation template and transfer usage to the secondary Region.

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

Selected Answer: C

Correct is C. For those voting with B, you missed the Instance configuration part. DLM will only backup the EBS volume not the instance settings also. AWS backup will backup ebs & instance settings.

Option C, using AWS Backup, provides a centralized and cost-effective solution for managing backups across multiple services, including EC2 instances. By creating a scheduled daily backup plan for the EC2 instances, AWS Backup ensures regular backups are taken. The backups can be configured to be stored in a vault in the secondary Region, fulfilling the requirement of maintaining backups in a separate Region. The EC2 instance volumes and configurations can then be restored from the backup vault using AWS Backup's restore capabilities. This allows for the recovery of EC2 instances and their configurations within the required timeframe of 1 business day, with a maximum data loss of 1 day's worth.

upvoted 8 times

 **Roontha** 3 months, 3 weeks ago

Answer is B.

<https://aws.amazon.com/ebs/data-lifecycle-manager/>

It has aws sponsored video which stated clearly can take EBS backed AMIs with AWS DLM

upvoted 1 times

 **Just_Ninja** 2 months, 1 week ago

B is Wrong!

Why? They must!! So that means Compliance is important. AWS Backup is a service for Compliance and Government Targets. C Match

upvoted 1 times

 **SK_Tyagi** Most Recent  1 month ago

Selected Answer: B

B

The explanation here fits the use-case

<https://aws.amazon.com/blogs/storage/automating-amazon-ebs-snapshot-and-ami-management-using-amazon-dlm/>

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C

B would be ok, if DLM supported restore. it doesn't

upvoted 2 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: C

I think correct is C. AWS Backup is easier and perfectly fits the scenario

upvoted 1 times

Maria2023 3 months ago

Selected Answer: C

B says "Use Amazon DLM to restore the EBS volumes and transfer usage to the secondary Region" - just tested it and could not find any option for DLM to restore volumes, think the snapshots are managed the usual way.

upvoted 1 times

easytoo 3 months ago

C-C-C-C-C-C-C-C-C

upvoted 1 times

Jonalb 3 months, 2 weeks ago

Selected Answer: B

Its B!!!!!!!!!!!!!!

upvoted 1 times

clownfishman 3 months, 2 weeks ago

Why not A?

upvoted 1 times

Jesuisleon 3 months, 3 weeks ago

Selected Answer: B

I prefer B to C as this sentence "The EC2 instances are persistent and store data on multiple attached Amazon Elastic Block Store (Amazon EBS) volumes", in this question, there is no database mentioned, I assume all persistent data is in EBS, so no need to backup ec2 instances, you can directly startup ec2 instance by cloudformation and load backedup ebs.

upvoted 2 times

rbm2023 3 months, 4 weeks ago

Selected Answer: C

AWS Backup is more cost effective so I would chose C as well. The DLM option B, does not contemplate the back up in another region as far as I could see.

upvoted 2 times

Jesuisleon 3 months, 3 weeks ago

DLM can copy snapshots to another region, see <https://aws.amazon.com/about-aws/whats-new/2019/12/amazon-data-lifecycle-manager-enables-automation-snapshot-copy-via-policies/>

upvoted 1 times

F_Eldin 3 months, 4 weeks ago

Selected Answer: B

AWS Backup is a latter service which tries to simplify the challenge of administering a backup in each service individually.

However AWS Lifecycle Manager originally only made EBS snapshots but has been expanded to create AMIs. I don't believe AWS Backup can trigger AMI creation.

upvoted 1 times

andreitugui 3 months, 4 weeks ago

But B mentions only EBS snapshots (Use Amazon Data Lifecycle Manager (Amazon DLM) to create daily multivolume snapshots of the EBS volumes)! Does not say anything about AMI's.

So IMO the answer is C

upvoted 1 times

deegadaze1 4 months ago

The answer is B

upvoted 2 times

deegadaze1 4 months ago

<https://aws.amazon.com/blogs/storage/automating-amazon-ebs-snapshots-management-using-data-lifecycle-manager/>

upvoted 1 times

Roontha 4 months ago

Answer : C

<https://aws.amazon.com/getting-started/hands-on/amazon-ec2-backup-and-restore-using-aws-backup/>

<https://docs.aws.amazon.com/aws-backup/latest/devguide/integrate-cloudformation-with-aws-backup.html>

upvoted 2 times

deegadaze1 4 months ago

B would be best bet. C may involve additional overhead for managing backup plans for EC2 instances. It focuses on backing up entire instances rather than specifically optimising EBS snapshots. if the goal is to optimise operational efficiency and cost for backup management of EBS volumes, leveraging Amazon Data Lifecycle Manager (Amazon DLM) to create daily multivolume snapshots is recommended. It provides automation, policy management, and cost optimisation features specifically tailored for EBS snapshots.

The answer is B

upvoted 2 times

✉️  **Roontha** 4 months ago

@deegadaze1: Agreed with answer B

<https://aws.amazon.com/blogs/storage/automating-amazon-ebs-snapshot-and-ami-management-using-amazon-dlm/>

In this blog post, we examine how you can use Amazon Data Lifecycle Manager (Amazon DLM) lifecycle policies to automate the creation, retention, and deletion of Amazon EBS snapshots. With Amazon DLM, the need for complicated and custom scripts to manage EBS snapshots is eliminated. Amazon DLM enables you to create, manage, and delete EBS snapshots in a simple, automated way based on resource tags for EBS volumes or Amazon EC2 instances. This reduces the operational complexity of managing EBS snapshots, thereby saving time and money. Also, let's not forget the best part: Amazon DLM is free to use and is available in all AWS Regions.

upvoted 1 times

Question #205

Topic 1

A company is designing a new website that hosts static content. The website will give users the ability to upload and download large files. According to company requirements, all data must be encrypted in transit and at rest. A solutions architect is building the solution by using Amazon S3 and Amazon CloudFront.

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

- A. Turn on S3 server-side encryption for the S3 bucket that the web application uses.
- B. Add a policy attribute of "aws:SecureTransport": "true" for read and write operations in the S3 ACLs.
- C. Create a bucket policy that denies any unencrypted operations in the S3 bucket that the web application uses.
- D. Configure encryption at rest on CloudFront by using server-side encryption with AWS KMS keys (SSE-KMS).
- E. Configure redirection of HTTP requests to HTTPS requests in CloudFront.
- F. Use the RequireSSL option in the creation of presigned URLs for the S3 bucket that the web application uses.

 **SkyZeroZx** Highly Voted  2 months, 3 weeks ago

Selected Answer: ACE

Answer : ACE

- A) SSE S3 sounds good encrypt in rest data
- B) sounds good until say in ACLs is incorrect
- C) Bucket Policy avoid upload unencrypted is correct sounds good
- D) CloudFront with KMS ? why ? not seems
- E) HTTP redirect to HTTPS sounds good is classic this case
- F) why ? not seems in this case

upvoted 5 times

 **Simon523** Most Recent  1 month ago

Selected Answer: ACE

How to Prevent Uploads of Unencrypted Objects to Amazon S3

<https://aws.amazon.com/tw/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/>

upvoted 1 times

 **RotterDam** 1 month, 1 week ago

ACE but why not F?

upvoted 1 times

 **chikorita** 3 weeks, 1 day ago

question nowhere mentions the use of pre-signed URLs
if it was used in this scenario then it could potentially be one of the right answers

upvoted 1 times

 **Just_Ninja** 2 months, 1 week ago

Selected Answer: ACE

ACE.

But A is deprecated :)

because since the 05.01.2023 S3 use automatical atRest encryption for new objekts.

upvoted 3 times

 **Christina666** 2 months, 2 weeks ago

Selected Answer: ACE

we don't have a "encryption at rest" for cloudfront in the console

upvoted 1 times

 **NikkDicky** 2 months, 3 weeks ago

Selected Answer: ACE

A and C are a bit redundant. I'd pick D instead of C, but for ACL reference

upvoted 1 times

 **easystoo** 3 months ago

a-d-e a-d-e a-d-e

upvoted 2 times

 **chathur** 3 months, 3 weeks ago

Selected Answer: ACE

Source: <https://repost.aws/knowledge-center/s3-bucket-policy-for-config-rule>

B is wrong as "aws:SecureTransport": "true" does not deny 'http' traffic

upvoted 1 times

 **consultornetwork** 3 months, 3 weeks ago

Why not B?

upvoted 2 times

 **chathur** 3 months, 3 weeks ago

<https://repost.aws/knowledge-center/s3-bucket-policy-for-config-rule>

it is not enough

upvoted 1 times

 **Jesuisleon** 3 months, 3 weeks ago

you should add "aws:SecureTransport": "true" in the S3 bucket policy not S3 ACL.

see <https://stackoverflow.com/questions/47815526/s3-bucket-policy-vs-access-control-list>

and " We recommend allowing only encrypted connections over HTTPS (TLS) by using the aws:SecureTransport condition in your Amazon S3 bucket policies" from <https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html>

upvoted 2 times

 **BabaP** 3 months, 3 weeks ago

Because C does just that

upvoted 1 times

 **andreitugui** 3 months, 4 weeks ago

Selected Answer: ACE

I will go with ACE

upvoted 2 times

 **Roontha** 4 months ago

Answer : ACE

upvoted 3 times

Question #206

Topic 1

A company is implementing a serverless architecture by using AWS Lambda functions that need to access a Microsoft SQL Server DB instance on Amazon RDS. The company has separate environments for development and production, including a clone of the database system.

The company's developers are allowed to access the credentials for the development database. However, the credentials for the production database must be encrypted with a key that only members of the IT security team's IAM user group can access. This key must be rotated on a regular basis.

What should a solutions architect do in the production environment to meet these requirements?

- A. Store the database credentials in AWS Systems Manager Parameter Store by using a SecureString parameter that is encrypted by an AWS Key Management Service (AWS KMS) customer managed key. Attach a role to each Lambda function to provide access to the SecureString parameter. Restrict access to the SecureString parameter and the customer managed key so that only the IT security team can access the parameter and the key.
- B. Encrypt the database credentials by using the AWS Key Management Service (AWS KMS) default Lambda key. Store the credentials in the environment variables of each Lambda function. Load the credentials from the environment variables in the Lambda code. Restrict access to the KMS key so that only the IT security team can access the key.
- C. Store the database credentials in the environment variables of each Lambda function. Encrypt the environment variables by using an AWS Key Management Service (AWS KMS) customer managed key. Restrict access to the customer managed key so that only the IT security team can access the key.
- D. Store the database credentials in AWS Secrets Manager as a secret that is associated with an AWS Key Management Service (AWS KMS) customer managed key. Attach a role to each Lambda function to provide access to the secret. Restrict access to the secret and the customer managed key so that only the IT security team can access the secret and the key.

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

Selected Answer: D

Answer : D

Rotation = Secret Manager (and Not Parameter store)

upvoted 5 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: D

its a D

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: D

Keys is DB credentials rotation

upvoted 2 times

 **easytoo** 3 months ago

d-d-d-d-dd-d-dd-d-d-d

upvoted 1 times

 **Jackhemo** 3 months, 1 week ago

Selected Answer: A

From olabiba.ai

"Based on the requirements of resolving scaling issues and minimizing licensing costs, the most cost-effective solution would be option A: Deploy Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer for the web tier and for the application tier. Use Amazon Aurora PostgreSQL with Babelfish turned on to replatform the SQL Server database."

upvoted 1 times

 **Just_Ninja** 2 months, 1 week ago

Nice description, but A is Wrong. Parameter Store is not the best practice for Secrets based on AWS Well Architected Framework

upvoted 2 times

 **Jackhemo** 3 months, 1 week ago

Answer is D. This is for the next question.

upvoted 2 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: A

I think the answer is A the requirement is to rotate the KEY and not the password, looks like this question was created to make us chose option D.

Option A stores the password in the Param Store encrypting it with KMS which is the requirement “the credentials for the production database must be encrypted with a key that only members of the IT security team's IAM user group can access.”

<https://docs.aws.amazon.com/systems-manager/latest/userguide/ps-integration-lambda-extensions.html>

Check the Authentication section.

upvoted 2 times

 **F_Eldin** 3 months, 3 weeks ago

A does not satisfy the requirement "This key must be rotated on a regular basis."

upvoted 3 times

 **andreitugui** 3 months, 4 weeks ago

Selected Answer: D

Answering D

upvoted 1 times

 **Masonryeh** 4 months ago

Selected Answer: D

D, Secret Manager is the accurate solution

upvoted 1 times

 **Roontha** 4 months ago

Answer : D

Keys is DB credentials rotation

upvoted 1 times

Question #207

Topic 1

An online retail company is migrating its legacy on-premises .NET application to AWS. The application runs on load-balanced frontend web servers, load-balanced application servers, and a Microsoft SQL Server database.

The company wants to use AWS managed services where possible and does not want to rewrite the application. A solutions architect needs to implement a solution to resolve scaling issues and minimize licensing costs as the application scales.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer for the web tier and for the application tier. Use Amazon Aurora PostgreSQL with Babelfish turned on to replatform the SQL Server database.
- B. Create images of all the servers by using AWS Database Migration Service (AWS DMS). Deploy Amazon EC2 instances that are based on the on-premises imports. Deploy the instances in an Auto Scaling group behind a Network Load Balancer for the web tier and for the application tier. Use Amazon DynamoDB as the database tier.
- C. Containerize the web frontend tier and the application tier. Provision an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Create an Auto Scaling group behind a Network Load Balancer for the web tier and for the application tier. Use Amazon RDS for SQL Server to host the database.
- D. Separate the application functions into AWS Lambda functions. Use Amazon API Gateway for the web frontend tier and the application tier. Migrate the data to Amazon S3. Use Amazon Athena to query the data.

 **kjcncjek** 3 weeks, 2 days ago

why not C

upvoted 1 times

 **chikorita** 1 month ago

A : the best of the worst

upvoted 2 times

 **ggrodsckiy** 2 months ago

Correct A.

upvoted 1 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: A

A. The other options sound fishy.

upvoted 2 times

 **rxhan** 1 month, 3 weeks ago

golden.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A by elimination

upvoted 1 times

 **easytoo** 3 months ago

a-a-a-a-a-a-a

after much consideration it's the babelfish to the rescue -

zaphod beeblebrox ftw

upvoted 1 times

 **F_Eldin** 3 months, 3 weeks ago

Selected Answer: A

There is no good solution here. A is just forcing that company to use AWS services as "MOST cost-effectively" alternative. Practically Babelfish has bad reviews, companies prefer to migrate SQL-Server as-is.

upvoted 3 times

 **rbm2023** 3 months, 4 weeks ago

Selected Answer: A

Agree with A the NLB with EKS might be an interesting choice if chose too fast.

The correct option should be A, using an ALB and rehost to from M SQL Server to Aurora using Babelfish.

<https://aws.amazon.com/rds/aurora/babelfish/>

"With Babelfish, Aurora PostgreSQL now understands T-SQL, Microsoft SQL Server's proprietary SQL dialect, and supports the same communications protocol, so your apps that were originally written for SQL Server can now work with Aurora with fewer code changes"

upvoted 2 times

andreitugui 3 months, 4 weeks ago

Selected Answer: A

Answer is A. B and C are wrong as putting web apps behind NLB is not the correct approach. Also D is wrong as having SQL DB on S3 is impossible to do it straight forward, will require to refactor everything in the backend side and data layer side.

upvoted 2 times

Roontha 4 months ago

Answer : A

It includes a network end-point added to PostgreSQL to enable your PostgreSQL database to understand the SQL Server wire protocol and commonly used SQL Server commands. With Babelfish, applications that were originally built for SQL Server can work directly with PostgreSQL, with little to no code changes, and without changing database drivers.

upvoted 4 times

ShinLi 4 months ago

agree A <https://aws.amazon.com/rds/aurora/babelfish/>

upvoted 1 times

Question #208

Topic 1

A software-as-a-service (SaaS) provider exposes APIs through an Application Load Balancer (ALB). The ALB connects to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that is deployed in the us-east-1 Region. The exposed APIs contain usage of a few non-standard REST methods: LINK, UNLINK, LOCK, and UNLOCK.

Users outside the United States are reporting long and inconsistent response times for these APIs. A solutions architect needs to resolve this problem with a solution that minimizes operational overhead.

Which solution meets these requirements?

- A. Add an Amazon CloudFront distribution. Configure the ALB as the origin.
- B. Add an Amazon API Gateway edge-optimized API endpoint to expose the APIs. Configure the ALB as the target.
- C. Add an accelerator in AWS Global Accelerator. Configure the ALB as the origin.
- D. Deploy the APIs to two additional AWS Regions: eu-west-1 and ap-southeast-2. Add latency-based routing records in Amazon Route 53.

 **chico2023** 1 month, 1 week ago

Selected Answer: B

Answer: B

I don't understand why people are choosing GA. I would rather go with option D.

From AWS documentation:

Edge-optimized API endpoint

The default hostname of an API Gateway API that is deployed to the specified Region while using a CloudFront distribution to facilitate client access typically from across AWS Regions. API requests are routed to the nearest CloudFront Point of Presence (POP), which typically improves connection time for geographically diverse clients.

I couldn't find any document mentioning that Edge-optimized API endpoints won't support non-standard REST methods.

upvoted 1 times

 **vn_thanh tung** 1 month ago

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-endpoint-types.html#api-gateway-api-endpoint-types-edge-optimized:~:text=traffic%20originates%20from.-,Edge%2Doptimized%20API%20endpoints,-An%20edge%2Doptimized>

I think can help you, C is answer

upvoted 1 times

 **chico2023** 1 month, 1 week ago

I know we can't trust AI assistants, but take a look at my little chat with:

==== Labiba

Yes, Amazon API Gateway Edge-optimized APIs can handle non-standard REST methods. Edge-optimized APIs are designed to provide low-latency access to your API by using the AWS CloudFront global network. You can set up API methods to handle any HTTP method, including non-standard ones, and configure them to work with your specific requirements and use cases.

==== Bard

Yes, Amazon API Gateway edge-optimized APIs can handle non-standard REST methods. However, there are some limitations.

The non-standard REST method must be supported by the integration that you use for the API method. For example, if you are using a Lambda integration, the Lambda function must be able to handle the non-standard REST method.

upvoted 1 times

 **chico2023** 1 month, 1 week ago

Now, why would I use GA?

I don't know you, but I would use in a situation where I have an application that connects to a database and I need to reduce the latency of my application for users by launching EC2 instances around the world. Note that I can't do that (not that easy, at least) with my RDS DB, so what I do? I use Global Accelerator to speed up communication between my instances in different countries to the database server in a single location, for example.

upvoted 1 times

 **Arnaud92** 1 month, 3 weeks ago

Selected Answer: C

Cloudfront cannot handle non standard REST methods. There are Cloud front involved behind API Gateway edge-optimized. So only C make sense here

upvoted 1 times

 **Just_Ninja** 2 months, 1 week ago

Selected Answer: B

It only can B...

Here is a AWS entry. <https://repost.aws/knowledge-center/api-gateway-cloudfront-distribution>

upvoted 1 times

NikkyDicky 2 months, 3 weeks ago

Selected Answer: C

B would be nice if edge-optimized was supported for HTTP APIs

upvoted 3 times

SandyIndia 3 months ago

Selected Answer: C

By adding an accelerator in AWS Global Accelerator and configuring the ALB as the origin, the traffic to the ALB will be routed through the global network, reducing latency and improving response times for users outside the United States.

This solution minimizes operational overhead as AWS Global Accelerator handles the routing and optimization automatically, without requiring additional infrastructure deployment or configuration changes.

upvoted 3 times

Maria2023 3 months ago

Selected Answer: C

I was also supporting answer B, however just tested API Gateway and it seems that it only supports GET, POST, PUT, PATCH, DELETE, HEAD, and OPTIONS methods. I personally couldn't find a way to create a custom method which is part of the requirement. Please share if you find a way

upvoted 3 times

SmileyCloud 3 months ago

Selected Answer: B

It's B. That's the point of an edge-optimized API endpoint.

upvoted 3 times

SandyIndia 3 months ago

Option B suggests adding an Amazon API Gateway edge-optimized API endpoint with the ALB as the target. While API Gateway can provide API management capabilities, it may not directly address the latency issue for non-standard REST methods.

upvoted 2 times

easytoo 3 months ago

C-C-CC-CC-C-CC--C-C-C-C-C

upvoted 1 times

gd1 3 months, 1 week ago

The solution that meets these requirements most effectively would be:

A. Add an Amazon CloudFront distribution. Configure the ALB as the origin.

CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. By configuring CloudFront with your Application Load Balancer (ALB) as the origin, users can access your API through the CloudFront edge location that's closest to them, reducing latency.

Option B, Amazon API Gateway, does not support non-standard REST methods. Option C, AWS Global Accelerator, is a networking service that improves your applications' availability and performance, but its benefits are more noticeable for TCP/UDP-based workloads rather than HTTP(S)-based APIs. Option D, deploying the APIs in multiple regions and using Amazon Route 53 latency-based routing, would require much more operational overhead compared to the recommended solution.

upvoted 2 times

Jesuisleon 3 months, 3 weeks ago

Selected Answer: B

I prefer B as in the question it emphasize API, edge-optimized API is perfect for the global users.

"An edge-optimized API endpoint is best for geographically distributed clients. API requests are routed to the nearest CloudFront Point of Presence (POP). This is the default endpoint type for API Gateway REST APIs." from

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

upvoted 3 times

Jesuisleon 3 months, 3 weeks ago

Why I think C is WRONG ? GA is usually for TCP/UDP level, in this question it explicitly points to rest api which is at OSI 7 layer(<https://stackoverflow.com/questions/29264855/in-which-osi-layer-is-the-rest-api-paradigm>), so GA is not suitable here.

upvoted 1 times

rbm2023 3 months, 4 weeks ago

Selected Answer: C

In my view you can use Global Accelerator with a load balancer.

I vote for C.

<https://cloudonaut.io/review-aws-global-accelerator-latency-multi-region-disaster-recovery/>

upvoted 1 times

rbm2023 3 months, 4 weeks ago

in addition the cloud front solution may not support the methods informed in the question - Option A.

D requires too much overhead.

upvoted 2 times

 **andreitugui** 3 months, 4 weeks ago

Selected Answer: C

AWS Global Accelerator is a service that improves the availability and performance of applications for global users. By adding an accelerator in AWS Global Accelerator and configuring the ALB as the origin, the traffic from users outside the United States will be routed through the Global Accelerator network, which uses the AWS global network infrastructure to optimize the delivery of the application traffic.

upvoted 3 times

 **nexus2020** 3 months, 3 weeks ago

Yes you can, see - <https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works.html>

--> For standard accelerators, the endpoints are Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses.

upvoted 2 times

 **AMEJack** 4 months ago

Selected Answer: A

A should be the answer as @deegadaze1 explanation

upvoted 1 times

 **deegadaze1** 4 months ago

Answer is : A

No, you cannot directly configure an Application Load Balancer (ALB) as the origin for an accelerator in AWS Global Accelerator.

AWS Global Accelerator is designed to improve the availability and performance of applications running over TCP or UDP protocols. It directs client traffic to the nearest AWS edge location and then routes it to your application's endpoints, such as Elastic IP addresses, Network Load Balancers (NLBs), or EC2 instances.

On the other hand, AWS Global Accelerator primarily focuses on improving the availability and reliability of TCP and UDP-based applications by directing traffic through the AWS global network backbone. While Global Accelerator can improve performance for certain use cases, such as minimising connection setup times, it may not provide the same level of optimisation for API response times compared to CloudFront.

upvoted 1 times

 **chathur** 3 months, 3 weeks ago

Global accelerator can expose an ALB

<https://aws.amazon.com/global-accelerator/faqs/#:~:text=If%20you%20have%20workloads%20hosted%20in%20a%20single%20AWS%20Region%20and%20used%20by%20clients%20in%20and%20around%20the%20same%20Region%2C%20you%20can%20use%20an%20Application%20Load%20Balancer%20or%20Network%20Load%20Balancer%20to%20manage%20your%20resources.>

upvoted 3 times

 **nexus2020** 3 months, 3 weeks ago

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-components.html>

Endpoint

An endpoint is the resource that Global Accelerator directs traffic to.

Endpoints for standard accelerators can be Network Load Balancers, Application Load Balancers, EC2 instances, or Elastic IP addresses. An Application Load Balancer endpoint can be an internet-facing or internal. Traffic for standard accelerators is routed to endpoints based on the health of the endpoint along with configuration options that you choose, such as endpoint weights. For each endpoint, you can configure weights, which are numbers that you can use to specify the proportion of traffic to route to each one. This can be useful, for example, to do performance testing within a Region.

upvoted 1 times

 **nexus2020** 3 months, 3 weeks ago

Well, not sure what were supported in the past, however as of today in the link above, ALB is supported as origin/endpoint behind the Global Accelerator

upvoted 2 times

 **Masonryeh** 4 months ago

Selected Answer: C

<https://aws.amazon.com/blogs/networking-and-content-delivery/accessing-an-aws-api-gateway-via-static-ip-addresses-provided-by-aws-global-accelerator/>

upvoted 4 times

 **Roontha** 4 months ago

Answer : A

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html>

upvoted 2 times

 **Roontha** 4 months ago

My bad...Answer : C

upvoted 2 times

Question #209

Topic 1

A company runs an IoT application in the AWS Cloud. The company has millions of sensors that collect data from houses in the United States. The sensors use the MQTT protocol to connect and send data to a custom MQTT broker. The MQTT broker stores the data on a single Amazon EC2 instance. The sensors connect to the broker through the domain named `iot.example.com`. The company uses Amazon Route 53 as its DNS service. The company stores the data in Amazon DynamoDB.

On several occasions, the amount of data has overloaded the MQTT broker and has resulted in lost sensor data. The company must improve the reliability of the solution.

Which solution will meet these requirements?

- A. Create an Application Load Balancer (ALB) and an Auto Scaling group for the MQTT broker. Use the Auto Scaling group as the target for the ALB. Update the DNS record in Route 53 to an alias record. Point the alias record to the ALB. Use the MQTT broker to store the data.
- B. Set up AWS IoT Core to receive the sensor data. Create and configure a custom domain to connect to AWS IoT Core. Update the DNS record in Route 53 to point to the AWS IoT Core Data-ATS endpoint. Configure an AWS IoT rule to store the data.
- C. Create a Network Load Balancer (NLB). Set the MQTT broker as the target. Create an AWS Global Accelerator accelerator. Set the NLB as the endpoint for the accelerator. Update the DNS record in Route 53 to a multivalue answer record. Set the Global Accelerator IP addresses as values. Use the MQTT broker to store the data.
- D. Set up AWS IoT Greengrass to receive the sensor data. Update the DNS record in Route 53 to point to the AWS IoT Greengrass endpoint. Configure an AWS IoT rule to invoke an AWS Lambda function to store the data.

 **bur4an** 1 week, 3 days ago

I think this is repeat question.

upvoted 1 times

 **SK_Tyagi** 1 month ago

Selected Answer: B

AWS service is the answer.

upvoted 1 times

 **lferrari** 1 month, 1 week ago

Selected Answer: B

IOT core for anything IOT

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

IOT core for anything IOT

upvoted 3 times

 **pupsik** 3 months ago

Selected Answer: B

Option C doesn't mention required auto-scaling group, hence eliminated.

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

voting for B. IoT Core

upvoted 2 times

 **Maria2023** 3 months ago

Selected Answer: B

Both C and B should work. I suggest AWS wants us to use as many native services as we can, therefore B should be the preferred answer.

upvoted 1 times

 **easytoo** 3 months ago

b-b-b-b-bb-

Greengrass is typically used for edge computing scenarios and may not be the most suitable solution for addressing MQTT broker reliability and scalability.

upvoted 2 times

 **chaiseed** 3 months, 1 week ago

Selected Answer: B

voting for B. IoT Core

upvoted 1 times

  **nexus2020** 3 months, 1 week ago**Selected Answer: B**

IoT core, B

upvoted 1 times

Question #210

Topic 1

A company has Linux-based Amazon EC2 instances. Users must access the instances by using SSH with EC2 SSH key pairs. Each machine requires a unique EC2 key pair.

The company wants to implement a key rotation policy that will, upon request, automatically rotate all the EC2 key pairs and keep the keys in a securely encrypted place. The company will accept less than 1 minute of downtime during key rotation.

Which solution will meet these requirements?

- A. Store all the keys in AWS Secrets Manager. Define a Secrets Manager rotation schedule to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances. Update the private keys in Secrets Manager.
- B. Store all the keys in Parameter Store, a capability of AWS Systems Manager, as a string. Define a Systems Manager maintenance window to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances. Update the private keys in Parameter Store.
- C. Import the EC2 key pairs into AWS Key Management Service (AWS KMS). Configure automatic key rotation for these key pairs. Create an Amazon EventBridge scheduled rule to invoke an AWS Lambda function to initiate the key rotation in AWS KMS.
- D. Add all the EC2 instances to Fleet Manager, a capability of AWS Systems Manager. Define a Systems Manager maintenance window to issue a Systems Manager Run Command document to generate new key pairs and to rotate public keys to all the instances in Fleet Manager.

 **wahaha2023** 1 month ago

Selected Answer: A

I think the Systems Manager maintenance window is to perform some potentially disruptive actions, which means the duration of the window is equal to system downtime. and I check the white paper, I seems the duration of system maintenance window should be longer than 1 hour.

upvoted 2 times

 **chico2023** 1 month, 1 week ago

Selected Answer: D

Seriously, all. While it can be done in A, it's better to do that with D. Here is why:

Question says:

"A company has Linux-based Amazon EC2 instances." and "Each machine requires a unique EC2 key pair."

We might be talking about thousands of EC2 instances. But let's continue. Option A says:

"Store all the keys in AWS Secrets Manager." which is OK, you can store up to 500,000 apparently but, seriously, think about. Instances are generated and deleted all the time. This would be cumbersome, even if you do that programmatically. Not convinced? Let me continue.

upvoted 1 times

 **vn_thanh tung** 1 month ago

With D how to "keep the keys in a securely encrypted place" ? Should be A

upvoted 1 times

 **chico2023** 1 month, 1 week ago

Same option A, says the following: "Define a Secrets Manager rotation schedule to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances."

Now, this is A lot, but how are we going to replace the public keys on EC2 instances? Answer doesn't say.

Finally, for those who are supporting their answer on an AWS blog showing how to use SM to rotate SSH key to manage servers, pay attention to this part: "A secret is created in AWS Secrets Manager. The secret holds the SSH keypair that the master node will use to connect to the other nodes in the cluster."

Their design is "one to many", that is not part of what question says, and I would like to remind you "Each machine requires a unique EC2 key pair."

upvoted 1 times

 **wahaha2023** 1 month ago

I am curious about how we can define a 1-minute Systems Manager maintenance window.

upvoted 1 times

 **easystoo** 1 month, 3 weeks ago

a-a-a-a-a-a-a-a

upvoted 1 times

 **Just_Ninja** 2 months, 1 week ago

Selected Answer: A

A: Based on the Well Architecting Framework for best Practices and that tutorial :) <https://aws.amazon.com/de/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 1 times

✉ **nicecurls** 2 months, 2 weeks ago

Selected Answer: D

Why A? Select D

upvoted 2 times

✉ **Just_Ninja** 2 months, 1 week ago

D is wrong, Parameter Store is a good practice to store Parameters but not the Secrets. I know you can use KMS to encrypt the Parameters, but you need a secure store for Secrets and here we have for example the secret manager with FIPS 140-2 Standard.

upvoted 1 times

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

Selected Answer: A

going with A

upvoted 1 times

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

Selected Answer: A

as someone pointed out D breaks the requirement for unique keys

upvoted 1 times

✉ **javitech83** 2 months, 4 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 1 times

✉ **Maria2023** 3 months ago

Selected Answer: A

According to the link below A is a better answer since the process does not require manual generation of the keys

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 3 times

✉ **SmileyCloud** 3 months ago

Selected Answer: D

D. Fleet Manager does this. <https://tutorialsdojo.com/automatic-ssh-key-pair-rotation-via-aws-systems-manager-fleet-manager/>

upvoted 2 times

✉ **javitech83** 2 months, 4 weeks ago

have in mind that every server has its own key.

upvoted 1 times

✉ **nicecurls** 2 months, 2 weeks ago

This solution provides the possibility to choose the correct instance, not all together, because fleet manager can do it

Please correct me if I was wrong

upvoted 2 times

✉ **easytoo** 3 months ago

Selected Answer: A

By storing the keys in AWS Secrets Manager, you can securely encrypt them. Defining a rotation schedule in Secrets Manager allows you to automatically generate new key pairs using an AWS Lambda function. This ensures that each machine has a unique key pair. During the rotation process, the public keys on the EC2 instances can be replaced, and the private keys can be updated in Secrets Manager. This solution minimizes downtime and provides a secure way to manage and rotate the EC2 key pairs

upvoted 2 times

Question #211

Topic 1

A company wants to migrate to AWS. The company is running thousands of VMs in a VMware ESXi environment. The company has no configuration management database and has little knowledge about the utilization of the VMware portfolio.

A solutions architect must provide the company with an accurate inventory so that the company can plan for a cost-effective migration.

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

- A. Use AWS Systems Manager Patch Manager to deploy Migration Evaluator to each VM. Review the collected data in Amazon QuickSight. Identify servers that have high utilization. Remove the servers that have high utilization from the migration list. Import the data to AWS Migration Hub.
- B. Export the VMware portfolio to a .csv file. Check the disk utilization for each server. Remove servers that have high utilization. Export the data to AWS Application Migration Service. Use AWS Server Migration Service (AWS SMS) to migrate the remaining servers.
- C. Deploy the Migration Evaluator agentless collector to the ESXi hypervisor. Review the collected data in Migration Evaluator. Identify inactive servers. Remove the inactive servers from the migration list. Import the data to AWS Migration Hub.
- D. Deploy the AWS Application Migration Service Agent to each VM. When the data is collected, use Amazon Redshift to import and analyze the data. Use Amazon QuickSight for data visualization.

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

Selected Answer: C

C no doubt

upvoted 1 times

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

Selected Answer: C

C

This solution can meet the requirements with the least operational overhead. and also, keyword for planning only

upvoted 1 times

✉  **javitech83** 2 months, 4 weeks ago

Selected Answer: C

I was first thinking about D because is is stated that the company has little knowledge about VMWare. But option D introduces operational overhead

upvoted 1 times

✉  **pupsik** 3 months ago

Selected Answer: C

C seems like a good choice:

<https://aws.amazon.com/migration-evaluator/features/>

upvoted 1 times

✉  **easytoo** 3 months ago

C-C-C-C-C-

migration evaluator ftw

upvoted 1 times

✉  **easytoo** 3 months ago

Question 210 is a-a-a-a-a-a-a-a

upvoted 1 times

✉  **yzrk** 3 months, 1 week ago

Selected Answer: C

C

This solution can meet the requirements with the least operational overhead. and also, keyword for planning only

upvoted 3 times

Question #212

Topic 1

A company runs a microservice as an AWS Lambda function. The microservice writes data to an on-premises SQL database that supports a limited number of concurrent connections. When the number of Lambda function invocations is too high, the database crashes and causes application downtime. The company has an AWS Direct Connect connection between the company's VPC and the on-premises data center. The company wants to protect the database from crashes.

Which solution will meet these requirements?

- A. Write the data to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda function to read from the queue and write to the existing database. Set a reserved concurrency limit on the Lambda function that is less than the number of connections that the database supports.
- B. Create a new Amazon Aurora Serverless DB cluster. Use AWS DataSync to migrate the data from the existing database to Aurora Serverless. Reconfigure the Lambda function to write to Aurora.
- C. Create an Amazon RDS Proxy DB instance. Attach the RDS Proxy DB instance to the Amazon RDS DB instance. Reconfigure the Lambda function to write to the RDS Proxy DB instance.
- D. Write the data to an Amazon Simple Notification Service (Amazon SNS) topic. Invoke the Lambda function to write to the existing database when the topic receives new messages. Configure provisioned concurrency for the Lambda function to be equal to the number of connections that the database supports.

 **ggrodskiy** 2 months ago

Correct A.

upvoted 1 times

 **Just_Ninja** 2 months, 1 week ago

Selected Answer: A

A tricky question :)

The RDS proxy sounds sexy, but it cannot be used because the database is on premise.

The creative solution here is SQS.

Such questions are partly about your understanding of the services and some solutions are good, even if they sound a bit strange at first :)

upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

Its an A

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: A

correct is A as database is on-premises

upvoted 2 times

 **bhanus** 3 months ago

Selected Answer: A

MODERATOR Please delete my previous comment. I commented about RDS proxy which is totally WRONG.

Answer is A

upvoted 1 times

 **awscerts023** 3 months ago

Selected Answer: C

Will go with C , don't think the question says they need to keep the on-prem db

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: A

apparently, we need to make the lambda "not to rush that much" and keep the connection within the limit of the on-pre DB. So if we want not to lose data while waiting we implement SQS before the lambda so it keeps the requests in the queue.

upvoted 3 times

 **SmileyCloud** 3 months ago

Selected Answer: A

C should be logical answer, that's what RDS proxy does. But, they want to keep the existing SQL on-prem and not migrate to RDS. So C and B are out. We need to throttle the connections. SNS is not designed for this. So, it's SQS (A).

upvoted 1 times

 **psyx21** 3 months ago

Selected Answer: A

Correct answer is A

upvoted 1 times

 **easystoo** 3 months ago

C-C-C-C-C-C

By creating an Amazon RDS Proxy DB instance and attaching it to the existing Amazon RDS DB instance, you can protect the database from crashes caused by a high number of Lambda function invocations. The RDS Proxy acts as an intermediary between the Lambda function and the database, managing the connections and pooling them efficiently

upvoted 1 times

 **easystoo** 1 month, 3 weeks ago

a-a-a-a-a-a-a-a-a

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: A

A is the answer. RDS proxy is meant to help with connection pooling. Amazon RDS Proxy instance maintains a pool of established connections to your RDS database instances, reducing the stress on database compute and memory resources that typically occurs when new connections are established. RDS Proxy also shares infrequently used database connections, so that fewer connections access the RDS database. This connection pooling enables your database to efficiently support a large number and frequency of application connections so that your application can scale without compromising performance.

upvoted 1 times

 **bhanus** 2 months, 4 weeks ago

Answer is A. But IGNORE my above comment on RDS. The current situation is database is on-premises. So RDS proxy has nothing to do with onprem DB. so Answer is A

upvoted 2 times

 **emiliocb4** 3 months, 1 week ago

Selected Answer: A

SNS is used for notification purpose not for data matter. we don't know how big can be the data to write.
i use SQS to decouple

upvoted 1 times

Question #213

Topic 1

A company uses a Grafana data visualization solution that runs on a single Amazon EC2 instance to monitor the health of the company's AWS workloads. The company has invested time and effort to create dashboards that the company wants to preserve. The dashboards need to be highly available and cannot be down for longer than 10 minutes. The company needs to minimize ongoing maintenance.

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

- A. Migrate to Amazon CloudWatch dashboards. Recreate the dashboards to match the existing Grafana dashboards. Use automatic dashboards where possible.
- B. Create an Amazon Managed Grafana workspace. Configure a new Amazon CloudWatch data source. Export dashboards from the existing Grafana instance. Import the dashboards into the new workspace.
- C. Create an AMI that has Grafana pre-installed. Store the existing dashboards in Amazon Elastic File System (Amazon EFS). Create an Auto Scaling group that uses the new AMI. Set the Auto Scaling group's minimum, desired, and maximum number of instances to one. Create an Application Load Balancer that serves at least two Availability Zones.
- D. Configure AWS Backup to back up the EC2 instance that runs Grafana once each hour. Restore the EC2 instance from the most recent snapshot in an alternate Availability Zone when required.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

gotta be a B

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

Def B.

upvoted 1 times

 **psyx21** 3 months ago

Selected Answer: B

Correct answer is B

upvoted 1 times

 **easytoo** 3 months ago

Selected Answer: B

By creating an Amazon Managed Grafana workspace, you can offload the operational overhead of managing and maintaining the Grafana infrastructure. Amazon Managed Grafana is a fully managed service that takes care of the underlying infrastructure, including scalability, availability, and updates.

upvoted 2 times

 **bhanus** 3 months ago

Selected Answer: B

B is the answer <https://aws.amazon.com/grafana/>

upvoted 1 times

Question #214

Topic 1

A company needs to migrate its customer transactions database from on premises to AWS. The database resides on an Oracle DB instance that runs on a Linux server. According to a new security requirement, the company must rotate the database password each year.

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

- A. Convert the database to Amazon DynamoDB by using the AWS Schema Conversion Tool (AWS SCT). Store the password in AWS Systems Manager Parameter Store. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function for yearly password rotation.
- B. Migrate the database to Amazon RDS for Oracle. Store the password in AWS Secrets Manager. Turn on automatic rotation. Configure a yearly rotation schedule.
- C. Migrate the database to an Amazon EC2 instance. Use AWS Systems Manager Parameter Store to keep and rotate the connection string by using an AWS Lambda function on a yearly schedule.
- D. Migrate the database to Amazon Neptune by using the AWS Schema Conversion Tool (AWS SCT). Create an Amazon CloudWatch alarm to invoke an AWS Lambda function for yearly password rotation.

 **dkcloudguru** 1 week, 5 days ago

Doubt in question it mention yearly rotation, if you can see in Secret Manager the dropdown options are hourly, days, week, and months it doesn't have the yearly option, however, you can mention 12 if that is the case then option B is correct else option C

upvoted 1 times

 **Simon523** 4 weeks, 1 day ago

Selected Answer: B

https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets_turn-on-for-other.html#rotate-secrets_turn-on-for-other_step1

upvoted 1 times

 **Just_Ninja** 2 months, 1 week ago

Selected Answer: B

It is sad that so many questions here are marked as correct with a wrong result.

Well Architeting Framework!!!

upvoted 1 times

 **nicecurls** 2 months, 2 weeks ago

Selected Answer: B

ofc it's B

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B for sure

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: B

Secrets manager has built-in rotation feature

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

keyword = Secrets Manager.

Then B

upvoted 1 times

 **psyx21** 3 months ago

Selected Answer: B

Correct answer is B

upvoted 1 times

 **easystoo** 3 months ago

b-b-b-b-b-b-b-b-b-b

upvoted 1 times

 **bhanus** 3 months ago

B is the answer

upvoted 1 times

 **chiaseed** 3 months, 1 week ago

Selected Answer: B
I'd vote for B. A keyword that leads me to B is "rotate the database password each year." This is referring to Secrets Manager.
upvoted 1 times

 **emiliocb4** 3 months, 1 week ago

Selected Answer: B
least operation... rds + secret manager
upvoted 1 times

 **nexus2020** 3 months, 1 week ago

Selected Answer: B
the LEAST operational overhead. So B is the easiest
upvoted 2 times

Question #215

Topic 1

A solutions architect is designing an AWS account structure for a company that consists of multiple teams. All the teams will work in the same AWS Region. The company needs a VPC that is connected to the on-premises network. The company expects less than 50 Mbps of total traffic to and from the on-premises network.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Create an AWS CloudFormation template that provisions a VPC and the required subnets. Deploy the template to each AWS account.
- B. Create an AWS CloudFormation template that provisions a VPC and the required subnets. Deploy the template to a shared services account. Share the subnets by using AWS Resource Access Manager.
- C. Use AWS Transit Gateway along with an AWS Site-to-Site VPN for connectivity to the on-premises network. Share the transit gateway by using AWS Resource Access Manager.
- D. Use AWS Site-to-Site VPN for connectivity to the on-premises network.
- E. Use AWS Direct Connect for connectivity to the on-premises network.

 **SK_Tyagi** 1 month ago

Selected Answer: BD

Direct Connect may be an overkill with 1GBPs

upvoted 1 times

 **kebmiockey** 1 month ago

Other problem with VPN is 1.25 Gb limitation.

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct AD.

I think A is correct because you can connect the VPN to each VPC by using a VPN connection resource in each AWS account. You do not need a shared network account for that. You can refer to this documentation for more details:

https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html

B is not correct because it will create a single VPC for all the AWS accounts, which will reduce the isolation and security for the different teams. It will also require sharing the subnets by using AWS Resource Access Manager, which will add complexity and overhead.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: BD

BD

they need a (one) VPC, no need for TGW.

Use case for subnet sharing via RAM

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: BD

Tgw is for VPCs communication.

upvoted 1 times

 **SmileyCloud** 2 months, 3 weeks ago

Selected Answer: BC

BC. There are multiple teams and accounts.

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: BD

BD? dont think we need tgw here.

upvoted 1 times

 **easystoo** 3 months ago

b-d...b-d

upvoted 1 times

 **psyx21** 3 months ago

Selected Answer: BD

BD is correct

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: BD

BD? dont think we need tgw here.

upvoted 1 times

 **emiliocb4** 3 months, 1 week ago

Selected Answer: BD

A is wrong because how to connect the vpn to each vpc? you need an account where you deploy the shared network part... i will go with B

upvoted 3 times

Question #216

Topic 1

A solutions architect at a large company needs to set up network security for outbound traffic to the internet from all AWS accounts within an organization in AWS Organizations. The organization has more than 100 AWS accounts, and the accounts route to each other by using a centralized AWS Transit Gateway. Each account has both an internet gateway and a NAT gateway for outbound traffic to the internet. The company deploys resources only into a single AWS Region.

The company needs the ability to add centrally managed rule-based filtering on all outbound traffic to the internet for all AWS accounts in the organization. The peak load of outbound traffic will not exceed 25 Gbps in each Availability Zone.

Which solution meets these requirements?

- A. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Create an Auto Scaling group of Amazon EC2 instances that run an open-source internet proxy for rule-based filtering across all Availability Zones in the Region. Modify all default routes to point to the proxy's Auto Scaling group.
- B. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Use an AWS Network Firewall firewall for rule-based filtering. Create Network Firewall endpoints in each Availability Zone. Modify all default routes to point to the Network Firewall endpoints.
- C. Create an AWS Network Firewall firewall for rule-based filtering in each AWS account. Modify all default routes to point to the Network Firewall firewalls in each account.
- D. In each AWS account, create an Auto Scaling group of network-optimized Amazon EC2 instances that run an open-source internet proxy for rule-based filtering. Modify all default routes to point to the proxy's Auto Scaling group.

 **duriselvan** 4 days, 21 hours ago

<https://aws.amazon.com/blogs/security/hands-on-walkthrough-of-the-aws-network-firewall-flexible-rules-engine/>

upvoted 1 times

 **xav1er** 1 month ago

Selected Answer: B

Given the available options and the requirements:

B. Create an interface VPC endpoint for API Gateway, and set an endpoint policy to only allow access to the specific API. Add a resource policy to API Gateway to only allow access from the VPC endpoint. Change the API Gateway endpoint type to private. is the correct answer.

upvoted 1 times

 **chikorita** 1 month ago

bro what?

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B for sure

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: B

centrally managed outbound traffic: tgw-> centralized VPC with network firewall with rules-> internet

upvoted 2 times

 **chiaseed** 3 months ago

Selected Answer: B

vote for B. The keyword is "centrally managed rule-based filtering on outbound traffic to the internet for all AWS accounts...". Network Firewall can centrally manage network security policies.

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B. Answer A is similar, but you have to deal with EC2 instances and dealing with 3rd party FW, not good - management overhead. C is impossible. D is waay to much hard to manage.

upvoted 1 times

 **easystoo** 3 months ago

b-b-b-b-b

Create a new VPC specifically dedicated to outbound traffic to the internet. This helps isolate and manage the outbound traffic separately from

other resources.

Connect the existing transit gateway to the new VPC. This ensures that the VPC is connected to the centralized transit gateway that routes traffic between AWS accounts.

Configure a new NAT gateway within the new VPC. This NAT gateway provides the necessary outbound connectivity to the internet for resources within the VPC.

Use AWS Network Firewall, a managed firewall service, for rule-based filtering on the outbound traffic. Network Firewall allows you to define and enforce custom rules for traffic leaving the VPC.

Create Network Firewall endpoints in each Availability Zone. These endpoints serve as the traffic inspection points where Network Firewall applies the filtering rules.

Modify all default routes in the VPCs to point to the Network Firewall endpoints. This ensures that all outbound traffic from the VPCs flows through the Network Firewall for rule-based filtering.

upvoted 2 times

 **psyx21** 3 months ago

Selected Answer: B

Correct answer is B

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: B

vote for B

upvoted 2 times

Question #217

Topic 1

A company uses a load balancer to distribute traffic to Amazon EC2 instances in a single Availability Zone. The company is concerned about security and wants a solutions architect to re-architect the solution to meet the following requirements:

- Inbound requests must be filtered for common vulnerability attacks.
- Rejected requests must be sent to a third-party auditing application.
- All resources should be highly available.

Which solution meets these requirements?

- A. Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target. Use Amazon Inspector to monitor traffic to the ALB and EC2 instances. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB. Use an AWS Lambda function to frequently push the Amazon Inspector report to the third-party auditing application.
- B. Configure an Application Load Balancer (ALB) and add the EC2 instances as targets. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB name and enable logging with Amazon CloudWatch Logs. Use an AWS Lambda function to frequently push the logs to the third-party auditing application.
- C. Configure an Application Load Balancer (ALB) along with a target group adding the EC2 instances as targets. Create an Amazon Kinesis Data Firehose with the destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.
- D. Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target. Create an Amazon Kinesis Data Firehose with a destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the WebACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.

 **Maria2023** Highly Voted  3 months ago

Selected Answer: D

Only A and D cover the requirement for high availability. A uses Inspector, which is a vulnerability scanner and does not monitor traffic. So - even that I don't like the complexity of D - this remains the only option

upvoted 5 times

 **SK_Tyagi** Most Recent  1 month ago

Selected Answer: D

I was confused between A and D, but seems WAF can deliver logs to Firehose
<https://docs.aws.amazon.com/waf/latest/developerguide/logging-kinesis.html>

upvoted 1 times

 **xav1er** 1 month ago

Selected Answer: D

It's D, makes most sense,

upvoted 1 times

 **chico2023** 1 month, 1 week ago

This is such a mal formed question...

You see, nowhere in the question we are told about customer's application. However we are told they want ALL their resources highly available. B would be sooo much better if there wasn't that "All resources should be highly available." because, seriously, D is not the best in my opinion. We don't know much what applications they use, what third party auditing application and so on...

Anyway, it might be D after all, but oh my...

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct D.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

its a D

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: D

ASG in Multiple AZ. WAF and WAF logs with kinesis
upvoted 1 times

chikorita 3 months ago

"enable logging by selecting the Kinesis Data Firehose as the destination"--- how can ALB write logs directly to Kinesis???
it should be CW logs group
any links for help??

upvoted 1 times

Masonryeh 3 months ago

Selected Answer: D
Amazon inspector does NOT inspect traffic coming to an Application Load Balancer (ALB)
upvoted 2 times

PhuocT 3 months ago

Selected Answer: D
D is correct answer
Inbound requests must be filtered for common vulnerability attacks -> WAF
Rejected requests must be sent to a third-party auditing application-> Enable access log and use kinesis stream to send logs to third party
All resources should be highly available -> Muti AZ auto scaling group.
upvoted 2 times

ozelliII 3 months ago

Selected Answer: D
Inspector does not filter inbound traffic for attack signatures, this is what WAF is for
upvoted 1 times

SmileyCloud 3 months ago

Selected Answer: A
B and C do not provide HA. D is similar to A but lacks Inspector -> "Amazon Inspector automatically discovers workloads, such as Amazon EC2 instances, containers, and Lambda functions, and scans them for software vulnerabilities and unintended network exposure."
upvoted 2 times

javitech83 2 months, 4 weeks ago

but you need logs of the reject request on WAF. So I think correct answer is D
upvoted 1 times

SmileyCloud 2 months, 3 weeks ago

It's probably B. C and D are not correct, ALB can't send logs to Kinesis Fire Hose.
upvoted 1 times

easytoo 3 months ago

a-a-a-a-a-a-a
multi-az for HA
upvoted 1 times

easytoo 1 month, 3 weeks ago

it's d-d-d-d-d-d-d-d
upvoted 1 times

bhanus 3 months ago

Selected Answer: D
I got with D. The reason to go with D is because other options ABC are wrong.

1. It says use Amazon Inspector to inspect traffic to ALB. This is wrong. Amazon inspector does NOT inspect traffic coming to an Application Load Balancer (ALB). Amazon Inspector is a security assessment service that helps you analyze the security and compliance of your EC2 instances and applications running on them. To inspect traffic coming to an ALB, you can consider using other services such as AWS WAF (Web Application Firewall) or AWS Shield. AWS WAF allows you to define rules to filter and block malicious traffic targeting your ALB.

B - Does NOT talk about HA as it is asked in ques

C - Does NOT talk about HA as it is asked in ques

upvoted 2 times

bhanus 3 months ago

Option B and C does NOT talk about HA. Its between A and D ..
upvoted 1 times

bhanus 2 months, 4 weeks ago

D is answer
A is wrong as Amazon inspector does NOT inspect traffic coming to an Application Load Balancer (ALB)
upvoted 1 times

emiliocb4 3 months, 1 week ago

Selected Answer: A
with B you don't guarantee the HA of the EC2s.... i will go with A

upvoted 2 times

Question #218

Topic 1

A company is running an application in the AWS Cloud. The application consists of microservices that run on a fleet of Amazon EC2 instances in multiple Availability Zones behind an Application Load Balancer. The company recently added a new REST API that was implemented in Amazon API Gateway. Some of the older microservices that run on EC2 instances need to call this new API.

The company does not want the API to be accessible from the public internet and does not want proprietary data to traverse the public internet.

What should a solutions architect do to meet these requirements?

- A. Create an AWS Site-to-Site VPN connection between the VPC and the API Gateway. Use API Gateway to generate a unique API Key for each microservice. Configure the API methods to require the key.
- B. Create an interface VPC endpoint for API Gateway, and set an endpoint policy to only allow access to the specific API. Add a resource policy to API Gateway to only allow access from the VPC endpoint. Change the API Gateway endpoint type to private.
- C. Modify the API Gateway to use IAM authentication. Update the IAM policy for the IAM role that is assigned to the EC2 instances to allow access to the API Gateway. Move the API Gateway into a new VPDeploy a transit gateway and connect the VPCs.
- D. Create an accelerator in AWS Global Accelerator, and connect the accelerator to the API Gateway. Update the route table for all VPC subnets with a route to the created Global Accelerator endpoint IP address. Add an API key for each service to use for authentication.

 **Just_Ninja** 2 months ago

Selected Answer: B

The quality control here is unfortunately not as expected when you buy access.

C is due nonsense.

B is correct.

VPC Endpoint to API Gateway and a policy on both sides!

Trust me, i'm a Ninja

upvoted 2 times

 **rxhan** 2 months ago

thanks Ninja

upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

B for sure

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: B

Tip: Anytime you see "don't want to traverse Internet traffic" always look for endpoint in the answers. Most likely, that's the answer.

upvoted 3 times

 **Alabi** 3 months ago

Selected Answer: B

B for sure

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

Tip: Anytime you see "don't want to traverse Internet traffic" always look for endpoint in the answers. Most likely, that's the answer.

upvoted 3 times

 **easystoo** 3 months ago

b-b-b-b-b-b-b

By implementing this solution, the company can ensure that the new API in API Gateway is not accessible from the public internet. The interface VPC endpoint provides private connectivity, allowing secure communication between the microservices running on EC2 instances and the API Gateway. This ensures the proprietary data does not traverse the public internet, enhancing security and data protection.

upvoted 3 times

 **bhanus** 3 months ago

I vote B

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: B

VPC endpoint usually is the perfect answer to avoid internet traffic

upvoted 1 times

Question #219

Topic 1

A company has set up its entire infrastructure on AWS. The company uses Amazon EC2 instances to host its ecommerce website and uses Amazon S3 to store static data. Three engineers at the company handle the cloud administration and development through one AWS account. Occasionally, an engineer alters an EC2 security group configuration of another engineer and causes noncompliance issues in the environment.

A solutions architect must set up a system that tracks changes that the engineers make. The system must send alerts when the engineers make noncompliant changes to the security settings for the EC2 instances.

What is the FASTEST way for the solutions architect to meet these requirements?

- A. Set up AWS Organizations for the company. Apply SCPs to govern and track noncompliant security group changes that are made to the AWS account.
- B. Enable AWS CloudTrail to capture the changes to EC2 security groups. Enable Amazon CloudWatch rules to provide alerts when noncompliant security settings are detected.
- C. Enable SCPs on the AWS account to provide alerts when noncompliant security group changes are made to the environment.
- D. Enable AWS Config on the EC2 security groups to track any noncompliant changes. Send the changes as alerts through an Amazon Simple Notification Service (Amazon SNS) topic.

 **Sweetedad** 3 weeks, 5 days ago

Selected Answer: D

Both B and D work, except B has no notification set.

<https://aws.amazon.com/blogs/security/how-to-monitor-aws-account-configuration-changes-and-api-calls-to-amazon-ec2-security-groups/>

upvoted 1 times

 **ghadxx** 1 month, 1 week ago

It's D

<https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>

upvoted 1 times

 **grodskiy** 2 months ago

Correct D.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

D works and faster

B would work with adding a CW alert, but D still better

upvoted 2 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: D

correct is D

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: D

D

reference link

<https://aws.amazon.com/es/blogs/industries/how-to-monitor-alert-and-remediate-non-compliant-hipaa-findings-on-aws/>

upvoted 3 times

 **SmileyCloud** 3 months ago

Selected Answer: D

It's D. Check this link, something similar: <https://aws.amazon.com/blogs/industries/how-to-monitor-alert-and-remediate-non-compliant-hipaa-findings-on-aws/>

upvoted 3 times

 **MoussaNoussa** 3 months ago

it's D of course!

upvoted 1 times

 **easytoo** 3 months ago

b-b-b-b-b-b-b

upvoted 1 times

✉  **easytoo** 3 months ago

changed to d-d-d-d-d-d

This solution is the FASTEST way to meet the requirements because it does not require any additional infrastructure or configuration. AWS Config can be enabled and configured in minutes, and it will immediately start tracking changes to the EC2 security groups.

The other solutions are not as fast. For example, setting up AWS Organizations and SCPs would require more time and effort. Additionally, enabling CloudTrail and CloudWatch rules would only track changes to the EC2 security groups, but they would not send alerts when noncompliant changes are detected

upvoted 2 times

✉  **bhanus** 3 months ago

Selected Answer: D

I vote D. aws config changes can be sent to SNS topic <https://docs.aws.amazon.com/config/latest/developerguide/notifications-for-AWS-Config.html>

upvoted 3 times

✉  **nexus2020** 3 months ago

Selected Answer: B

CloudTrail and aws config can both track config changes, but sending to SNS (D)?

I would go with B

upvoted 1 times

✉  **javitech83** 2 months, 4 weeks ago

Cloudwatch is not useful at all for sending alerts, we would need Eventbridge to alert based on cloudtrail events. And for D, yes aws config can send events to SNS <https://docs.aws.amazon.com/config/latest/developerguide/notifications-for-AWS-Config.html>

upvoted 1 times

Question #220

Topic 1

A company has IoT sensors that monitor traffic patterns throughout a large city. The company wants to read and collect data from the sensors and perform aggregations on the data.

A solutions architect designs a solution in which the IoT devices are streaming to Amazon Kinesis Data Streams. Several applications are reading from the stream. However, several consumers are experiencing throttling and are periodically encountering a `ReadProvisionedThroughputExceeded` error.

Which actions should the solutions architect take to resolve this issue? (Choose three.)

- A. Reshard the stream to increase the number of shards in the stream.
- B. Use the Kinesis Producer Library (KPL). Adjust the polling frequency.
- C. Use consumers with the enhanced fan-out feature.
- D. Reshard the stream to reduce the number of shards in the stream.
- E. Use an error retry and exponential backoff mechanism in the consumer logic.
- F. Configure the stream to use dynamic partitioning.

 **easytoo** Highly Voted 3 months ago

To resolve the issue of throttling and ReadProvisionedThroughputExceeded errors in the Amazon Kinesis Data Streams scenario, the solutions architect should take the following actions:

1. A. Reshard the stream to increase the number of shards in the stream: By increasing the number of shards, you can increase the overall throughput capacity of the stream, allowing for more concurrent consumers to read from the stream without being throttled.
2. C. Use consumers with the enhanced fan-out feature: Enhanced fan-out allows for multiple consumers to read from the same shard concurrently, without being limited by the read capacity of the shard. This helps distribute the load and reduces the chances of throttling.
3. E. Use an error retry and exponential backoff mechanism in the consumer logic: Implementing an error retry mechanism with exponential backoff in the consumer logic will help handle throttling errors gracefully. When a ReadProvisionedThroughputExceeded error occurs, the consumer can retry the read operation after a certain delay, gradually increasing the delay between retries to avoid overwhelming the system.

upvoted 7 times

 **ggrodsckiy** Most Recent 2 months ago

Correct ACE.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: ACE

ACE it

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: ACE

ACE is correct

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: ACE

Eliminate B, KPL is for writing. "The Kinesis Producer Library (KPL) simplifies producer application development, allowing developers to achieve high write throughput to a Kinesis data stream. " The error was reading.

F, dynamic partitioning is used for different use cases.<https://docs.aws.amazon.com/firehose/latest/dev/dynamic-partitioning.html>

upvoted 2 times

 **psyx21** 3 months ago

Selected Answer: ACE

ACE is correct

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: ACE

not sure about E, but I would go with AC

upvoted 1 times

Question #221

Topic 1

A company uses AWS Organizations to manage its AWS accounts. The company needs a list of all its Amazon EC2 instances that have underutilized CPU or memory usage. The company also needs recommendations for how to downsize these underutilized instances.

Which solution will meet these requirements with the LEAST effort?

- A. Install a CPU and memory monitoring tool from AWS Marketplace on all the EC2 instances. Store the findings in Amazon S3. Implement a Python script to identify underutilized instances. Reference EC2 instance pricing information for recommendations about downsizing options.
- B. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in the organization's management account. Use the recommendations to downsize underutilized instances in all accounts of the organization.
- C. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in each account of the organization. Use the recommendations to downsize underutilized instances in all accounts of the organization.
- D. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Create an AWS Lambda function to extract CPU and memory usage from all the EC2 instances. Store the findings as files in Amazon S3. Use Amazon Athena to find underutilized instances. Reference EC2 instance pricing information for recommendations about downsizing options.

 **SK_Tyagi** 1 month ago

Selected Answer: B

IMO it could be done with either B or D. But the differentiator is "Least Effort" that makes it B

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

its a B

upvoted 1 times

 **bhanus** 2 months, 4 weeks ago

Selected Answer: B

Though I vote B. No better choice. This is worst ques. How can cost explorer provide recommendations?. Its should be cost optimizer

upvoted 2 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

Classic usage de Cloudwatch metrics and AWS Organization in master account .

C not because more overhead each account for example 100 accounts.

Note : Compute Optimizer is more apropiate in this case but no exist option

upvoted 1 times

 **Maria2023** 3 months ago

Actually, the right answer is to use Compute Optimizer, I don't understand why it was not part of the choices here

<https://aws.amazon.com/compute-optimizer/>

upvoted 3 times

 **easystoo** 3 months ago

B. Install the Amazon CloudWatch agent on all the EC2 instances using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in the organization's management account. Use the recommendations to downsize underutilized instances in all accounts of the organization.

This solution leverages the capabilities of AWS CloudWatch and AWS Cost Explorer to monitor and analyze the CPU and memory usage of EC2 instances. By installing the CloudWatch agent, you can collect the necessary metrics for monitoring. AWS Cost Explorer provides resource optimization recommendations, which can be accessed from the organization's management account. These recommendations can then be used to identify underutilized instances and make informed decisions about downsizing.

This solution requires minimal effort as it utilizes existing AWS services and tools, eliminating the need for additional installations or custom scripts. It also provides a centralized approach by retrieving recommendations from the organization's management account, allowing for efficient management of all accounts within the organization.

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B. That's why you have the management account so you don't have to go to 1000+ accounts and get metrics.

upvoted 3 times

 **bhanus** 3 months ago

Selected Answer: B

B - Management account is the key word

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: B

B. the standard way AWS recommended

upvoted 1 times

Question #222

Topic 1

A company wants to run a custom network analysis software package to inspect traffic as traffic leaves and enters a VPC. The company has deployed the solution by using AWS CloudFormation on three Amazon EC2 instances in an Auto Scaling group. All network routing has been established to direct traffic to the EC2 instances.

Whenever the analysis software stops working, the Auto Scaling group replaces an instance. The network routes are not updated when the instance replacement occurs.

Which combination of steps will resolve this issue? (Choose three.)

- A. Create alarms based on EC2 status check metrics that will cause the Auto Scaling group to replace the failed instance.
- B. Update the CloudFormation template to install the Amazon CloudWatch agent on the EC2 instances. Configure the CloudWatch agent to send process metrics for the application.
- C. Update the CloudFormation template to install AWS Systems Manager Agent on the EC2 instances. Configure Systems Manager Agent to send process metrics for the application.
- D. Create an alarm for the custom metric in Amazon CloudWatch for the failure scenarios. Configure the alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
- E. Create an AWS Lambda function that responds to the Amazon Simple Notification Service (Amazon SNS) message to take the instance out of service. Update the network routes to point to the replacement instance.
- F. In the CloudFormation template, write a condition that updates the network routes when a replacement instance is launched.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: BDE

CW agent->CW metric->CW alarm->Lambda action

upvoted 3 times

 **Piccaso** 2 months, 3 weeks ago

Selected Answer: BDE

A and F must be wrong.

upvoted 1 times

 **PhuocT** 3 months ago

Selected Answer: BDE

B, D and E

upvoted 2 times

 **easytoo** 3 months ago

b-d-e seems reasonable.

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: BDE

A is redundant because "Whenever the analysis software stops working, the Auto Scaling group replaces an instance."

C is not correct. AWS System Manager Agebt is not used "to send process metrics for the application."

So, B, D and E because they make a flow.

upvoted 3 times

 **james55** 3 months ago

Selected Answer: BDE

b----d----e

upvoted 1 times

Question #223

Topic 1

A company is developing a new on-demand video application that is based on microservices. The application will have 5 million users at launch and will have 30 million users after 6 months. The company has deployed the application on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. The company developed the application by using ECS services that use the HTTPS protocol.

A solutions architect needs to implement updates to the application by using blue/green deployments. The solution must distribute traffic to each ECS service through a load balancer. The application must automatically adjust the number of tasks in response to an Amazon CloudWatch alarm.

Which solution will meet these requirements?

- A. Configure the ECS services to use the blue/green deployment type and a Network Load Balancer. Request increases to the service quota for tasks per service to meet the demand.
- B. Configure the ECS services to use the blue/green deployment type and a Network Load Balancer. Implement Auto Scaling group for each ECS service by using the Cluster Autoscaler.
- C. Configure the ECS services to use the blue/green deployment type and an Application Load Balancer. Implement an Auto Scaling group for each ECS service by using the Cluster Autoscaler.
- D. Configure the ECS services to use the blue/green deployment type and an Application Load Balancer. Implement Service Auto Scaling for each ECS service.

 **ggrodskiy** 2 months ago

Correct D.

upvoted 1 times

 **Hypercuber** 2 months ago

Selected Answer: D

Answer is D. For those voting C, remember that it's on Fargate, so there is no such cluster autoscaling.

upvoted 1 times

 **nicecurls** 2 months, 2 weeks ago

Selected Answer: D

select D. for Fargate there is no Cluster Auto Scaling there.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

D

no NLB for ECS, no Cluster for Fargate

upvoted 1 times

 **vjp_training** 1 month, 1 week ago

D is correct but you can use NLB for ECS. Key word is Service Auto Scaling

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/create-network-load-balancer.html>

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: D

@MODERATOR, PLEASE remove my previous comment as I mentioned C.

As per comment from SmileyCloud , C is not correct because there is no Cluster Auto Scaling. D is the answer.

Thank you @SmileyCloud for clarifying

D is the answer

upvoted 2 times

 **SkyZeroZx** 3 months ago

Selected Answer: D

<https://repost.aws/knowledge-center/ecs-fargate-service-auto-scaling>

upvoted 2 times

 **easystoo** 3 months ago

d-d-d-d-d-d-d

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: D

A and B are out, it says the app uses HTTPS.

C is out because we have Fargate and there is no Cluster Auto Scaling there.

So, it's D because we have Service Auto Scaling. -> <https://repost.aws/knowledge-center/ecs-fargate-service-auto-scaling>

upvoted 4 times

 **emiliocb4** 3 months ago

NLB supports HTTPS so why excluding A?

upvoted 1 times

 **SmileyCloud** 2 months, 3 weeks ago

Unlike a Classic Load Balancer or an Application Load Balancer, a Network Load Balancer can't have application layer (layer 7) HTTP or HTTPS listeners. It only supports transport layer (layer 4) TCP listeners. HTTP and HTTPS traffic can be routed to your environment over TCP.

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-nlb.html#>

upvoted 3 times

 **james55** 3 months ago

Selected Answer: D

"Amazon ECS cluster auto scaling is only supported with Auto Scaling group capacity providers. For Amazon ECS workloads that are hosted on AWS Fargate, see AWS Fargate capacity providers."

upvoted 2 times

 **bhanus** 3 months ago

Selected Answer: C

AB are eliminated because of NLB

C has Auto Scaling Group with Cluster Autoscaler: As per ChatGPT - By implementing an Auto Scaling group for each ECS service using the Cluster Autoscaler, you can automatically adjust the number of tasks (containers) based on the demand. The Cluster Autoscaler scales the ECS tasks in response to CloudWatch alarms, allowing you to scale the infrastructure up or down to handle the increasing number of users.

upvoted 3 times

 **bhanus** 2 months, 4 weeks ago

changing my vote to D as SmileyCloud pointed. for Fargate there is no Cluster Auto Scaling there.

upvoted 2 times

Question #224

Topic 1

A company is running a containerized application in the AWS Cloud. The application is running by using Amazon Elastic Container Service (Amazon ECS) on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group.

The company uses Amazon Elastic Container Registry (Amazon ECR) to store its container images. When a new image version is uploaded, the new image version receives a unique tag.

The company needs a solution that inspects new image versions for common vulnerabilities and exposures. The solution must automatically delete new image tags that have Critical or High severity findings. The solution also must notify the development team when such a deletion occurs.

Which solution meets these requirements?

- A. Configure scan on push on the repository. Use Amazon EventBridge to invoke an AWS Step Functions state machine when a scan is complete for images that have Critical or High severity findings. Use the Step Functions state machine to delete the image tag for those images and to notify the development team through Amazon Simple Notification Service (Amazon SNS).
- B. Configure scan on push on the repository. Configure scan results to be pushed to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Lambda function when a new message is added to the SQS queue. Use the Lambda function to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).
- C. Schedule an AWS Lambda function to start a manual image scan every hour. Configure Amazon EventBridge to invoke another Lambda function when a scan is complete. Use the second Lambda function to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- D. Configure periodic image scan on the repository. Configure scan results to be added to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Step Functions state machine when a new message is added to the SQS queue. Use the Step Functions state machine to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A, but I think step function need to call Lambda to delete tag. there is not direct ecr integration
upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: A

Use the building feature if you can, so scan on push.
I go with A because other options are not good B - you cannot use SES.
upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: A

I vote A since I tested it and confirm it's achievable. As for B - I couldn't find any option to publish the result of the scan to SQS so I stopped there
upvoted 1 times

 **elanelans** 3 months ago

Selected Answer: A

A meet the requirements.
<https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html>
<https://docs.aws.amazon.com/AmazonECR/latest/userguide/ecr-eventbridge.html>
upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: A

C and D are out because they are not automatic but rather scheduled.
B is out because you don't need SQS for this and def don't need SES.
A makes sense because it's much leaner solution.
upvoted 2 times

 **nexus2020** 3 months ago

Selected Answer: A

Use the building feature if you can, so scan on push. And A make more sense

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: A

I go with A because other options are not good
B - you cannot use SES. SES is generally used to send Bulk/marketing emails.
C- schedule Lambda to scan every hour is not a good approach
D - like B you cannot use SES for this use case.
So A sounds reasonable

upvoted 2 times

 **emiliocb4** 3 months, 1 week ago

why not A ?

upvoted 1 times

Question #225

Topic 1

A company runs many workloads on AWS and uses AWS Organizations to manage its accounts. The workloads are hosted on Amazon EC2, AWS Fargate, and AWS Lambda. Some of the workloads have unpredictable demand. Accounts record high usage in some months and low usage in other months.

The company wants to optimize its compute costs over the next 3 years. A solutions architect obtains a 6-month average for each of the accounts across the organization to calculate usage.

Which solution will provide the MOST cost savings for all the organization's compute usage?

- A. Purchase Reserved Instances for the organization to match the size and number of the most common EC2 instances from the member accounts.
- B. Purchase a Compute Savings Plan for the organization from the management account by using the recommendation at the management account level.
- C. Purchase Reserved Instances for each member account that had high EC2 usage according to the data from the last 6 months.
- D. Purchase an EC2 Instance Savings Plan for each member account from the management account based on EC2 usage data from the last 6 months.

 **elanelans** Highly Voted  3 months ago

Selected Answer: B

- A. Incorrect: RI's Supports only EC2 instances.
- B. Correct: Compute savings plan supports EC2, Fargate and Lambda. Applied in Organization's management account.
- C. Incorrect: RI's Supports only EC2 instances and Changes to be applied at Organizations management account.
- D. Incorrect: Instance Saving plan supports only EC2.

upvoted 5 times

 **NikkyDicky** Most Recent  2 months, 3 weeks ago

Selected Answer: B

its a B

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

- A. Incorrect: RI's Supports only EC2 instances.
- B. Correct: Compute savings plan supports EC2, Fargate and Lambda. Applied in Organization's management account.
- C. Incorrect: RI's Supports only EC2 instances and Changes to be applied at Organizations management account.
- D. Incorrect: Instance Saving plan supports only EC2.

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B, magic keywords - Management account and Compute savings Plan.

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: B

Compute Savings plan is made for this usage type

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: B

B- compute savings plans covers all ec2, fargate, lambda.

upvoted 1 times

Question #226

Topic 1

A company has hundreds of AWS accounts. The company uses an organization in AWS Organizations to manage all the accounts. The company has turned on all features.

A finance team has allocated a daily budget for AWS costs. The finance team must receive an email notification if the organization's AWS costs exceed 80% of the allocated budget. A solutions architect needs to implement a solution to track the costs and deliver the notifications.

Which solution will meet these requirements?

- A. In the organization's management account, use AWS Budgets to create a budget that has a daily period. Add an alert threshold and set the value to 80%. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.
- B. In the organization's management account, set up the organizational view feature for AWS Trusted Advisor. Create an organizational view report for cost optimization. Set an alert threshold of 80%. Configure notification preferences. Add the email addresses of the finance team.
- C. Register the organization with AWS Control Tower. Activate the optional cost control (guardrail). Set a control (guardrail) parameter of 80%. Configure control (guardrail) notification preferences. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.
- D. Configure the member accounts to save a daily AWS Cost and Usage Report to an Amazon S3 bucket in the organization's management account. Use Amazon EventBridge to schedule a daily Amazon Athena query to calculate the organization's costs. Configure Athena to send an Amazon CloudWatch alert if the total costs are more than 80% of the allocated budget. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.

 **nicecurls** 2 months, 2 weeks ago

Selected Answer: A

ofc it's A

https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-professional-sap-c02/view/#
upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

straight A

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: A

- A. Makes sense.
- B. Trusted advisor not required.
- C. Control Tower not required.
- D. Budgets can be managed in Org's Mgmt account itself.

upvoted 1 times

 **rxhan** 1 month, 4 weeks ago

you copy and paste other people answers

upvoted 4 times

 **easytoo** 3 months ago

a-a-a-a-a-a-a

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: A

This one is simple. A

upvoted 1 times

 **elanelans** 3 months ago

Selected Answer: A

- A. Makes sense.
- B. Trusted advisor not required.
- C. Control Tower not required.
- D. Budgets can be managed in Org's Mgmt account itself.

upvoted 4 times

 **nexus2020** 3 months ago

Selected Answer: A

A, simple one

upvoted 1 times

 **MoussaNoussa** 3 months ago

A is the answer

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: A

A is the answer

upvoted 1 times

Question #227

Topic 1

A company provides auction services for artwork and has users across North America and Europe. The company hosts its application in Amazon EC2 instances in the us-east-1 Region. Artists upload photos of their work as large-size, high-resolution image files from their mobile phones to a centralized Amazon S3 bucket created in the us-east-1 Region. The users in Europe are reporting slow performance for their image uploads.

How can a solutions architect improve the performance of the image upload process?

- A. Redeploy the application to use S3 multipart uploads.
- B. Create an Amazon CloudFront distribution and point to the application as a custom origin.
- C. Configure the buckets to use S3 Transfer Acceleration.
- D. Create an Auto Scaling group for the EC2 instances and create a scaling policy.

 **skyhiker** 1 month ago

I would choose A. Why does C say "Configure the buckets [more than one] to use S3 Transfer Acceleration? Sometimes you have to hate how these questions and answers are worded.

upvoted 1 times

 **skyhiker** 1 month ago

C would be the answer if the 's' was removed. Will go with C.

upvoted 1 times

 **chico2023** 1 month, 1 week ago

Selected Answer: C

Main point of the question: "The users in Europe are reporting slow performance for their image uploads."

How do we improve performance? If we look on the latency side, sure, S3 Transfer Acceleration (option C), but the question puts another variable to our scenario: "Artists upload photos of their work as large-size, high-resolution image files from their mobile phones..."

If you just look at that above, you would switch to A as we can improve upload with multipart.

Here comes the plot twist "The users in Europe are reporting slow performance for their image uploads." - Meaning, in "Europe", not in the "NA". Of course! The bucket in the US... So yeah, question really bad, not objective (in my pov) and with lots of interpretations, but C would help them with the perception of performance in this context.

upvoted 3 times

 **RGR21** 1 month, 3 weeks ago

Selected Answer: A

I have some doubts about this question, it makes more sense to use multipart upload to split the file and gain upload speed. AWS Transfer Accelerator seems to be applied to reduce delay.

<http://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C

would be good in combination with A, but better as a standalone choice

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: C

upload performance-> transfer acceleration

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: C

correct is C

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: A

Transfer Acceleration doesn't guarantee a significant increase in upload speed.

A multi-part upload on the other hand does, because it uploads multiple smaller chunks of the files in parallel.

Ideally multi-part upload and Transfer Accelerator should be deployed together. If we had to pick only one of the two, multi-part upload would result in better performance.

<https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>
upvoted 1 times

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

Using your link, the tests mentioned show C is faster
Single upload with transfer acceleration 40% faster
Multipart upload without transfer acceleration 38% faster
upvoted 3 times

✉ **SkyZeroZx** 3 months ago

Selected Answer: C

C. <https://aws.amazon.com/s3/transfer-acceleration/>

upvoted 1 times

✉ **SmileyCloud** 3 months ago

Selected Answer: C

C. <https://aws.amazon.com/s3/transfer-acceleration/>

upvoted 1 times

✉ **MoussaNoussa** 3 months ago

C of course

upvoted 1 times

✉ **bhanus** 3 months ago

Selected Answer: C

C - Transfer acceleration. S3 Transfer Acceleration utilizes the Amazon CloudFront global network of edge locations to accelerate the transfer of data to and from S3 buckets. By enabling S3 Transfer Acceleration on the centralized S3 bucket, the users in Europe will experience faster uploads as their data will be routed through the closest CloudFront edge location.

upvoted 1 times

Question #228

Topic 1

A company wants to containerize a multi-tier web application and move the application from an on-premises data center to AWS. The application includes web, application, and database tiers. The company needs to make the application fault tolerant and scalable. Some frequently accessed data must always be available across application servers. Frontend web servers need session persistence and must scale to meet increases in traffic.

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

- A. Run the application on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Use Amazon Elastic File System (Amazon EFS) for data that is frequently accessed between the web and application tiers. Store the frontend web server session data in Amazon Simple Queue Service (Amazon SQS).
- B. Run the application on Amazon Elastic Container Service (Amazon ECS) on Amazon EC2. Use Amazon ElastiCache for Redis to cache frontend web server session data. Use Amazon Elastic Block Store (Amazon EBS) with Multi-Attach on EC2 instances that are distributed across multiple Availability Zones.
- C. Run the application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure Amazon EKS to use managed node groups. Use ReplicaSets to run the web servers and applications. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system across all EKS pods to store frontend web server session data.
- D. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure Amazon EKS to use managed node groups. Run the web servers and application as Kubernetes deployments in the EKS cluster. Store the frontend web server session data in an Amazon DynamoDB table. Create an Amazon Elastic File System (Amazon EFS) volume that all applications will mount at the time of deployment.

 **pupsik** Highly Voted 3 months ago

Selected Answer: D

A looked good until "store session data in SQS".

upvoted 5 times

 **rsn** Most Recent 1 week, 5 days ago

Selected Answer: C

There is a requirement for fault tolerance. I feel 'C' satisfies that as it has replicaset.

upvoted 1 times

 **skyhiker** 1 month ago

Now i'll have to go with B. Check out what alabiba says to question, "Can aws sqs be used to store web server session data?" alabiba "No, AWS SQS (Simple Queue Service) is not typically used for storing web server session data. SQS is a message queuing service that is designed for reliable and scalable message communication between distributed systems. For storing session data, it is more common to use dedicated session storage solutions such as databases (e.g., Amazon DynamoDB) or in-memory caches (e.g., Redis)."

upvoted 2 times

 **chikorita** 1 week, 6 days ago

problem with option B is " Multi-Attach on EC2 instances that are distributed across multiple Availability Zones"; please note that multi-attach can only span since AZ
option D is correct

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

D - best of the worst

upvoted 3 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: D

A looked good until "store session data in SQS".

upvoted 1 times

 **Henrytml** 2 months, 3 weeks ago

A looked good until "store session data in SQS".

upvoted 2 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: D

A looked good until "store session data in SQS".

upvoted 1 times

✉️  **SkyZeroZx** 3 months ago

Selected Answer: D

what a worst ques

- A - Why do you need SQS to store web sever session data. SQS is for decoupling services
- B - EBS multi attach is for SAME availability zone. The ques says multipel availability zones
- C - Why do you need EFS to store web sever session data. Its damn expensive
- D - Better answer- But again why need for EKS.

If I were to choose one option, its D as its better compared to ABC

upvoted 4 times

✉️  **Maria2023** 3 months ago

Selected Answer: A

Fargate is the service, the only question remains the storage. Amazon EBS Multi-Attach is single-az service, so remains A. Even though I am not very confident with SQS caching web service sessions.

upvoted 1 times

✉️  **PhuocT** 3 months ago

Agree, this is a worst question

D is best choice for this question, but I would prefer to change EKS to ECS Fargate for compute and ElastiCache for Redis for session.

upvoted 2 times

✉️  **gd1** 3 months ago

Gpt 4.0 - Answer is D

upvoted 1 times

✉️  **easytoo** 3 months ago

C-C-C-C-C

upvoted 1 times

✉️  **easytoo** 3 months ago

prefer d-d-d-d-d-d-d-d

upvoted 1 times

✉️  **SmileyCloud** 3 months ago

Selected Answer: B

A comes with the least operational overhead, but storing session data in SQS is wrong.

Session data can either be stored in ElastiCache or DynamoDB, so it's either B or D.

I am going with B because ECS on EC2 is probably less demanding in terms of operations than EKS.

upvoted 1 times

✉️  **SmileyCloud** 3 months ago

Actually, it's D. Multi-Attach is the same AZ as someone pointed out.

upvoted 3 times

✉️  **jubileu84** 3 months ago

D is the best. Multi-attach is a single az feature

upvoted 1 times

✉️  **nexus2020** 3 months ago

Selected Answer: A

Question is badly formated, I agree on that. But the question is asking: which one has the LEAST ongoing operational overhead.

in general, EC2 has more operational task, and EKS has even more than Fargate.

so A is the LEAST ongoing operational overhead?

upvoted 1 times

✉️  **MoussaNoussa** 3 months ago

the best answer is D. but using EKS here is a bad choice

upvoted 2 times

✉️  **bhanus** 3 months ago

what a worst ques

- A - Why do you need SQS to store web sever session data. SQS is for decoupling services
- B - EBS multi attach is for SAME availability zone. The ques says multipel availability zones
- C - Why do you need EFS to store web sever session data. Its damn expensive
- D - Better answer- But again why need for EKS.

If I were to choose one option, its D as its better compared to ABC

upvoted 4 times

Question #229

Topic 1

A solutions architect is planning to migrate critical Microsoft SQL Server databases to AWS. Because the databases are legacy systems, the solutions architect will move the databases to a modern data architecture. The solutions architect must migrate the databases with near-zero downtime.

Which solution will meet these requirements?

- A. Use AWS Application Migration Service and the AWS Schema Conversion Tool (AWS SCT). Perform an in-place upgrade before the migration. Export the migrated data to Amazon Aurora Serverless after cutover. Repoint the applications to Amazon Aurora.
- B. Use AWS Database Migration Service (AWS DMS) to rehost the database. Set Amazon S3 as a target. Set up change data capture (CDC) replication. When the source and destination are fully synchronized, load the data from Amazon S3 into an Amazon RDS for Microsoft SQL Server DB instance.
- C. Use native database high availability tools. Connect the source system to an Amazon RDS for Microsoft SQL Server DB instance. Configure replication accordingly. When data replication is finished, transition the workload to an Amazon RDS for Microsoft SQL Server DB instance.
- D. Use AWS Application Migration Service. Rehost the database server on Amazon EC2. When data replication is finished, detach the database and move the database to an Amazon RDS for Microsoft SQL Server DB instance. Reattach the database and then cut over all networking.

 **SmileyCloud** Highly Voted  3 months ago

Selected Answer: C

C. The proper way is to use AWS DMS, but the answer here uses S3 (???) which will take forever. So the answer is C.
upvoted 7 times

 **duriselvan** Most Recent  3 days ago

In this post, we showed you how to configure transactional replication with native backup and restore that replicates data from an on-premises SQL Server or SQL Server on an EC2 instance. You can use this strategy to migrate your large mission-critical workloads to an RDS for SQL Server instance with minimal to near-zero downtime.

C ans

upvoted 1 times

 **Ganshank** 1 month ago

C

<https://aws.amazon.com/blogs/database/part-3-migrating-to-amazon-rds-for-sql-server-using-transactional-replication-with-native-backup-and-restore/>

upvoted 3 times

 **billtran** 1 month ago

Selected Answer: B

Only B can do it.

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PostgreSQL.S3Import.html

upvoted 2 times

 **longngo0924** 1 month, 1 week ago

Selected Answer: B

Correct answer is B.

<https://repost.aws/questions/QUw-bHxHYITuC3lqDwgxyx6fw/is-it-possible-to-use-aws-rds-sql-server-as-an-aag-target-from-on-premise-primary>

upvoted 1 times

 **rxhan** 1 month, 4 weeks ago

RDS SQL Server is a managed service, so it will not be possible to add RDS Instance as an extension node to your on-premise primary instance. However, you can connect directly from your on-premise App to hosted RDS SQL Server instance in AWS. Alternatively, if you need RDS as a DR node for your on-premises primary, you can use an option like DMS (Database Migration Service) to set up on-going replication to RDS.

upvoted 1 times

 **PhilTheAnimal** 1 month, 2 weeks ago

So what is your answer then ?

upvoted 1 times

 **Arnaud92** 2 months ago

Selected Answer: B

Correct B

Always On Availability Groups (AG) cannot be used between an on-premise SQL Server database and Amazon RDS for SQL Server on AWS. Always On Availability Groups is a feature specific to SQL Server Enterprise Edition and requires Windows Failover Clustering-based network connectivity.

Amazon RDS for SQL Server supports both Standard and Enterprise editions of SQL Server, but it does not support the cluster failover features required for Always On Availability Groups.

So only DMS is the correct answer

upvoted 3 times

 **ggrodsckiy** 2 months ago

Correct B.

upvoted 1 times

 **Bengi** 2 months, 1 week ago

B - Refer to

<https://docs.aws.amazon.com/dms/latest/sbs/chap-manageddatabases.sqlserveralwayson.html>

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C for no downtime

upvoted 1 times

 **Jackhemo** 3 months ago

Olabiba says "C"...so it is C.

upvoted 1 times

 **gd1** 3 months ago

GPT 4.0 is B

upvoted 1 times

 **easystoo** 3 months ago

C-C-C-C-C

Microsoft SQL Server provides native high availability tools such as Always On Availability Groups or database mirroring. These tools enable real-time data replication and failover capabilities, allowing for minimal downtime during the migration process.

upvoted 2 times

 **nexus2020** 3 months ago

Selected Answer: C

Native Database High Availability Tools: AWS provides native high availability tools for Microsoft SQL Server, such as database mirroring, Always On Availability Groups, and transactional replication. These tools are designed to minimize downtime during the migration process and ensure data consistency and integrity.

upvoted 4 times

Question #230

Topic 1

A company's solutions architect is analyzing costs of a multi-application environment. The environment is deployed across multiple Availability Zones in a single AWS Region. After a recent acquisition, the company manages two organizations in AWS Organizations. The company has created multiple service provider applications as AWS PrivateLink-powered VPC endpoint services in one organization. The company has created multiple service consumer applications in the other organization.

Data transfer charges are much higher than the company expected, and the solutions architect needs to reduce the costs. The solutions architect must recommend guidelines for developers to follow when they deploy services. These guidelines must minimize data transfer charges for the whole environment.

Which guidelines meet these requirements? (Choose two.)

- A. Use AWS Resource Access Manager to share the subnets that host the service provider applications with other accounts in the organization.
- B. Place the service provider applications and the service consumer applications in AWS accounts in the same organization.
- C. Turn off cross-zone load balancing for the Network Load Balancer in all service provider application deployments.
- D. Ensure that service consumer compute resources use the Availability Zone-specific endpoint service by using the endpoint's local DNS name.
- E. Create a Savings Plan that provides adequate coverage for the organization's planned inter-Availability Zone data transfer usage.

 **elmoh** 2 weeks, 4 days ago

i beleieve C is wrong

Cross-zone load balancing

By default, each load balancer node distributes traffic across the registered targets in its Availability Zone only. If you turn on cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones.

upvoted 1 times

 **xav1er** 2 weeks, 4 days ago

Selected Answer: CD

- **C. Turn off cross-zone load balancing for the Network Load Balancer in all service provider application deployments.**
- **D. Ensure that service consumer compute resources use the Availability Zone-specific endpoint service by using the endpoint's local DNS name.**

upvoted 1 times

 **hglopes** 1 month ago

Isn't C and D achieving the same outcome?

- In C Provider Account turns off cross zone load balancing to ensure traffic stays in requested AZ
 - In D, Consumer Account is using specific provider AZ endpoints to ensure traffic stays in requested AZ
- If this is the case, C seems a lower maintenance solution?

upvoted 1 times

 **aviathor** 1 month ago

Selected Answer: BD

- B: allows data transfer between linked accounts to be free of charge;
- D: reduces data transfer charges across AZs

upvoted 2 times

 **SK_Tyagi** 1 month ago

Selected Answer: BD

That just feels right

upvoted 2 times

 **chikorita** 1 month, 1 week ago

wow! the comment section is divided

here's my honest take:

it definitely not A and D. why?

A: can't share resources using RAM across AWS Org

E: ain't no way Savings Plan helps with "data transfer charges"

I am left w BCD

B: allows data transfer between linked accounts to be free of charge; rightly mentioned by @easytoo

C: disabling "cross-zone load balancing" would saves money real quick

D: reduces data transfer charges across AZs

now, D is for sure the correct answer!!!
i am confused between B and C

tho a good Solution Architect should not compromise on High Availability which arises if we opt for C!!!
So, i choose BA :)
upvoted 1 times

 **chikorita** 1 week, 6 days ago

okay guys!!!
I tested this and can confirm that using you can share RAM resources across "External AWS IDs"
Please refer --> <https://medium.com/@vanchi811/how-to-share-resources-with-multiple-accounts-using-aws-resource-access-manager-ram-b131d76b2641>
so changing my answer to AD (which is also most voted option presently) ;)
upvoted 1 times

 **chikorita** 1 month, 1 week ago

typo up there :(
i choose ****BD***
upvoted 1 times

 **magmichal05** 1 month, 1 week ago

Selected Answer: BD

B. Place the service provider applications and the service consumer applications in AWS accounts in the same organization. This helps avoid or minimize data transfer charges when communicating between accounts within the same AWS Organization.

D. Ensure that service consumer compute resources use the Availability Zone-specific endpoint service by using the endpoint's local DNS name. This helps keep data transfer within the same Availability Zone, reducing data transfer charges.

upvoted 2 times

 **kjcncjek** 2 weeks, 4 days ago

can you provide a link to prove that B is true?
B. Place the service provider applications and the service consumer applications in AWS accounts in the same organization. This helps avoid or minimize data transfer charges when communicating between accounts within the same AWS Organization.
upvoted 2 times

 **MRL110** 1 month, 4 weeks ago

Selected Answer: CD

Subnets can't be shared across organizations:

<https://aws.amazon.com/blogs/networking-and-content-delivery/vpc-sharing-a-new-approach-to-multiple-accounts-and-vpc-management/#:~:text=In%20AWS%20RAM%2C%20we%20can,within%20the%20same%20AWS%20Organization>.

upvoted 2 times

 **ggrodsckiy** 2 months ago

Correct BD.

upvoted 1 times

 **Just_Ninja** 2 months ago

Selected Answer: BD

Why i choose B and D?

B: If you use Organisations and you create accounts, then the AZ-1a is the same Physical ID like it in the Child Account!
Otherwise it's possible that my AZ-1a and your AZ-1a in the same Region can have different Availability Zone ID's for example euc1-az2 or euc1-az1.
(If you are not sure about it, check your VPC Subnets there you can find it.)

D: Ensure that service consumer compute resources use the Availability Zone-specific endpoint service by using the endpoint's local DNS name.
Explanation: By using the endpoint's local DNS name, the service consumer's requests will be directed to the VPC endpoint within the same Availability Zone, reducing the data transfer across Availability Zones. This can help minimize the data transfer charges associated with using resources across different Availability Zones.

upvoted 1 times

 **study_aws1** 2 months, 1 week ago

A & B can form a combination here, not A & D (subnets cannot be shared only within a organization). But the question here is asking for Data Transfer costs reduction, not whole scale changes in Organization approach.
With this, C) & D) forms the right combination for the question.

upvoted 1 times

 **study_aws1** 2 months ago

Small typo....(subnets can be shared only within a organization). Rest all remains same.

upvoted 1 times

 **kiss22** 2 months, 1 week ago

The answer is C and D, it can't be A because there are two AWS Organizations involved.
upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: CD

cross-zone traffic is where money going

upvoted 2 times

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

Selected Answer: AD

A By sharing the subnets that host the service provider applications using AWS Resource Access Manager (RAM), the service consumer applications can be deployed in the same organization's accounts. This allows the traffic between the service consumer and service provider applications to stay within the organization's network, reducing data transfer charges.

D By using the Availability Zone-specific endpoint service's local DNS name, the service consumer compute resources can directly access the service provider applications within the same Availability Zone. This eliminates the need for cross-Availability Zone data transfer, thus reducing data transfer charges.

upvoted 4 times

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

Selected Answer: AD

A By sharing the subnets that host the service provider applications using AWS Resource Access Manager (RAM), the service consumer applications can be deployed in the same organization's accounts. This allows the traffic between the service consumer and service provider applications to stay within the organization's network, reducing data transfer charges.

D By using the Availability Zone-specific endpoint service's local DNS name, the service consumer compute resources can directly access the service provider applications within the same Availability Zone. This eliminates the need for cross-Availability Zone data transfer, thus reducing data transfer charges.

upvoted 3 times

✉️ **pupsik** 3 months ago

Selected Answer: AD

Explanation by @easytoo is spot on.

upvoted 1 times

✉️ **easytoo** 1 month, 3 weeks ago

Changed to B-D now pupsik.

Please see amendment to my previous answer.

upvoted 1 times

✉️ **PhuocT** 3 months ago

Selected Answer: BD

B and D seem reasonable choices

upvoted 2 times

Question #231

Topic 1

A company has an on-premises Microsoft SQL Server database that writes a nightly 200 GB export to a local drive. The company wants to move the backups to more robust cloud storage on Amazon S3. The company has set up a 10 Gbps AWS Direct Connect connection between the on-premises data center and AWS.

Which solution meets these requirements MOST cost-effectively?

- A. Create a new S3 bucket. Deploy an AWS Storage Gateway file gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share.
- B. Create an Amazon FSx for Windows File Server Single-AZ file system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system. Enable nightly backups.
- C. Create an Amazon FSx for Windows File Server Multi-AZ file system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system. Enable nightly backups.
- D. Create a new S3 bucket. Deploy an AWS Storage Gateway volume gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share on the volume gateway, and automate copies of this data to an S3 bucket.

 **SkyZeroZx** Highly Voted  2 months, 3 weeks ago

Selected Answer: A

File Gateway == SMB , NFS
 Volumes Gateway == iSCSI
 Tape Gateway = VTL
 upvoted 8 times

 **SK_Tyagi** Most Recent  1 month ago

Selected Answer: A

<https://aws.amazon.com/storagegateway/features/>
 upvoted 1 times

 **rafael796** 1 month, 3 weeks ago

Selected Answer: A

file gateway = most cheap
 upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

A - SMB mount = file gwy
 upvoted 1 times

 **RockyLeon** 3 months ago

Selected Answer: A

file gateway -> used to store file inside s3
 volume gateway -> used to store file in on-premises using iSCSI connectivity
 upvoted 2 times

 **Jackhemo** 3 months ago

Using Olabiba.ai to learn not to find an answer:

Jack: Labiba, what is the Microsoft SQL Server database export is it block or file?

oLabiba: The Microsoft SQL Server database export is typically a block-level backup. It captures the data at the database level, including the schema, tables, and records, and stores it in a binary format. This allows for efficient backup and restoration of the database.

In summary, if you primarily need file-level access to your backups, File Gateway is a better choice. If you require block-level storage and want to optimize for low-latency access, Volume Gateway is a better fit.

Let me know if you know the answer now.

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: A

File Gateway could be mapped as SMB file share and used by the database or other automation to transfer database backups. Volume Gateway is more used to perform volume snapshots on the on-premise system so I don't believe it's a sustainable approach here.

upvoted 3 times

 **SmileyCloud** 3 months ago

Selected Answer: A

It's A (file gateway). Volume gateway is iSCSI.

upvoted 2 times

 **Jackhemo** 3 months ago

Selected Answer: D

olabiba.ai says D

Option D: Using an AWS Storage Gateway volume gateway allows you to write the nightly database exports to an SMB file share on the volume gateway, which can be stored locally and automatically backed up to an S3 bucket. This solution is cost-effective as it utilizes the existing Direct Connect connection and requires minimal additional infrastructure.

upvoted 2 times

 **easystoo** 3 months ago

d-d-d-d-d-d

By deploying an AWS Storage Gateway volume gateway within the VPC connected to the Direct Connect connection, the company can leverage the high-speed, low-latency connection to transfer the nightly database exports to the SMB file share on the volume gateway. This allows for efficient and reliable data transfer.

Automating copies of this data from the SMB file share to an S3 bucket provides a cost-effective solution for storing the backups in more robust cloud storage on Amazon S3. The company can take advantage of the durability, scalability, and cost-effectiveness of S3 for long-term storage.

upvoted 2 times

 **nexus2020** 3 months ago

Selected Answer: A

Between A and D:

write to local drive can also be a network drive mapped to the windows server. therefore SME file share is enough (A), D is Block level, for sure will cost more.

the File Gateway is designed for file-level access and presents Amazon S3 storage as a file share, while the Volume Gateway provides block-level access and appears as local block storage volumes. The choice between the two depends on the specific needs and requirements of your applications and data access patterns.

upvoted 2 times

 **bhanus** 3 months ago

I am between A and D. ChatGpt says A. But The reason why I think D is because, the question says backups are written to local drive(which means its a volume on onpremises machine). So I thought a volume can be attached to volume gateway. But ChatGPT says In terms of cost-effectiveness and simplicity, option A is a better choice. It involves using an AWS Storage Gateway file gateway, which directly stores the data as objects in Amazon S3 without the need for on-premises storage. This eliminates the complexity and costs associated with maintaining an on-premises volume gateway.

upvoted 1 times

 **bhanus** 2 months, 4 weeks ago

I might be wrong with my theory. Going with A

upvoted 1 times

 **Jackhemo** 3 months ago

Use olabiba.ai. It is better.

upvoted 1 times

 **PhuocT** 3 months ago

Q: are you using openAI as your AI engine?

olabiba.com: Yes, I am powered by OpenAI's advanced AI technology. It allows me to understand and respond to your messages in a conversational manner. OpenAI provides the foundation for my capabilities, but the Olabiba team has also customized and trained me to better suit your needs. So, feel free to ask me anything or share your thoughts!

upvoted 1 times

 **gd1** 3 months ago

Volume will iSCSI so hat is out. Therefor A is correct

upvoted 1 times

Question #232

Topic 1

A company needs to establish a connection from its on-premises data center to AWS. The company needs to connect all of its VPCs that are located in different AWS Regions with transitive routing capabilities between VPC networks. The company also must reduce network outbound traffic costs, increase bandwidth throughput, and provide a consistent network experience for end users.

Which solution will meet these requirements?

- A. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VPC. Create VPC peering connections that initiate from the central VPC to all other VPCs.
- B. Create an AWS Direct Connect connection between the on-premises data center and AWS. Provision a transit VIF, and connect it to a Direct Connect gateway. Connect the Direct Connect gateway to all the other VPCs by using a transit gateway in each Region.
- C. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VPC. Use a transit gateway with dynamic routing. Connect the transit gateway to all other VPCs.
- D. Create an AWS Direct Connect connection between the on-premises data center and AWS. Establish an AWS Site-to-Site VPN connection between all VPCs in each Region. Create VPC peering connections that initiate from the central VPC to all other VPCs.

Gabehcoud 1 month, 1 week ago

what if the situation is 1 AWS account, different VPC's across different regions? Can we still use a TGW?

upvoted 1 times

hexie 2 months, 3 weeks ago

Selected Answer: B

B.

Cant be D because TGW doesnt support transitive connections, so if users connect to a VPN it invalidate this options.
A and C are skippable on the first phrase.

upvoted 1 times

NikkyDicky 2 months, 3 weeks ago

Selected Answer: B

B no doubt

upvoted 1 times

SkyZeroZx 3 months ago

Selected Answer: B

direct connect + vpc = direct connect gw + TGW. so B

upvoted 3 times

rxhan 1 month, 4 weeks ago

Mr. copy and paste

upvoted 3 times

Maria2023 3 months ago

Selected Answer: B

Transit gateway is a regional service but you can peer different TGs in different regions

<https://aws.amazon.com/about-aws/whats-new/2019/12/aws-transit-gateway-supports-inter-region-peering/>

upvoted 1 times

SmileyCloud 3 months ago

Selected Answer: B

B. No need for D and S2S VPN.

upvoted 1 times

aragon_saa 3 months ago

BBBBBBBBBBB?

upvoted 1 times

nexus2020 3 months ago

Selected Answer: B

direct connect + vpc = direct connect gw + TGW. so B

upvoted 3 times

Question #233

Topic 1

A company is migrating its development and production workloads to a new organization in AWS Organizations. The company has created a separate member account for development and a separate member account for production. Consolidated billing is linked to the management account. In the management account, a solutions architect needs to create an IAM user that can stop or terminate resources in both member accounts.

Which solution will meet this requirement?

- A. Create an IAM user and a cross-account role in the management account. Configure the cross-account role with least privilege access to the member accounts.
- B. Create an IAM user in each member account. In the management account, create a cross-account role that has least privilege access. Grant the IAM users access to the cross-account role by using a trust policy.
- C. Create an IAM user in the management account. In the member accounts, create an IAM group that has least privilege access. Add the IAM user from the management account to each IAM group in the member accounts.
- D. Create an IAM user in the management account. In the member accounts, create cross-account roles that have least privilege access. Grant the IAM user access to the roles by using a trust policy.

 **skyhiker** 1 month ago

Hmm, seems like alot of work. What if the question was, In the management account, a solutions architect needs to create an IAM user that can stop or terminate resources in 100 organization or member accounts? Asked AI "Using AWS Organizations, can you create both IAM user and permission sets in the management account for accessing managed organization resources?" The answer was Yes.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

its a D

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: D

One user is sufficient and you need cross-account role.

upvoted 1 times

 **MoussaNoussa** 3 months ago

D - Cross account role should be created in destination(member) account. The role has trust entity to master account.

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: D

D - Cross account role should be created in destination(member) account. The role has trust entity to master account.

upvoted 2 times

 **bhanus** 3 months ago

Selected Answer: D

D - Cross account role should be created in destination account(which is member account) and trust policy should be there

upvoted 2 times

Question #234

Topic 1

A company wants to use AWS for disaster recovery for an on-premises application. The company has hundreds of Windows-based servers that run the application. All the servers mount a common share.

The company has an RTO of 15 minutes and an RPO of 5 minutes. The solution must support native failover and fallback capabilities.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an AWS Storage Gateway File Gateway. Schedule daily Windows server backups. Save the data to Amazon S3. During a disaster, recover the on-premises servers from the backup. During failback, run the on-premises servers on Amazon EC2 instances.
- B. Create a set of AWS CloudFormation templates to create infrastructure. Replicate all data to Amazon Elastic File System (Amazon EFS) by using AWS DataSync. During a disaster, use AWS CodePipeline to deploy the templates to restore the on-premises servers. Fail back the data by using DataSync.
- C. Create an AWS Cloud Development Kit (AWS CDK) pipeline to stand up a multi-site active-active environment on AWS. Replicate data into Amazon S3 by using the s3 sync command. During a disaster, swap DNS endpoints to point to AWS. Fail back the data by using the s3 sync command.
- D. Use AWS Elastic Disaster Recovery to replicate the on-premises servers. Replicate data to an Amazon FSx for Windows File Server file system by using AWS DataSync. Mount the file system to AWS servers. During a disaster, fail over the on-premises servers to AWS. Fail back to new or existing servers by using Elastic Disaster Recovery.

 **SK_Tyagi** 1 month ago

Selected Answer: D

FSX for Windows and Elastic Disaster Recovery

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

its a D

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: D

You need FSx, not EFS and def not S3.

upvoted 1 times

 **PhuocT** 3 months ago

Selected Answer: D

D is the answer

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: D

D for sure

B is wrong because you cannot use EFS for Windows EC2 Servers

upvoted 1 times

 **MoussaNoussa** 3 months ago

D is the right answer

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: D

Considering RTO and RPO, D is correct answer

A is incorrect because, thought backups are in s3, its not possible to recover ec2 within 15-minute RTO and a 5-minute RPO

upvoted 3 times

Question #235

Topic 1

A company has built a high performance computing (HPC) cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations.

Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Choose three.)

- A. Ensure the HPC cluster is launched within a single Availability Zone.
- B. Launch the EC2 instances and attach elastic network interfaces in multiples of four.
- C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.
- D. Ensure the cluster is launched across multiple Availability Zones.
- E. Replace Amazon EFS with multiple Amazon EBS volumes in a RAID array.
- F. Replace Amazon EFS with Amazon FSx for Lustre.

 **aviathor** 1 month ago

Selected Answer: ACF

- A. Ensure the HPC cluster is launched within a single Availability Zone: This choice ensures that the EC2 instances in the cluster have low network latency and high bandwidth, as they are located within the same data center.
- C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled: EFA is a network interface that provides low-latency, high-bandwidth communication between EC2 instances. By selecting instance types with EFA enabled, the cluster can benefit from improved inter-instance communication.
- F. Replace Amazon EFS with Amazon FSx for Lustre: Amazon FSx for Lustre is a high-performance file system optimized for HPC workloads. By using FSx for Lustre instead of Amazon EFS, the cluster can achieve better performance for the large number of shared files generated by the workload.

And what about a cluster placement group?

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: ACF

ACF for performance
upvoted 1 times

 **bhanus** 2 months, 4 weeks ago

Selected Answer: ACF

@MODERATOR - Please remove my previous comment. I agree with ACF. Thank you MoussaNoussa for clarifying
upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: ACF

ACF is the correct answer
upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: ACF

A, C and F
upvoted 1 times

 **SkyZeroZx** 3 months ago

- B) Not is correct because ENI not more performance in this case with HPC Cluster
 - D) sounds good but not is good option because performance is required in same AZ is the cluster placement group strategy more adequate
 - E) replace EFS by EBS not is appropriate for performance
- upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: ACF

A - Single AZ is better than multi AZ for performance
C - Use EFA. <https://aws.amazon.com/hpc/efa/> - It tells you that's HPC is a use case.
F - Use FSx for Lustre - <https://aws.amazon.com/fsx/lustre/>. HPC is a use case.
upvoted 1 times

 **PhuocT** 3 months ago

Selected Answer: ACF

A, C and F

upvoted 1 times

 ozelli 3 months ago

Selected Answer: ACF

ACF is the correct answer

upvoted 1 times

 easytoo 3 months ago

a-c-f...a-c-f...a-c-f

To achieve maximum performance from the HPC cluster, the following design choices should be made:

A. Ensure the HPC cluster is launched within a single Availability Zone: This choice ensures that the EC2 instances in the cluster have low network latency and high bandwidth, as they are located within the same data center.

C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled: EFA is a network interface that provides low-latency, high-bandwidth communication between EC2 instances. By selecting instance types with EFA enabled, the cluster can benefit from improved inter-instance communication.

F. Replace Amazon EFS with Amazon FSx for Lustre: Amazon FSx for Lustre is a high-performance file system optimized for HPC workloads. By using FSx for Lustre instead of Amazon EFS, the cluster can achieve better performance for the large number of shared files generated by the workload.

upvoted 1 times

 nexus2020 3 months ago

Selected Answer: CDF

B: more interface does not mean faster. so B is not a good choice.

E: RAID? is often not recommended on Cloud Platform, aws has already raid the drive for you underlay.

A: HPC recommended to use multiregion.

so CDF

upvoted 1 times

 MoussaNoussa 3 months ago

ACF is the right answer

upvoted 2 times

 bhanus 3 months ago

Selected Answer: CDF

CDF are correct

C - EFA provides low-latency and high-bandwidth communication between EC2 instances. It can optimize the network performance of the HPC cluster.

D - Launching the HPC cluster across multiple Availability Zones allows you to distribute the workload and resources, reducing the chances of a single point of failure and increasing overall performance.

F - FSx for Lustre is a high-performance file system optimized for HPC workloads.

upvoted 1 times

 bhanus 2 months, 4 weeks ago

changing my vote to ACF as per below suggestion

upvoted 1 times

 MoussaNoussa 3 months ago

performance is the main goal. so running HPC in the same AZ is the right choice here

upvoted 4 times

 bhanus 3 months ago

Thank you @ MoussaNoussa for clarifying. Agreed.

upvoted 1 times

Question #236

Topic 1

A company is designing an AWS Organizations structure. The company wants to standardize a process to apply tags across the entire organization. The company will require tags with specific values when a user creates a new resource. Each of the company's OUs will have unique tag values.

Which solution will meet these requirements?

- A. Use an SCP to deny the creation of resources that do not have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the OUs.
- B. Use an SCP to deny the creation of resources that do not have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the organization's management account.
- C. Use an SCP to allow the creation of resources only when the resources have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the OUs.
- D. Use an SCP to deny the creation of resources that do not have the required tags. Define the list of tags. Attach the SCP to the OUs.

 **nicecurls** 2 months, 2 weeks ago

Selected Answer: A

FOR EACH OU's

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

it's an A

upvoted 1 times

 **dkx** 2 months, 3 weeks ago

The correct answer is B.

Imagine if you had an AWS Organization with 50+ OUs, it would be very inefficient to manually apply a generic tagging policy to each OU, so that's why there is the concept of policy inheritance: when you attach a policy to the organization root, all OUs and accounts in the organization inherit that policy

When you attach a tag policy to your organization root, the tag policy applies to all of that root's member OUs and accounts.
<https://docs.aws.amazon.com/organizations/latest/userguide/attach-tag-policy.html>

Understanding policy inheritance: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_inheritance.html
 upvoted 1 times

 **santi1975** 2 months ago

The question clearly says "Each of the company's OUs will have unique tag values", you cannot inherit what is different. The answer is B
 upvoted 1 times

 **santi1975** 2 months ago

Sorry, I mean cannot be B, and the correct answer is A!

upvoted 1 times

 **Piccaso** 2 months, 3 weeks ago

Selected Answer: A

C and D must be wrong, because of "allow ... "

B is weird.

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: A

Each of the company's OUs will have unique tag values.

Then A because each OU unique tags A is the unique with approved this case

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: A

You go to the management account -> Organizations console -> Policies -> Tag policies -> "name of the policy" -> attach to OU. That's it - A is correct

upvoted 4 times

 **SmileyCloud** 3 months ago

Selected Answer: A

It's A. The policies are different for each account, so you can't assign it to the management account. Exact same scenario:
<https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>
upvoted 1 times

✉ **bhanus** 3 months ago

Selected Answer: A

MODERATOR - Please remove my previous comment. From the discussion it looks like A is the answer. Looks like the tag policies should be attached at the OU level to ensure that each OU has its own unique tag values.

upvoted 1 times

✉ **PhuocT** 3 months ago

I think it's A

upvoted 2 times

✉ **gd1** 3 months ago

GPT 4. 0 says A - I agree. Values per OU

upvoted 1 times

✉ **easytoo** 3 months ago

b-b-b-b-b-b

upvoted 1 times

✉ **MoussaNoussa** 3 months ago

option A is the right answer, we need a have a list of allowed tag values per OU

upvoted 1 times

✉ **bhanus** 3 months ago

Selected Answer: B

B - you don't have apply SCPs to each account or OU. Attaching the tag policies to the organization's management account ensures that the policies are applied consistently to all OUs within the organization.

C is incorrect because SCP are NOT used for ALLOW action. They are used for DENY actions (setting boundaries)

upvoted 3 times

✉ **bhanus** 2 months, 4 weeks ago

changing my vote to A. The policies are different for each account, so you can't assign it to the management account.

upvoted 1 times

Question #237

Topic 1

A company has more than 10,000 sensors that send data to an on-premises Apache Kafka server by using the Message Queuing Telemetry Transport (MQTT) protocol. The on-premises Kafka server transforms the data and then stores the results as objects in an Amazon S3 bucket.

Recently, the Kafka server crashed. The company lost sensor data while the server was being restored. A solutions architect must create a new design on AWS that is highly available and scalable to prevent a similar occurrence.

Which solution will meet these requirements?

- A. Launch two Amazon EC2 instances to host the Kafka server in an active/standby configuration across two Availability Zones. Create a domain name in Amazon Route 53. Create a Route 53 failover policy. Route the sensors to send the data to the domain name.
- B. Migrate the on-premises Kafka server to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create a Network Load Balancer (NLB) that points to the Amazon MSK broker. Enable NLB health checks. Route the sensors to send the data to the NLB.
- C. Deploy AWS IoT Core, and connect it to an Amazon Kinesis Data Firehose delivery stream. Use an AWS Lambda function to handle data transformation. Route the sensors to send the data to AWS IoT Core.
- D. Deploy AWS IoT Core, and launch an Amazon EC2 instance to host the Kafka server. Configure AWS IoT Core to send the data to the EC2 instance. Route the sensors to send the data to AWS IoT Core.

 **duriselvan** 22 hours, 5 minutes ago

C :Anshttps://docs.aws.amazon.com/lambda/latest/dg/services-kinesisfirehose.html

upvoted 1 times

 **SK_Tyagi** 1 month ago

Selected Answer: C

Option B is missing the Data Transformation to be done by Lambda

upvoted 2 times

 **softarts** 1 month, 1 week ago

Selected Answer: C

C, because it said new design and obviously IoT is what aws recommend.

upvoted 3 times

 **chico2023** 1 month, 2 weeks ago

Selected Answer: C

Answer: C

To me C is still the best option as it is not wrong and there is an uncertainty regarding NLB support for MQTT protocol. You can, yes, however, not out of the box, you would need solutions like HiveMQ, for example: <https://github.com/mqtt/mqtt.org/wiki/Server%20support>

Now, when I read this part of the question "Recently, the Kafka server crashed. The company lost sensor data while the server was being restored", to me it seems that it would be OK for the company to look for different ways in having their data stored in S3, be it using a Kafka server or not.

Therefore and, just because the question doesn't say anything regarding cost effectiveness, least operational overhead, least dev overhead and so on, it's safe to assume (to me) that IoT Core would be the option AWS wants us to think about.

upvoted 1 times

 **andy7t** 2 months ago

Selected Answer: B

Both B and C will work?

NLB + MSK is a well defined pattern. MSK is highly available and scaleable. MQTT will pass through NLB as it's just a network port. No changes to the application.

C would also work, but seems to involve more refactoring.

upvoted 1 times

 **Just_Ninja** 2 months ago

Selected Answer: B

It's B,

because MSK can handle the lightweight MQTT protocol.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

its a C
mqtt->IoT core
upvoted 1 times

✉ **javitech83** 2 months, 4 weeks ago

Selected Answer: C

IoT perfect for MQTT. Option D could have the same problem as on-premises
upvoted 2 times

✉ **SmileyCloud** 3 months ago

Selected Answer: C

It's C. Anytime you see sensors, your best bet is IoT. It's not D because you'll have one Kafka EC2 instance and it's not HA.
upvoted 2 times

✉ **bhanus** 3 months ago

Selected Answer: C

MODERATOR - please remove my previous comment. Looks is C is correct answer
upvoted 1 times

✉ **SkyZeroZx** 3 months ago

Selected Answer: C

IOT core is designed to handle this. and NLB does not support MQTT.
upvoted 1 times

✉ **PhuocT** 3 months ago

Agree with C

upvoted 2 times

✉ **nexus2020** 3 months ago

Selected Answer: C

IOT core is designed to handle this. and NLB does not support MQTT.
upvoted 3 times

✉ **gd1** 3 months ago

Agree and IPT Core supports MQTT

upvoted 1 times

✉ **MoussaNoussa** 3 months ago

C is the correct Answer

upvoted 2 times

✉ **bhanus** 3 months ago

Selected Answer: B

<https://aws.amazon.com/blogs/big-data/secure-connectivity-patterns-to-access-amazon-msk-across-aws-regions/>
upvoted 1 times

✉ **Just_Ninja** 2 months ago

Don't switch to C, B is right. MSK can handle MQTT. No special IOT Service is needed.

upvoted 1 times

✉ **bhanus** 2 months, 4 weeks ago

changing my vote to C as per below suggestion

upvoted 1 times

✉ **MoussaNoussa** 3 months ago

This is incorrect, the solution needs to use IoT Core

upvoted 1 times

✉ **bhanus** 3 months ago

Thank you again MoussaNoussa. I might be wrong. I have read NLB supports MQTT and hence chose this answer. But I am also unsure
upvoted 1 times

Question #238

Topic 1

A company recently started hosting new application workloads in the AWS Cloud. The company is using Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) file systems, and Amazon RDS DB instances.

To meet regulatory and business requirements, the company must make the following changes for data backups:

- Backups must be retained based on custom daily, weekly, and monthly requirements.
- Backups must be replicated to at least one other AWS Region immediately after capture.
- The backup solution must provide a single source of backup status across the AWS environment.
- The backup solution must send immediate notifications upon failure of any resource backup.

Which combination of steps will meet these requirements with the LEAST amount of operational overhead? (Choose three.)

- A. Create an AWS Backup plan with a backup rule for each of the retention requirements.
- B. Configure an AWS Backup plan to copy backups to another Region.
- C. Create an AWS Lambda function to replicate backups to another Region and send notification if a failure occurs.
- D. Add an Amazon Simple Notification Service (Amazon SNS) topic to the backup plan to send a notification for finished jobs that have any status except BACKUP_JOB_COMPLETED.
- E. Create an Amazon Data Lifecycle Manager (Amazon DLM) snapshot lifecycle policy for each of the retention requirements.
- F. Set up RDS snapshots on each database.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: ABD

its ABD

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: ABD

ABD. You don't need Lambda for cross-region backup. You don't need RDS snaps.

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: ABD

ABD. You don't need Lambda for cross-region backup. You don't need RDS snaps.

upvoted 4 times

 **easystoo** 3 months ago

a-b-d...a-b-d

upvoted 1 times

 **MoussaNoussa** 3 months ago

ABD is the correct answer

upvoted 2 times

 **bhanus** 3 months ago

Selected Answer: ABD

ABD

E is incorrect because Amazon Data Lifecycle Manager is used to automate the creation, retention, and deletion of EBS snapshots and EBS-backed AMIs. It CANNOT be used for backups for EC2, EFS, RDS

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/snapshot-lifecycle.html>

upvoted 4 times

Question #239

Topic 1

A company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population. The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide information back to researchers. The data platform must meet the following requirements:

- Provide near-real-time analytics of the inbound genomic data
- Ensure the data is flexible, parallel, and durable
- Deliver results of processing to a data warehouse

Which strategy should a solutions architect use to meet these requirements?

- A. Use Amazon Kinesis Data Firehose to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon RDS instance.
- B. Use Amazon Kinesis Data Streams to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon Redshift cluster using Amazon EMR.
- C. Use Amazon S3 to collect the inbound device data, analyze the data from Amazon SQS with Kinesis, and save the results to an Amazon Redshift cluster.
- D. Use an Amazon API Gateway to put requests into an Amazon SQS queue, analyze the data with an AWS Lambda function, and save the results to an Amazon Redshift cluster using Amazon EMR.

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

Selected Answer: B

B for sure

upvoted 1 times

✉  **SmileyCloud** 3 months ago

Selected Answer: B

B. Real-time is either firehose (A) or streams (B). But they require a data warehouse and that's RedShift not RDS.

upvoted 2 times

✉  **easystoo** 3 months ago

b=b=b=b=b=b

upvoted 1 times

✉  **nexus2020** 3 months ago

Selected Answer: B

B is the one for real time

upvoted 1 times

✉  **MoussaNoussa** 3 months ago

Answer B is the right one

upvoted 2 times

✉  **bhanus** 3 months ago

Selected Answer: B

B is correct

B - Kinesis Data Streams is a real-time streaming service and provide near-real-time analytics. Also the question "Deliver results of processing to a data warehouse" and this option has redshift cluster which is a powerful data warehousing solution that can handle large-scale analytics workloads.

A - incorrect because Kinesis Data Firehose is NOT ideal for near-real-time analytics and may introduce some latency in the data processing pipeline. Additionally, saving the results to an Amazon RDS instance may not provide the scalability and flexibility required for processing and analyzing large volumes of genomic data.

upvoted 4 times

✉  **bhanus** 2 months, 4 weeks ago

Between A and B, B is better because questions asks for data warehousing capabilities. So option B has Redshift which is correct answer.

upvoted 1 times

✉  **bhanus** 3 months ago

What a worst framed ques. The ques says "NEAR real time" which means its Kinesis data firehose. But this option has RDS which is not good for analysis

upvoted 1 times

Question #240

Topic 1

A solutions architect needs to define a reference architecture for a solution for three-tier applications with web, application, and NoSQL data layers. The reference architecture must meet the following requirements:

- High availability within an AWS Region
- Able to fail over in 1 minute to another AWS Region for disaster recovery
- Provide the most efficient solution while minimizing the impact on the user experience

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

- A. Use an Amazon Route 53 weighted routing policy set to 100/0 across the two selected Regions. Set Time to Live (TTL) to 1 hour.
- B. Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live (TTL) to 30 seconds.
- C. Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.
- D. Back up data from an Amazon DynamoDB table in the primary Region every 60 minutes and then write the data to Amazon S3. Use S3 cross-Region replication to copy the data from the primary Region to the disaster recovery Region. Have a script import the data into DynamoDB in a disaster recovery scenario.
- E. Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources.
- F. Use Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use Spot Instances for the required resources.

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: BCE

BCE for sure

upvoted 2 times

 **Piccaso** 2 months, 3 weeks ago

Selected Answer: BCE

A and D must be wrong. They cannot meet the performance requirement.

F is not good. Spot Instances are not reliable.

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: BCE

BCE is correct

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: BCE

BCE is correct

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: ACE

A - Failover Rt 53

C - Global DynamoDB tables to take care of regional replication

E - Minimum EC2 across regions with reserved and on-demand

upvoted 1 times

 **SmileyCloud** 3 months ago

Sorry BCE.

upvoted 3 times

 **SkyZeroZx** 3 months ago

To meet the requirements of high availability within an AWS Region, failover to another AWS Region for disaster recovery, and provide an efficient solution while minimizing user impact, the following three steps should be taken:

Step B: Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live (TTL) to 30 seconds.

By using the failover routing policy in Amazon Route 53, you can configure DNS failover between the primary and disaster recovery Regions. This allows traffic to be redirected to the disaster recovery Region in the event of a failure in the primary Region.

upvoted 1 times

✉️ **SkyZeroZx** 3 months ago

Step C: Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.

Amazon DynamoDB global tables enable automatic multi-region replication, allowing the data to be accessed in both the primary and disaster recovery Regions. This ensures data availability and low-latency access to the data.

upvoted 1 times

✉️ **SkyZeroZx** 3 months ago

Step E: Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources.

By implementing a hot standby model with Auto Scaling groups across multiple Availability Zones in both the primary and disaster recovery Regions, you can ensure high availability within the Region. Using zonal Reserved Instances for the minimum number of servers helps optimize costs, while On-Demand Instances provide flexibility for additional resource provisioning.

upvoted 2 times

✉️ **SkyZeroZx** 3 months ago

Selected Answer: BCE

B, C and E

upvoted 1 times

✉️ **PhuocT** 3 months ago

B, C and E

upvoted 1 times

✉️ **nexus2020** 3 months ago

Selected Answer: BCE

BCE here as well

A: 1 hour is too long

D: just use global table....

F: hot spot?

upvoted 1 times

✉️ **MoussaNoussa** 3 months ago

BCE is the right answer

upvoted 2 times

Question #241

Topic 1

A company manufactures smart vehicles. The company uses a custom application to collect vehicle data. The vehicles use the MQTT protocol to connect to the application. The company processes the data in 5-minute intervals. The company then copies vehicle telematics data to on-premises storage. Custom applications analyze this data to detect anomalies.

The number of vehicles that send data grows constantly. Newer vehicles generate high volumes of data. The on-premises storage solution is not able to scale for peak traffic, which results in data loss. The company must modernize the solution and migrate the solution to AWS to resolve the scaling challenges.

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

- A. Use AWS IoT Greengrass to send the vehicle data to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create an Apache Kafka application to store the data in Amazon S3. Use a pretrained model in Amazon SageMaker to detect anomalies.
- B. Use AWS IoT Core to receive the vehicle data. Configure rules to route data to an Amazon Kinesis Data Firehose delivery stream that stores the data in Amazon S3. Create an Amazon Kinesis Data Analytics application that reads from the delivery stream to detect anomalies.
- C. Use AWS IoT FleetWise to collect the vehicle data. Send the data to an Amazon Kinesis data stream. Use an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use the built-in machine learning transforms in AWS Glue to detect anomalies.
- D. Use Amazon MQ for RabbitMQ to collect the vehicle data. Send the data to an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use Amazon Lookout for Metrics to detect anomalies.

 **SK_Tyagi** 1 month ago

Selected Answer: B

The confusion seem to be b/w IoTCore and FleetWise (B & C), however for anomaly detection one uses Kinesis Data Analytics(KDA) and other uses Glue ML algorithms. Least overhead is using Random Cut Forest in (KDA) as compared to Glue
upvoted 1 times

 **chico2023** 1 month, 2 weeks ago

Selected Answer: B

I agree with everyone. Even olabiba agrees. It's B.
upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

it's a B
C - there is no Fleetwise to Kinesis integration
upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

A - too complex
B - It's B. You se IoT Code, Kinesis Firehose and Kinesis Data Analytics for anomalies
<https://docs.aws.amazon.com/kinesisanalytics/latest/dev/app-anomaly-detection.html>
C - IoT FleetWise is a perfect use case but this solution does not detect anomalies. You need Lookout for this as described here.
<https://docs.aws.amazon.com/kinesisanalytics/latest/dev/app-anomaly-detection.html>
D - This is also possible, but the use case for RabbitMQ is different.
upvoted 2 times

 **easytoo** 3 months ago

C-C-C-C-C-C
upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

B for me opinion i need use Amazon Kinesis Data Analytics for detect anomalies
C sounds goood but i don't know how AWS Glue detect anomalies , usually use case is ETL
upvoted 1 times

 **Jackhemo** 3 months ago

Selected Answer: B

Olabiba says 'B'.
upvoted 1 times

 **gd1** 3 months ago

Selected Answer: B

AWS IoT Core provides a good way to handle data from IoT devices like these smart vehicles, especially as the MQTT protocol is used. Amazon Kinesis Data Firehose can capture, transform, and load streaming data into data lakes, data stores, and analytics services. It can handle large volumes of data from hundreds of thousands of sources, and it can scale automatically. Amazon Kinesis Data Analytics makes it easy to analyze streaming data in real-time with Java, SQL, or Apache Flink, without having to learn new programming languages or processing frameworks. It could be used to analyze the streaming data and detect anomalies

upvoted 3 times

 **Alabi** 3 months ago

Selected Answer: B

B. Use AWS IoT Core to receive the vehicle data. Configure rules to route data to an Amazon Kinesis Data Firehose delivery stream that stores the data in Amazon S3. Create an Amazon Kinesis Data Analytics application that reads from the delivery stream to detect anomalies.

Explanation:

This solution leverages AWS IoT Core, which is designed for handling IoT device communication and data ingestion. The vehicle data is received by AWS IoT Core and routed using rules to an Amazon Kinesis Data Firehose delivery stream. Kinesis Data Firehose can handle high volumes of data and seamlessly store it in Amazon S3, ensuring scalability for peak traffic. To detect anomalies, an Amazon Kinesis Data Analytics application can be created to analyze the data from the delivery stream. This solution requires the least operational overhead as it leverages managed services and provides scalability and analytics capabilities for the growing volume of vehicle data.

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: C

AWS IoT FleetWise makes it easier for you to collect, transform, and transfer vehicle data to the cloud in near real time and use that data to improve...

upvoted 3 times

 **mashandpie** 1 month, 1 week ago

FleetWise only allows you to store data in TimeStream or S3 (more recently), hence the choice of IoT Core

upvoted 1 times

Question #242

Topic 1

During an audit, a security team discovered that a development team was putting IAM user secret access keys in their code and then committing it to an AWS CodeCommit repository. The security team wants to automatically find and remediate instances of this security vulnerability.

Which solution will ensure that the credentials are appropriately secured automatically?

- A. Run a script nightly using AWS Systems Manager Run Command to search for credentials on the development instances. If found, use AWS Secrets Manager to rotate the credentials
- B. Use a scheduled AWS Lambda function to download and scan the application code from CodeCommit. If credentials are found, generate new credentials and store them in AWS KMS.
- C. Configure Amazon Macie to scan for credentials in CodeCommit repositories. If credentials are found, trigger an AWS Lambda function to disable the credentials and notify the user.
- D. Configure a CodeCommit trigger to invoke an AWS Lambda function to scan new code submissions for credentials. If credentials are found, disable them in AWS IAM and notify the user.

 **SmileyCloud** Highly Voted  3 months ago

Selected Answer: D

A - AWS Secrets Manager can't rotate the credentials if they are part of the code
 B - You don't store creds in KMS, that's the job of Secrets Manager
 C - Macie can do S3 only. CodeCommit backend is also S3 but it's transparent for us, so you can't use Macie.
 D - Correct. See this use case <https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/>
 upvoted 5 times

 **ggrodskiy** Most Recent  2 months ago

Correct C.
 Macie can scan for credentials in CodeCommit repositories. According to the AWS documentation, Macie supports scanning for credentials in CodeCommit repositories and triggering actions based on the findings. You can use Macie to discover sensitive data such as AWS access keys, AWS secret access keys, private keys, and more in your CodeCommit repositories. You can also configure Macie to send notifications, invoke Lambda functions, or publish findings to AWS Security Hub when it detects sensitive data in CodeCommit repositories. For more information, see Data protection in AWS CodeCommit <https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html> and Amazon Macie | AWS Blog <https://aws.amazon.com/blogs/aws/category/amazon-macie/>. <https://docs.aws.amazon.com/codecommit/latest/userguide/data-protection.html> <https://aws.amazon.com/blogs/aws/category/amazon-macie/>

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

D - <https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/>
 upvoted 1 times

 **River007** 3 months ago

D can resolve the code that already commit to codecommit
 upvoted 1 times

 **RockyLeon** 2 months, 4 weeks ago

D says Codecommit trigger to scan new code submissions....
 how already commit code will scan ?
 upvoted 1 times

 **RockyLeon** 2 months, 4 weeks ago

whereas question did not ask for existing code
 upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: D

Macie sounds good but not is use case is only scans S3.
 Then D is more appropriate in this case , similar question in this exam practice on Tutoriales Dojo
 upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: D

Macie would be a great choice but at the moment it only scans S3. And even if CodeCommit ends in S3 (according to the AWS documentation) it is not visible for us and therefore I don't believe we can configure Macie to scan. At the moment Lambda remains the best choice
 upvoted 1 times

 **gd1** 3 months ago

Selected Answer: D

Need auto-disable and D does it
upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: D

D. Configure a CodeCommit trigger to invoke an AWS Lambda function to scan new code submissions for credentials. If credentials are found, disable them in AWS IAM and notify the user.

Explanation:

This solution leverages a CodeCommit trigger to automatically invoke an AWS Lambda function whenever new code is submitted to the repository. The Lambda function can scan the code for credentials and if found, take appropriate actions such as disabling those credentials in AWS IAM and notifying the user. This approach ensures that the security vulnerability is automatically identified and remediated as part of the development process, providing a proactive security measure.

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: D

I would go with D. reason is ABC are all post event action, meaning the credential are already leaked AFTER the code submition.

only D would prevent it from happeninng by doing a check BEFORE it get submitted.

upvoted 3 times

 **MoussaNoussa** 3 months ago

option D is the correct one of course

upvoted 3 times

 **bhanus** 3 months ago

Selected Answer: C

C - <https://docs.aws.amazon.com/macie/latest/user/managed-data-identifiers.html#managed-data-identifiers-credentials>

upvoted 2 times

 **bhanus** 2 months, 4 weeks ago

change it to D as it would prevent it from happeninng by doing a check BEFORE it get submitted.

upvoted 1 times

Question #243

Topic 1

A company has a data lake in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts. The company's information security policy states that the S3 bucket must not be accessed over the public internet and that each application should have the minimum permissions necessary to function.

To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs for each application.

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

- A. Create an S3 access point for each application in the AWS account that owns the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
- B. Create an interface endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Create a VPC gateway attachment for the S3 endpoint.
- C. Create a gateway endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Specify the route table that is used to access the access point.
- D. Create an S3 access point for each application in each AWS account and attach the access points to the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
- E. Create a gateway endpoint for Amazon S3 in the data lake's VPC. Attach an endpoint policy to allow access to the S3 bucket. Specify the route table that is used to access the bucket.

 **Gabehcoud** 3 weeks, 5 days ago

Selected Answer: BD

Gateway endpoint is public whereas S3 access point and Interface endpoint can be private and limited to VPC.
<https://aws.amazon.com/s3/features/access-points/>

upvoted 1 times

 **chikorita** 1 month ago

can anyone tell me why B is incorrect
 from what I know
 gateway endpoint resolves to Public AWS IP
 interface endpoint is completely private
 please correct me if wrong

upvoted 3 times

 **vn_thanh tung** 3 weeks, 4 days ago

Because To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs for each application => using access endpoint instead of interface endpoints

upvoted 1 times

 **chikorita** 2 weeks, 4 days ago

thanks, got it
 upvoted 1 times

 **vn_thanh tung** 3 weeks, 4 days ago

interface endpoint is completely private, you are wrong interface endpoint is public
 upvoted 1 times

 **softarts** 1 month, 2 weeks ago

Selected Answer: AE

Stephane sap-c02 practice test2-Q72.
 C is wrong. There is no need to create separate VPCs for each application, as just a single data lake VPC can house all applications, which allows you to configure a single S3 gateway endpoint having a policy with a condition to limit access via a common prefix for the access points of all the S3 buckets for the data lake. So this option is not the best fit.

upvoted 1 times

 **softarts** 1 month, 2 weeks ago

however I think E also has problem "route table that is used to access the bucket" should be access point
 upvoted 1 times

 **Arnaud92** 1 month, 3 weeks ago

Selected Answer: AC

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

You can access Amazon S3 from your VPC using gateway VPC endpoints. After you create the gateway endpoint, you can add it as a target in your route table for traffic destined from your VPC to Amazon S3.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: AC

AC - <https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: AC

A C is correct.

S3: gateway endpoint, policy-> allow access point DNS

access point: choose S3 vpc endpoint as origin

upvoted 1 times

 **SkyZeroZx** 2 months, 4 weeks ago

Selected Answer: AC

A) manage with granular permissions from the master account the connection to the bucket sounds like a good idea and according to what is required

B) interface endpoint , usually use case is for enable public connection , not is required is incorrect in this case

C) Gateway Endpoint, it is usually used for the internal AWS network which would be useful in this additional case that is configured for each account and client application which is granular, sounds like a good idea

D) use access point in the clients, but it does not make sense because the one who will grant the permissions has to be the owner of the bucket so we discard it

E) gateway endpoint , doesn't sound appropriate in the owner's bucket because you have to use granular permissions as directed with the access point

Then correct is AC

upvoted 3 times

 **Maria2023** 3 months ago

Selected Answer: DE

I vote D and E. D - because we need to create the endpoint in the account, which hosts the application and to limit it to VPC and E - since we need to create gateway endpoint in the data lake's account so the traffic does not traverse via the internet.

Below is the official documentation

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/creating-access-points.html>

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: AC

AC - Correct

upvoted 2 times

 **SmileyCloud** 2 months, 3 weeks ago

<https://repost.aws/knowledge-center/s3-access-bucket-restricted-to-vpc>

upvoted 1 times

 **easystoo** 3 months ago

a-c-a-c-a-c

upvoted 1 times

 **awscerts023** 3 months ago

Selected Answer: AC

Adding the weightage on right answer , AC according to <https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 1 times

 **PhuocT** 3 months ago

Selected Answer: AC

Agree with A and C

upvoted 1 times

 **ozelllll** 3 months ago

Selected Answer: AC

It's AC. <https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 3 times

 **gd1** 3 months ago

Selected Answer: AC

GPT : Step A enables each application to have its own access point, which can be configured to allow only the necessary permissions for that application. This satisfies the requirement for least privilege access.

Step C involves creating a gateway VPC endpoint for S3 in each application's VPC. This endpoint provides a private path for traffic between the VPC and the S3 bucket, ensuring that the data does not traverse the public internet. The endpoint policy should be configured to allow access to the specific S3 access point created for the application, maintaining the least privilege principle.

upvoted 2 times

✉ **Jackhemo** 3 months ago

Bud, GPT Regenerate and check again.
upvoted 1 times

✉ **Alabi** 3 months ago

Selected Answer: AB

Explanation:

Step A involves creating an S3 access point for each application in the AWS account that owns the S3 bucket. By configuring each access point to be accessible only from the application's VPC, access to the bucket is restricted to specific VPCs. Updating the bucket policy to require access from an access point ensures that applications can only access the bucket through the designated access point.

Step B is about creating an interface endpoint for Amazon S3 in each application's VPC. By configuring the endpoint policy to allow access to an S3 access point, the applications can communicate with the S3 bucket through the access point. Creating a VPC gateway attachment for the S3 endpoint enables connectivity between the VPC and the S3 service.

upvoted 1 times

✉ **nexus2020** 3 months ago

Selected Answer: AD

Gateway Endpoint = VPC connecting VPC privately with no internet connectivity

S3 access point = unique DNS address for applications to interact with a specific portion of a bucket, while allowing granular control over permissions and policies.

Interface Endpoint = AWS Service connecting VPC privately without internet connectivity

So the question is application accessing S3, so Gateway endpoint is out (CE out), also Interface Endpoint is out as well (B).

only AD left.

upvoted 2 times

Question #244

Topic 1

A company has developed a hybrid solution between its data center and AWS. The company uses Amazon VPC and Amazon EC2 instances that send application logs to Amazon CloudWatch. The EC2 instances read data from multiple relational databases that are hosted on premises.

The company wants to monitor which EC2 instances are connected to the databases in near-real time. The company already has a monitoring solution that uses Splunk on premises. A solutions architect needs to determine how to send networking traffic to Splunk.

How should the solutions architect meet these requirements?

- A. Enable VPC flows logs, and send them to CloudWatch. Create an AWS Lambda function to periodically export the CloudWatch logs to an Amazon S3 bucket by using the pre-defined export function. Generate ACCESS_KEY and SECRET_KEY AWS credentials. Configure Splunk to pull the logs from the S3 bucket by using those credentials.
- B. Create an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination. Configure a pre-processing AWS Lambda function with a Kinesis Data Firehose stream processor that extracts individual log events from records sent by CloudWatch Logs subscription filters. Enable VPC flows logs, and send them to CloudWatch. Create a CloudWatch Logs subscription that sends log events to the Kinesis Data Firehose delivery stream.
- C. Ask the company to log every request that is made to the databases along with the EC2 instance IP address. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs grouped by database name. Export Athena results to another S3 bucket. Invoke an AWS Lambda function to automatically send any new file that is put in the S3 bucket to Splunk.
- D. Send the CloudWatch logs to an Amazon Kinesis data stream with Amazon Kinesis Data Analytics for SQL Applications. Configure a 1-minute sliding window to collect the events. Create a SQL query that uses the anomaly detection template to monitor any networking traffic anomalies in near-real time. Send the result to an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination.

 **bhanus** Highly Voted  3 months ago

Selected Answer: B

Answer is B

Question asks for "near real time" analysis

For near real time -->use Kinesis Datafirehose.

For real time ---> use Kineses data streams

real-time is instant, whereas near real-time is delayed

upvoted 6 times

 **ggrodsckiy** Most Recent  2 months ago

correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

its a B

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: B

B, in this link <https://docs.aws.amazon.com/firehose/latest/dev/creating-the-stream-to-splunk.html#:~:text=In%20this%20part%20of%20the%20Kinesis%20Data%20Firehose%20tutorial%2C%20you%20create%20an%20Amazon%20Kinesis%20Data%20Firehose%20delivery%20stream%20to%20receive%20the%20log%20data%20from%20Amazon%20CloudWatch%20and%20deliver%20that%20data%20to%20Splunk.>, the traffic flow is: CW logs-> Kinesis Datafirehose delivery-> Splunk. In our case, we need custom logs, so need to subscribe VPC flow logs to send to splunk for specific monitoring

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: B

Answer is B

Question asks for "near real time" analysis

For near real time -->use Kinesis Datafirehose.

For real time ---> use Kineses data streams

real-time is instant, whereas near real-time is delayed

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: B

It's B - Rest is too complex. <https://docs.aws.amazon.com/firehose/latest/dev/creating-the-stream-to-splunk.html>

upvoted 3 times

✉  PhuocT 3 months ago

Selected Answer: B

B is answer, I think

upvoted 1 times

✉  ozelllll 3 months ago

Selected Answer: B

B. <https://docs.aws.amazon.com/firehose/latest/dev/vpc-splunk-tutorial.html>

upvoted 2 times

✉  gd1 3 months ago

Selected Answer: B

GPT - Amazon VPC Flow Logs can be enabled to capture information about the IP traffic going to and from network interfaces in the VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. Once the logs are in CloudWatch, you can create a subscription filter that forwards events to a Kinesis Data Firehose stream.

AWS Lambda can preprocess records in the Kinesis Data Firehose stream before they are delivered to Splunk. This solution provides near-real-time delivery of VPC Flow Logs to Splunk. Other options are less optimal because they involve unnecessary complexity or do not provide near-real-time monitoring.

upvoted 2 times

Question #245

Topic 1

A company has five development teams that have each created five AWS accounts to develop and host applications. To track spending, the development teams log in to each account every month, record the current cost from the AWS Billing and Cost Management console, and provide the information to the company's finance team.

The company has strict compliance requirements and needs to ensure that resources are created only in AWS Regions in the United States. However, some resources have been created in other Regions.

A solutions architect needs to implement a solution that gives the finance team the ability to track and consolidate expenditures for all the accounts. The solution also must ensure that the company can create resources only in Regions in the United States.

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

- A. Create a new account to serve as a management account. Create an Amazon S3 bucket for the finance team. Use AWS Cost and Usage Reports to create monthly reports and to store the data in the finance team's S3 bucket.
- B. Create a new account to serve as a management account. Deploy an organization in AWS Organizations with all features enabled. Invite all the existing accounts to the organization. Ensure that each account accepts the invitation.
- C. Create an OU that includes all the development teams. Create an SCP that allows the creation of resources only in Regions that are in the United States. Apply the SCP to the OU.
- D. Create an OU that includes all the development teams. Create an SCP that denies the creation of resources in Regions that are outside the United States. Apply the SCP to the OU.
- E. Create an IAM role in the management account. Attach a policy that includes permissions to view the Billing and Cost Management console. Allow the finance team users to assume the role. Use AWS Cost Explorer and the Billing and Cost Management console to analyze cost.
- F. Create an IAM role in each AWS account. Attach a policy that includes permissions to view the Billing and Cost Management console. Allow the finance team users to assume the role.

 **SkyZeroZx** 2 months, 2 weeks ago

Selected Answer: BDE

Remember SCP Only deny not allow (in definition)

upvoted 2 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: BDE

BDE - going with the crowd, although C seems like it'd work too. Is the issue that it can be overridden at account level?

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: BDE

BDE

Org -> enable all feature-> invite all member account-> member account accept invitation

Org-> mgmt account-> create IAM role to access to member account-> login member account assume this role to view billings

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: BDE

For C, do an allow statement with StringEqual, for D, do a deny statement with StringNotEqual of US region. So C & D are both right. Cost Explorer has all the reports, creating a S3 is NOT operationally efficient – A is out

IAM role is needed to view billing - E

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: BDE

correct answer is BDE

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: BDE

B - You need AWS Orgs to manage all other accts

D - You need to deny creating resources

E - You create the role in the mgmt acct not in each AWS acct. That's the point of the mgmt acct.

upvoted 4 times

 **Arnaud92** 1 month ago

I'm not sure for E. The management account in AWS Organisations is to manage members account and policies but not roles. I'll go for F instead.

upvoted 1 times

 **easystoo** 3 months ago

b-c-e...b-c-e

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: BDE

For C, do an allow statement with StringEqual, for D, do a deny statement with StringNotEqual of US region. So C & D are both right. Cost Explorer has all the reports, creating a S3 is NOT operationally efficient – A is out

IAM role is needed to view billing - E

upvoted 2 times

 **PhuocT** 3 months ago

B, D an E

upvoted 1 times

 **ozelliII** 3 months ago

Selected Answer: BDF

it's BDF

upvoted 2 times

 **gd1** 3 months ago

Selected Answer: ABD

Option A suggests using AWS Cost and Usage Reports to automatically generate and store consolidated monthly cost reports in an S3 bucket that is accessible to the finance team. B. Create a new account to serve as a management account. Deploy an organization in AWS Organizations with all features enabled. D. Create an OU that includes all the development teams. Create an SCP that denies the creation of resources in Regions that are outside the United States. Apply the SCP to the OU.

upvoted 1 times

Question #246

Topic 1

A company needs to create and manage multiple AWS accounts for a number of departments from a central location. The security team requires read-only access to all accounts from its own AWS account. The company is using AWS Organizations and created an account for the security team.

How should a solutions architect meet these requirements?

- A. Use the OrganizationAccountAccessRole IAM role to create a new IAM policy with read-only access in each member account. Establish a trust relationship between the IAM policy in each member account and the security account. Ask the security team to use the IAM policy to gain access.
- B. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the IAM role to gain access.
- C. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the management account from the security account. Use the generated temporary credentials to gain access.
- D. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the member account from the security account. Use the generated temporary credentials to gain access.

 **ggrodskiy** 2 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

its a b

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: B

So there is 3 parts, security account, member account, org account

Goal: Security account-> member account

In org account, use org crossAccountAccessRole-> create ReadOnlyRole in member account

Build trust: security account & member account

Security account assume member account ReadOnlyRole

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B - You need a role.

upvoted 1 times

 **easystoo** 3 months ago

b-b-b-b-b-b-b

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

B is classic usage of Cross Account Role

upvoted 1 times

 **Jackhemo** 3 months ago

oh labiba is 'B'

To meet the requirements, a solutions architect should choose option B. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the IAM role to gain access.

By using the OrganizationAccountAccessRole IAM role, the solutions architect can create a new IAM role with read-only access in each member account. This allows the security team to have read-only access to all accounts from their own AWS account. The trust relationship between the IAM role in each member account and the security account ensures that the security team can assume the IAM role and access the necessary resources.

upvoted 1 times

 **PhuocT** 3 months ago

B is the answer

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: B

GPT: This approach aligns with the AWS best practice of using IAM roles to delegate permissions across AWS accounts. The OrganizationAccountAccessRole is a role that is automatically created when you create a new account in an organization. This role can be assumed by the master account, but it can also be assumed by other accounts if a trust relationship is established.

upvoted 3 times

 **Alabi** 3 months ago

Selected Answer: B

Option B suggests using the OrganizationAccountAccessRole IAM role to create a new IAM role in each member account. This IAM role will have read-only access permissions. By establishing a trust relationship between the IAM role in each member account and the security account, the security team's AWS account is granted access to the member accounts.

upvoted 2 times

 **bhanus** 3 months ago

Selected Answer: B

B is right

A is incorrect as you CANNOT establish a trust relationship between the IAM policy and account

C and D does NOT talk about readonly access

upvoted 3 times

Question #247

Topic 1

A large company runs workloads in VPCs that are deployed across hundreds of AWS accounts. Each VPC consists of public subnets and private subnets that span across multiple Availability Zones. NAT gateways are deployed in the public subnets and allow outbound connectivity to the internet from the private subnets.

A solutions architect is working on a hub-and-spoke design. All private subnets in the spoke VPCs must route traffic to the internet through an egress VPC. The solutions architect already has deployed a NAT gateway in an egress VPC in a central AWS account.

Which set of additional steps should the solutions architect take to meet these requirements?

- A. Create peering connections between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet.
- B. Create a transit gateway, and share it with the existing AWS accounts. Attach existing VPCs to the transit gateway. Configure the required routing to allow access to the internet.
- C. Create a transit gateway in every account. Attach the NAT gateway to the transit gateways. Configure the required routing to allow access to the internet.
- D. Create an AWS PrivateLink connection between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet.

 **ggrodsckiy** 2 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

b for sure

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: B

hundreds of VPCs-> TGW

then we only have B and C

C: create TGW in each account, wrong

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B - Hub and spoke is based on transit GW

upvoted 2 times

 **easystoo** 3 months ago

b-b-b-b-b-b-b

upvoted 1 times

 **PhuocT** 3 months ago

yep, it's B

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: B

Option B suggests creating a transit gateway, which acts as a hub for connectivity between multiple VPCs and on-premises networks. By sharing the transit gateway with the existing AWS accounts, the solutions architect can attach the VPCs, including the spoke VPCs, to the transit gateway. The required routing can then be configured to direct traffic from the spoke VPCs to the transit gateway, which will route it to the egress VPC with the NAT gateway. This allows for centralized routing and connectivity to the internet for the spoke VPCs.

upvoted 2 times

 **gd1** 3 months ago

Selected Answer: B

GPT = B; AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. It simplifies the management of network connectivity across a large number of accounts/VPCs.

upvoted 1 times

 **jubileu84** 3 months ago

B is correct because we have hundreds of vpcs and default quota for peering peer vpc is = 50

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: B

SHould be B

upvoted 1 times

Question #248

Topic 1

An education company is running a web application used by college students around the world. The application runs in an Amazon Elastic Container Service (Amazon ECS) cluster in an Auto Scaling group behind an Application Load Balancer (ALB). A system administrator detects a weekly spike in the number of failed login attempts, which overwhelm the application's authentication service. All the failed login attempts originate from about 500 different IP addresses that change each week. A solutions architect must prevent the failed login attempts from overwhelming the authentication service.

Which solution meets these requirements with the MOST operational efficiency?

- A. Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses.
- B. Create an AWS WAF web ACL with a rate-based rule, and set the rule action to Block. Connect the web ACL to the ALB.
- C. Use AWS Firewall Manager to create a security group and security group policy to allow access only to specific CIDR ranges.
- D. Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Block. Connect the web ACL to the ALB.

 **ggrodskiy** 2 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: B

easyu B

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: B

B, if login hit at a certain ratio, block this IP

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: B

B and not D because of "500 different IP addresses that change each week"

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B and not D because of "500 different IP addresses that change each week"

upvoted 3 times

 **easytoo** 3 months ago

b-b-b-b-b-b

upvoted 1 times

 **PhuocT** 3 months ago

yep, it's B

upvoted 1 times

 **elanelans** 3 months ago

Selected Answer: B

B Is Correct.

Since IP address keeps changing, WAF can't block on IP/CIDR.

upvoted 2 times

 **bhanus** 3 months ago

Selected Answer: B

B is the answer

upvoted 3 times

Question #249

Topic 1

A company operates an on-premises software-as-a-service (SaaS) solution that ingests several files daily. The company provides multiple public SFTP endpoints to its customers to facilitate the file transfers. The customers add the SFTP endpoint IP addresses to their firewall allow list for outbound traffic. Changes to the SFTP endpoint IP addresses are not permitted.

The company wants to migrate the SaaS solution to AWS and decrease the operational overhead of the file transfer service.

Which solution meets these requirements?

- A. Register the customer-owned block of IP addresses in the company's AWS account. Create Elastic IP addresses from the address pool and assign them to an AWS Transfer for SFTP endpoint. Use AWS Transfer to store the files in Amazon S3.
- B. Add a subnet containing the customer-owned block of IP addresses to a VPC. Create Elastic IP addresses from the address pool and assign them to an Application Load Balancer (ALB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the ALB. Store the files in attached Amazon Elastic Block Store (Amazon EBS) volumes.
- C. Register the customer-owned block of IP addresses with Amazon Route 53. Create alias records in Route 53 that point to a Network Load Balancer (NLB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the NLB. Store the files in Amazon S3.
- D. Register the customer-owned block of IP addresses in the company's AWS account. Create Elastic IP addresses from the address pool and assign them to an Amazon S3 VPC endpoint. Enable SFTP support on the S3 bucket.

 **Simon523** 4 weeks, 1 day ago

Selected Answer: A

should use AWS Transfer for SFTP

upvoted 1 times

 **breadops** 1 month, 3 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/storage/use-ip-whitelisting-to-secure-your-aws-transfer-for-sftp-servers/>

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct A.

upvoted 1 times

 **nicecurls** 2 months, 2 weeks ago

Selected Answer: A

it's A

upvoted 1 times

 **Piccaso** 2 months, 3 weeks ago

Selected Answer: A

D is too manual

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: A

its an A

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: A

A - AWS Managed SFTP

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: A

AWS Transfer for SFTP, fully managed service, no operational overhead

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: A

Option A suggests using AWS Transfer for SFTP, which is a fully managed service that enables the transfer of files over the Secure File Transfer Protocol (SFTP) directly into and out of Amazon S3. By registering the customer-owned block of IP addresses in the company's AWS account and creating Elastic IP addresses from that address pool, the company can assign those IP addresses to an AWS Transfer for SFTP endpoint.

This allows the customers to continue using their existing firewall allow lists without requiring any changes. The files transferred through the SFTP endpoints are stored directly in Amazon S3, reducing operational overhead.

upvoted 3 times

gd1 3 months ago

Selected Answer: A

AWS Transfer Family provides fully managed support for Secure File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS), and File Transfer Protocol (FTP). AWS Transfer Family provides a seamless migration experience while preserving authentications and security policies, and it can handle the scale of demanding file transfer workloads. The file transfer can be stored directly into Amazon S3 or Amazon EFS.

upvoted 1 times

MoussaNoussa 3 months ago

A is the right answer

upvoted 1 times

Question #250

Topic 1

A company has a new application that needs to run on five Amazon EC2 instances in a single AWS Region. The application requires high-throughput, low-latency network connections between all of the EC2 instances where the application will run. There is no requirement for the application to be fault tolerant.

Which solution will meet these requirements?

- A. Launch five new EC2 instances into a cluster placement group. Ensure that the EC2 instance type supports enhanced networking.
- B. Launch five new EC2 instances into an Auto Scaling group in the same Availability Zone. Attach an extra elastic network interface to each EC2 instance.
- C. Launch five new EC2 instances into a partition placement group. Ensure that the EC2 instance type supports enhanced networking.
- D. Launch five new EC2 instances into a spread placement group. Attach an extra elastic network interface to each EC2 instance.

NikkyDicky 2 months, 3 weeks ago

Selected Answer: A

easy A

upvoted 1 times

SmileyCloud 3 months ago

Selected Answer: A

A - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

upvoted 3 times

Alabi 3 months ago

Selected Answer: A

A for sure

upvoted 1 times

gd1 3 months ago

Selected Answer: A

A cluster placement group is a type of placement group that packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of high performance computing (HPC) applications.

upvoted 1 times

elanelans 3 months ago

Selected Answer: A

A- Provides Low latency and high throughput.

Auto scaling with additional ENI, spread placement and partition placement won't achieve the requirement.

upvoted 1 times

bhanus 3 months ago

Selected Answer: A

A - Cluster placement group

C is incorrect because Partition placement groups are used for large distributed workloads, like Hadoop, Cassandra, and Kafka. They do not offer the same low-latency, high-throughput benefits as cluster placement groups.

upvoted 2 times

Question #251

Topic 1

A company is creating a REST API to share information with six of its partners based in the United States. The company has created an Amazon API Gateway Regional endpoint. Each of the six partners will access the API once per day to post daily sales figures.

After initial deployment, the company observes 1,000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic is originating from a botnet and wants to secure its API while minimizing cost.

Which approach should the company take to secure its API?

- A. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Configure CloudFront with an origin access identity (OAI) and associate it with the distribution. Configure API Gateway to ensure only the OAI can run the POST method.
- B. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Add a custom header to the CloudFront distribution populated with an API key. Configure the API to require an API key on the POST method.
- C. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API. Create a resource policy with a request limit and associate it with the API. Configure the API to require an API key on the POST method.
- D. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API. Create a usage plan with a request limit and associate it with the API. Create an API key and add it to the usage plan.

 **xav1er** 1 month ago

Selected Answer: D

def answ D as described here
<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-aws-waf.html>
 upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct D.

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: D

D fits
 upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: D

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

Users from a specified AWS account.

Specified source IP address ranges or CIDR blocks.

Specified virtual private clouds (VPCs) or VPC endpoints (in any account).

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: D

It's D. The IP filtering is done with the WAF ACL so there is no need to do another IP filtering by using resource policies which can do exactly that. <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-resource-policies.html>
 upvoted 2 times

 **easystoo** 3 months ago

d-d-d-d-d-d

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: D

D is classic use of "usage plan" in API Gateway additionally more appropriate practice is API Key for authentication or other methods
 upvoted 2 times

 **Maria2023** 3 months ago

Selected Answer: D

I vote for D since I couldn't find a way to set up a request limit in resource policy
<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-resource-policies.html>

upvoted 2 times

 shree2023 3 months ago

Selected Answer: D

Ans is Opt D, A usage plan provides select customers with specific access permissions and request quotas, which helps manage and restrict usage to prevent overuse of resources.

API keys are used for tracking and controlling how the API is used. This additional layer of security ensures that only those with the key can access the API.

Why not Opt C, Amazon API Gateway doesn't support request limiting through resource policies. You can set permissions on who can access your API using a resource policy, but rate limiting isn't handled by resource policies.

API keys alone do not provide throttling or rate limiting. For throttling, you typically would need to use them along with usage plans

upvoted 4 times

 Alabi 3 months ago

Selected Answer: C

Option C provides a cost-effective approach to securing the API while allowing access only to the IP addresses used by the six partners. By creating an AWS WAF web ACL and configuring it to allow access only to the IP addresses of the trusted partners, the company can effectively block requests originating from unauthorized sources. Associating the web ACL with the API ensures that the filtering rules are applied to the API traffic.

Additionally, creating a resource policy with a request limit allows the company to set a maximum limit on the number of requests that can be made to the API within a given time frame. This helps mitigate the impact of potential botnet traffic, ensuring that the API is not overwhelmed with excessive requests.

Requiring an API key on the POST method adds an extra layer of security by enforcing authentication for accessing the API. This ensures that only authorized partners with valid API keys can successfully make requests to the API.

upvoted 1 times

 gd1 3 months ago

Selected Answer: D

GPT 4.0: AWS WAF is a web application firewall that lets you monitor HTTP and HTTPS requests that are forwarded to Amazon API Gateway. The solution architect can create a WAF rule that allows access only from the IP addresses of the six partners.

A usage plan in API Gateway provides throttling and quota limits to manage the rate of requests from your customers and prevent attacks. Setting a request limit that matches the expected usage of the partners would help to protect the API.

upvoted 1 times

Question #252

Topic 1

A company uses an Amazon Aurora PostgreSQL DB cluster for applications in a single AWS Region. The company's database team must monitor all data activity on all the databases.

Which solution will achieve this goal?

- A. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an Amazon OpenSearch Service cluster for further analysis.
- B. Start a database activity stream on the Aurora DB cluster to capture the activity stream in Amazon EventBridge. Define an AWS Lambda function as a target for EventBridge. Program the Lambda function to decrypt the messages from EventBridge and to publish all database activity to Amazon S3 for further analysis.
- C. Start a database activity stream on the Aurora DB cluster to push the activity stream to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to consume the Kinesis data stream and to deliver the data to Amazon S3 for further analysis.
- D. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an Amazon Redshift cluster. Run queries on the Amazon Redshift data to determine database activities on the Aurora database.

✉ **ggrodskiy** 2 months ago

Correct C.

upvoted 1 times

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

Selected Answer: C

its a C

upvoted 1 times

✉ **SmileyCloud** 3 months ago

C - Correct. <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

upvoted 2 times

✉ **SkyZeroZx** 3 months ago

Selected Answer: C

C achieves the Goal.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

upvoted 1 times

✉ **shree2023** 3 months ago

Selected Answer: C

C indeed

upvoted 1 times

✉ **gd1** 3 months ago

Selected Answer: C

GPT: Option A and D are incorrect because AWS DMS's Change Data Capture (CDC) functionality captures changes made at the database level, not data activity.

upvoted 1 times

✉ **elanelans** 3 months ago

Selected Answer: C

C achieves the Goal.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

upvoted 3 times

✉ **MoussaNoussa** 3 months ago

C is the right answer

upvoted 1 times

✉ **bhanus** 3 months ago

Selected Answer: C

I go with C

upvoted 1 times

Question #253

Topic 1

An entertainment company recently launched a new game. To ensure a good experience for players during the launch period, the company deployed a static quantity of 12 r6g.16xlarge (memory optimized) Amazon EC2 instances behind a Network Load Balancer. The company's operations team used the Amazon CloudWatch agent and a custom metric to include memory utilization in its monitoring strategy.

Analysis of the CloudWatch metrics from the launch period showed consumption at about one quarter of the CPU and memory that the company expected. Initial demand for the game has subsided and has become more variable. The company decides to use an Auto Scaling group that monitors the CPU and memory consumption to dynamically scale the instance fleet. A solutions architect needs to configure the Auto Scaling group to meet demand in the most cost-effective way.

Which solution will meet these requirements?

- A. Configure the Auto Scaling group to deploy c6g.4xlarge (compute optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- B. Configure the Auto Scaling group to deploy m6g.4xlarge (general purpose) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- C. Configure the Auto Scaling group to deploy r6g.4xlarge (memory optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- D. Configure the Auto Scaling group to deploy r6g.8xlarge (memory optimized) instances. Configure a minimum capacity of 2, a desired capacity of 2, and a maximum capacity of 6.

 **chico2023** 1 month, 2 weeks ago

Selected Answer: C

Initially I was thinking on how the ASG would handle the spikes knowing that each r6g.4xlarge might have troubles handle the load, but the question is to handle the demand in the most cost-effective way.

In terms of cost, Maria2023 and Nexus2020 made a point that can't be beaten here.

I am still thinking on the load, but if there is something I am learning with these questions is that many of them won't give you enough to make a REAL informed decision, so you should go with your best judgement.

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

C I guess. weird question

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C makes most sense.

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: C

1 r6g.4xlarge - \$0.8064/h

1 r6g.8xlarge - \$1.6128/h

During peak times both C and D will cost 9.6768/h

However, during non-peak times, C will cost less - 2.4192/h vs 3.2256

Plus that I think D will be a bit underutilized most of the times if the trends remain the same

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: C

16large = 64CPU,

4Large = 16 CPU

8Large = 32 CPU

1/4 usage of 64 = 16CPU

1/4 of 12 EC2 = 3 instance, so C is a better choice.

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: C

Memory optimized and cost optimized

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: D

The company initially deployed 12 r6g.16xlarge instances but found that the consumption was much lower than expected. To optimize cost, it is necessary to scale down the instance type while still meeting the demand.

Option D suggests configuring the Auto Scaling group to use r6g.8xlarge instances, which have less memory capacity compared to r6g.16xlarge instances. With a minimum capacity of 2, desired capacity of 2, and maximum capacity of 6, the Auto Scaling group will scale up or down based on CPU and memory utilization.

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: C

The requirements state that the current set of instances (r6g.16xlarge - memory optimized) are only using about a quarter of the available CPU and memory. Therefore, a smaller instance size would be more cost-effective while still meeting the demand. In this case, the r6g.4xlarge instances would be appropriate, as they are a quarter of the size of the currently used instances (r6g.16xlarge).

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: C

C . From the question, app is running on memory-optimized instances (r6g.16xlarge) but only utilizing about one quarter of the CPU and memory. So cost-effective to use smaller instances (r6g.4xlarge), which provide a quarter of r6g.16xlarge instances.

upvoted 4 times

Question #254

Topic 1

A financial services company loaded millions of historical stock trades into an Amazon DynamoDB table. The table uses on-demand capacity mode. Once each day at midnight, a few million new records are loaded into the table. Application read activity against the table happens in bursts throughout the day, and a limited set of keys are repeatedly looked up. The company needs to reduce costs associated with DynamoDB.

Which strategy should a solutions architect recommend to meet this requirement?

- A. Deploy an Amazon ElastiCache cluster in front of the DynamoDB table
- B. Deploy DynamoDB Accelerator (DAX). Configure DynamoDB auto scaling. Purchase Savings Plans in Cost Explorer.
- C. Use provisioned capacity mode. Purchase Savings Plans in Cost Explorer.
- D. Deploy DynamoDB Accelerator (DAX). Use provisioned capacity mode. Configure DynamoDB auto scaling.

✉ **chico2023** 1 month, 2 weeks ago

Selected Answer: D

It's D. Purchase Savings Plans in Cost Explorer is not for DynamoDB. At least not today.

upvoted 3 times

✉ **MRL110** 1 month, 4 weeks ago

Selected Answer: D

Repeated lookups = DAX

Avoid bursts = Provisioned Capacity

upvoted 2 times

✉ **Just_Ninja** 2 months ago

Selected Answer: B

Did you read the question?

To reduce costs you can use DAX.

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

Here is nothing in the question about saving plans or else.

upvoted 1 times

✉ **Just_Ninja** 2 months ago

I now switch to D, because it's an expedited workload.

upvoted 1 times

✉ **rxhan** 1 month, 3 weeks ago

loool

upvoted 1 times

✉ **ggrodsckiy** 2 months ago

Correct D.

upvoted 1 times

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

Selected Answer: C

The D looks like a perfect solution. But the question is only asking to reduce the cost, so I would like to choose C instead.

upvoted 3 times

✉ **rxhan** 1 month, 3 weeks ago

what about caching?

upvoted 1 times

✉ **rrrrrrrrr1** 2 months, 2 weeks ago

Isn't DAX extremely expensive? Weird question.

upvoted 1 times

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

Selected Answer: D

its a D

upvoted 1 times

✉ **Christina666** 2 months, 3 weeks ago

Selected Answer: D

DAX + Provision Capacity + Auto Scaling meets the need

upvoted 1 times

SmileyCloud 3 months ago

Selected Answer: D

Savings plan is for EC2, B and C are out. A is for read boost. D is correct.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html#HowItWorks.ProvisionedThroughput.Manual>

upvoted 1 times

nexus2020 3 months ago

Selected Answer: D

DynamoDB Accelerator (DAX) is an in-memory caching service provided by AWS that is specifically designed to enhance the performance of Amazon DynamoDB. It acts as a caching layer between your application and DynamoDB, reducing the need to directly access the DynamoDB service for frequently accessed data.

D!

upvoted 1 times

shree2023 3 months ago

Selected Answer: D

DAX + Provision Capacity + Auto Scaling meets the need

upvoted 2 times

gd1 3 months ago

Selected Answer: D

Deploying DynamoDB Accelerator (DAX) will help in caching read activity, which can reduce the read cost because DAX is a fully managed, highly available, in-memory cache for DynamoDB that can improve the read performance by up to 10 times, even at millions of requests per second.

The use of provisioned capacity mode allows you to set the capacity for your table to handle expected workloads, and the table's capacity will not scale up and down based on traffic patterns, which could potentially reduce cost when compared to on-demand capacity mode if your usage is predictable.

upvoted 1 times

elanelans 3 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/80440-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

bhanus 3 months ago

Selected Answer: D

D provisioned capacity mode.

As per charGPT company is currently using on-demand capacity mode. On-demand capacity mode is priced higher than provisioned capacity mode because it automatically accommodates your workload's capacity needs based on the volume of reads and writes your application performs. For workloads with predictable capacity needs, provisioned capacity mode can be more cost effective.

upvoted 1 times

Question #255

A company is creating a centralized logging service running on Amazon EC2 that will receive and analyze logs from hundreds of AWS accounts. AWS PrivateLink is being used to provide connectivity between the client services and the logging service.

In each AWS account with a client, an interface endpoint has been created for the logging service and is available. The logging service running on EC2 instances with a Network Load Balancer (NLB) are deployed in different subnets. The clients are unable to submit logs using the VPC endpoint.

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

- A. Check that the NACL is attached to the logging service subnet to allow communications to and from the NLB subnets. Check that the NACL is attached to the NLB subnet to allow communications to and from the logging service subnets running on EC2 instances.
- B. Check that the NACL is attached to the logging service subnets to allow communications to and from the interface endpoint subnets. Check that the NACL is attached to the interface endpoint subnet to allow communications to and from the logging service subnets running on EC2 instances.
- C. Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the NLB subnets.
- D. Check the security group for the logging service running on EC2 instances to ensure it allows ingress from the clients.
- E. Check the security group for the NLB to ensure it allows ingress from the interface endpoint subnets.

 **cmoreira** 3 weeks, 2 days ago

Selected Answer: AC

AC

3rd point on <https://docs.aws.amazon.com/vpc/latest/privatelink/create-endpoint-service.html#considerations-endpoint-services>
upvoted 2 times

 **vjp_training** 1 month, 1 week ago

Selected Answer: AC

<https://www.examtopics.com/discussions/amazon/view/36058-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 2 times

 **Just_Ninja** 2 months ago

Selected Answer: BC

B and C.

The NLB is places in the destination Account. That means the EC2 logging instance get traffic from the NLB.
So the source for the Logging EC2 instance must be the NLB.

<https://aws.amazon.com/de/blogs/architecture/building-saas-services-for-aws-customers-with-privatelink/>
Old but not outdated

upvoted 3 times

 **emupsx1** 2 months, 1 week ago

Selected Answer: AC

When service consumers send traffic to a service through an interface endpoint, the source IP addresses provided to the application are the private IP addresses of the load balancer nodes, not the IP addresses of the service consumers.

<https://docs.aws.amazon.com/vpc/latest/privatelink/create-endpoint-service.html>
upvoted 3 times

 **study_aws1** 2 months, 1 week ago

Foe those selecting options B), D) over A), C). Please note Consumer & Service providers are in different VPCs that are not peered (connected through PrivateLink) & can have overlapping IPs also. You'll not be able to reference SGs across VPCs not peered & even by private IPs which can be overlapping.

A) - We can reference IP of the Network LB with the subnet of EC2s via NACL, though it's allowed by default within VPC unless we want to make this more restrictive.

C) - Network LB itself does not have a SG, but the option states allowing the IP range of CIDR associated with Network LB subnet in the SG associated with the EC2 instances, which is a valid option.

IMO, options B) & D) are feasible only if hundreds of AWS accounts (client services) lie in the same VPC as the logging service, which the question does not seem to state.

upvoted 3 times

 **shacky** 2 months, 2 weeks ago

Selected Answer: AC

It's actually AC.

Logging service will receive traffic from NLB, not from the clients directly. That architecture (PrivateLink endpoint service) allows you to have overlapping CIDR block between client and service provider.

upvoted 2 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: BD

its BD

no SG for NLB

upvoted 1 times

 **NikkyDicky** 2 months ago

after reading newer comments, I'm switching to AC

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: BD

NLB no security groups

AWS Network Load Balancer does not support security groups today. You can use Amazon VPC NACLs, AWS Network Firewall, and/or a marketplace firewall with AWS Gateway Load Balancer to provide various levels of protection for your NLB. You can also use security groups on your targets if client IP preservation is enabled (see more here about when client IP preservation is supported)

<https://repost.aws/questions/QUuuueXAi20QuisbkOhinnbzQ/aws-nlb-security-group>

upvoted 1 times

 **finesse_999** 1 month, 1 week ago

You can associate a security group to your NLB. Please find link below:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-security-groups.html>

Based on this, the answer should be B and E.

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: BD

B and D. C is out, you don't configure ingress from NLB subnets, same with E, NLBs don't have security groups. A - same concept. NLB is transparent unlike classic ELB and ALB.

upvoted 4 times

 **nexus2020** 3 months ago

Selected Answer: BD

Sender (Client's interface endpoint) --> private link --> Receiver (NLB --> EC2 of Logging service)

so the NACL and Security group are all on the receiver side, therefore it should include the sender (client) ip.

so B & D

upvoted 2 times

 **PhuocT** 3 months ago

I think it B and D

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: BD

B&D seems right

upvoted 1 times

Question #256

Topic 1

A company has millions of objects in an Amazon S3 bucket. The objects are in the S3 Standard storage class. All the S3 objects are accessed frequently. The number of users and applications that access the objects is increasing rapidly. The objects are encrypted with server-side encryption with AWS KMS keys (SSE-KMS).

A solutions architect reviews the company's monthly AWS invoice and notices that AWS KMS costs are increasing because of the high number of requests from Amazon S3. The solutions architect needs to optimize costs with minimal changes to the application.

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

- A. Create a new S3 bucket that has server-side encryption with customer-provided keys (SSE-C) as the encryption type. Copy the existing objects to the new S3 bucket. Specify SSE-C.
- B. Create a new S3 bucket that has server-side encryption with Amazon S3 managed keys (SSE-S3) as the encryption type. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Specify SSE-S3.
- C. Use AWS CloudHSM to store the encryption keys. Create a new S3 bucket. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Encrypt the objects by using the keys from CloudHSM.
- D. Use the S3 Intelligent-Tiering storage class for the S3 bucket. Create an S3 Intelligent-Tiering archive configuration to transition objects that are not accessed for 90 days to S3 Glacier Deep Archive.

 **gd1** Highly Voted 3 months ago

Selected Answer: B

This option switches the encryption method from using AWS Key Management Service (AWS KMS) to using server-side encryption with S3 managed keys (SSE-S3). This change can significantly reduce costs because AWS KMS charges per API request, while SSE-S3 does not have additional charges per API request beyond the S3 usage.

upvoted 6 times

 **shizhan** Most Recent 1 month ago

B

<https://aws.amazon.com/about-aws/whats-new/2020/12/amazon-s3-bucket-keys-reduce-the-costs-of-server-side-encryption-with-aws-key-management-service-sse-kms/>

upvoted 1 times

 **Just_Ninja** 2 months ago

Selected Answer: B

B...

Because SSE-S3 has no additional costs.

SSE-C cost per month 0,00040 USD per GB encrypted Data on Top

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct B.

upvoted 2 times

 **nicecurls** 2 months, 2 weeks ago

Selected Answer: B

this is B

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

B for sure

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

None of this is correct. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-key.html>, but let's go with B.

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: B

I would actually expect an option with a bucket key as a possible answer since that's the purpose of it. From the available choices, I choose B.

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: B

By choosing option B, you can switch the encryption type from SSE-KMS to SSE-S3, which eliminates the need for AWS KMS requests, thereby reducing the associated costs. This solution requires minimal changes to the application and avoids additional operational overhead.

upvoted 3 times

 **i_am_robot** 3 months ago

Selected Answer: B

The goal here is to reduce the cost related to the usage of AWS KMS keys for server-side encryption. Using SSE-S3, which uses Amazon S3 managed keys for server-side encryption, would eliminate the additional cost related to KMS key usage while still maintaining a high level of security. Amazon S3 handles key management, which also reduces operational overhead. S3 Batch Operations can be used to efficiently copy the existing objects to the new bucket.

upvoted 3 times

 **PhuocT** 3 months ago

B, SSE-S3 does not incur additional costs.

upvoted 2 times

 **shree2023** 3 months ago

Selected Answer: B

B is the least operational overhead

upvoted 1 times

Question #257

Topic 1

A media storage application uploads user photos to Amazon S3 for processing by AWS Lambda functions. Application state is stored in Amazon DynamoDB tables. Users are reporting that some uploaded photos are not being processed properly. The application developers trace the logs and find that Lambda is experiencing photo processing issues when thousands of users upload photos simultaneously. The issues are the result of Lambda concurrency limits and the performance of DynamoDB when data is saved.

Which combination of actions should a solutions architect take to increase the performance and reliability of the application? (Choose two.)

- A. Evaluate and adjust the RCUs for the DynamoDB tables.
- B. Evaluate and adjust the WCUs for the DynamoDB tables.
- C. Add an Amazon ElastiCache layer to increase the performance of Lambda functions.
- D. Add an Amazon Simple Queue Service (Amazon SQS) queue and reprocessing logic between Amazon S3 and the Lambda functions.
- E. Use S3 Transfer Acceleration to provide lower latency to users.

 **ggrodskiy** 2 months ago

Correct BD

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: BD

BD for sure

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: BD

B - because "performance of DynamoDB when data is saved."

D - you need a queue to slow things down and not loose any uploads

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: BD

SQS and write to DDB.

upvoted 1 times

 **i_am_robot** 3 months ago

Selected Answer: BD

Adding an Amazon Simple Queue Service (Amazon SQS) queue and reprocessing logic between Amazon S3 and the Lambda functions will help to decouple the Lambda functions from the S3 events and allow the Lambda functions to process photos in batches. This will help to improve the performance of the Lambda functions and reduce the risk of photos not being processed properly.

Evaluating and adjusting the WCUs for the DynamoDB tables will help to improve the performance of the DynamoDB tables when data is saved. This will help to reduce the risk of Lambda functions experiencing errors when saving data to DynamoDB.

upvoted 1 times

 **PhuocT** 3 months ago

Selected Answer: BD

B and D, I think

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: BD

WCU & SQS will solve the issue

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: BD

B -Ques says app has performance issues when data is SAVED. So this is a write. So increase WCU.

D- can help decouple

upvoted 2 times

Question #258

Topic 1

A company runs an application in an on-premises data center. The application gives users the ability to upload media files. The files persist in a file server. The web application has many users. The application server is overutilized, which causes data uploads to fail occasionally. The company frequently adds new storage to the file server. The company wants to resolve these challenges by migrating the application to AWS.

Users from across the United States and Canada access the application. Only authenticated users should have the ability to access the application to upload files. The company will consider a solution that refactors the application, and the company needs to accelerate application development.

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

- A. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Modify the application to use Amazon S3 to persist the files. Use Amazon Cognito to authenticate users.
- B. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Set up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application. Modify the application to use Amazon S3 to persist the files.
- C. Create a static website for uploads of media files. Store the static assets in Amazon S3. Use AWS AppSync to create an API. Use AWS Lambda resolvers to upload the media files to Amazon S3. Use Amazon Cognito to authenticate users.
- D. Use AWS Amplify to create a static website for uploads of media files. Use Amplify Hosting to serve the website through Amazon CloudFront. Use Amazon S3 to store the uploaded media files. Use Amazon Cognito to authenticate users.

 **ggrodskiy** 2 months ago

Correct D.

upvoted 1 times

 **rrrrrrrrr1** 2 months, 2 weeks ago

Why not C?

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: D

its a D

upvoted 1 times

 **Christina666** 2 months, 3 weeks ago

Selected Answer: D

key words: "development"

AWS Amplify is a complete solution that lets frontend web and mobile developers easily build, ship, and host full-stack applications on AWS

upvoted 2 times

 **SmileyCloud** 3 months ago

D - <https://aws.amazon.com/amplify/>

upvoted 2 times

 **nexus2020** 3 months ago

Selected Answer: D

LEAST operational overhead

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: D

Option D leverages AWS Amplify, a development platform, to create a static website for uploading media files. Amplify simplifies the process of building and deploying web applications. With Amplify Hosting, the website can be easily served through Amazon CloudFront, which provides low-latency content delivery.

Amazon S3 is used to store the uploaded media files. S3 is a highly scalable and durable object storage service that can handle large amounts of data. It provides secure storage for the files and allows easy integration with other AWS services.

This solution requires minimal operational overhead as AWS Amplify abstracts away much of the underlying infrastructure setup and configuration. It enables faster application development and deployment while providing scalability, security, and authentication features needed for the requirements of the application.

upvoted 4 times

✉  **Maria2023** 3 months ago

Selected Answer: D

Think the key here is this requirement "accelerate application development." Which is one of the things Amplify does
upvoted 1 times

✉  **PhuocT** 3 months ago

Selected Answer: D

solution will meet these requirements with the LEAST operational overhead and the company will consider a solution that refactors the application.

with those info, I think D is the answer

upvoted 1 times

✉  **gd1** 3 months ago

Selected Answer: D

AWS Amplify simplifies the process of building, deploying, and hosting web applications, providing a streamlined way to create a new application that would address the company's needs. Amplify Hosting provides fast, global hosting for the static website. Plus S3

upvoted 1 times

✉  **shree2023** 3 months ago

Selected Answer: A

A is least operational overhead.

D is lot of work upfront

upvoted 2 times

✉  **bhanus** 3 months ago

Selected Answer: D

D aws amplify facilitates the building, deploying, and hosting of the web application. It integrates with Amazon CloudFront for global content delivery and Amazon S3 for file storage

upvoted 1 times

Question #259

Topic 1

A company has an application that is deployed on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are part of an Auto Scaling group. The application has unpredictable workloads and frequently scales out and in. The company's development team wants to analyze application logs to find ways to improve the application's performance. However, the logs are no longer available after instances scale in.

Which solution will give the development team the ability to view the application logs after a scale-in event?

- A. Enable access logs for the ALB. Store the logs in an Amazon S3 bucket.
- B. Configure the EC2 instances to publish logs to Amazon CloudWatch Logs by using the unified CloudWatch agent.
- C. Modify the Auto Scaling group to use a step scaling policy.
- D. Instrument the application with AWS X-Ray tracing.

 **ggrodskiy** 2 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

easy B

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B - custom logs

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: B

The question states that the development team wants to analyze application logs, and these logs disappear after EC2 instances scale in. To solve this, you can configure the EC2 instances to send their logs to Amazon CloudWatch Logs using the unified CloudWatch agent. This allows you to keep the logs for a longer time period and enables the development team to analyze them at any time, even after the instances have been terminated.

upvoted 1 times

 **shree2023** 3 months ago

B is correct indeed

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: B

B is correct

Option A - ALB access logs only has details about requests sent to the load balancer, not application

Option C - change autoscaling behavior would NOT address the problem

Option D AWS X-Ray is more suitable for tracing requests as they travel through your application, It doesn't store output logs from your application.

upvoted 2 times

Question #260

Topic 1

A company runs an unauthenticated static website (www.example.com) that includes a registration form for users. The website uses Amazon S3 for hosting and uses Amazon CloudFront as the content delivery network with AWS WAF configured. When the registration form is submitted, the website calls an Amazon API Gateway API endpoint that invokes an AWS Lambda function to process the payload and forward the payload to an external API call.

During testing, a solutions architect encounters a cross-origin resource sharing (CORS) error. The solutions architect confirms that the CloudFront distribution origin has the Access-Control-Allow-Origin header set to www.example.com.

What should the solutions architect do to resolve the error?

- A. Change the CORS configuration on the S3 bucket. Add rules for CORS to the AllowedOrigin element for www.example.com.
- B. Enable the CORS setting in AWS WAF. Create a web ACL rule in which the Access-Control-Allow-Origin header is set to www.example.com.
- C. Enable the CORS setting on the API Gateway API endpoint. Ensure that the API endpoint is configured to return all responses that have the Access-Control-Allow-Origin header set to www.example.com.
- D. Enable the CORS setting on the Lambda function. Ensure that the return code of the function has the Access-Control-Allow-Origin header set to www.example.com.

 **ggrodsckiy** 2 months ago

Correct C.

upvoted 1 times

 **rrrrrrrrr1** 2 months, 2 weeks ago

I guess it can't be D because lambda doesn't have a Cors setting. However, there are use-cases where you need to return the cors header inside the lambda return.

"Configure your REST API integrations to return the required CORS headers

Configure your backend AWS Lambda function or HTTP server to send the required CORS headers in its response. Keep in mind the following:"

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

eaasy C

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - use case -> <https://repost.aws/knowledge-center/api-gateway-cors-errors>

upvoted 2 times

 **Alabi** 3 months ago

Selected Answer: C

In this case, when the registration form on the static website (hosted on Amazon S3) is submitted and makes a request to the API Gateway API endpoint, a CORS error occurs. This error indicates that the API response lacks the appropriate Access-Control-Allow-Origin header, which specifies the allowed origin domains for the response.

upvoted 3 times

 **Maria2023** 3 months ago

Selected Answer: A

I vote for A since I was not able for find an option to configure CORS on API gateway plus this information <https://docs.aws.amazon.com/sdk-for-javascript/v2/developer-guide/cors.html>

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

yes you can

Choose the API:

Choose the "Resources" option in the API Gateway console.

In the "Resources" pane, choose the resource you want to enable CORS for.

Choose "Actions" -> "Enable CORS".

C is correct

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: C

Cross-Origin Resource Sharing (CORS) is a security measure that allows or denies scripts on webpages from making requests to a different domain than the one the script came from. The CORS policy is configured on the server side, and servers use the Access-Control-Allow-Origin header to tell the browser which domains are allowed to make requests.

In the scenario provided, the error message is likely occurring because the API Gateway API endpoint used by the static website is not configured to allow www.example.com as an origin for requests.

upvoted 4 times

Question #261

Topic 1

A company has many separate AWS accounts and uses no central billing or management. Each AWS account hosts services for different departments in the company. The company has a Microsoft Azure Active Directory that is deployed.

A solutions architect needs to centralize billing and management of the company's AWS accounts. The company wants to start using identity federation instead of manual user management. The company also wants to use temporary credentials instead of long-lived access keys.

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

- A. Create a new AWS account to serve as a management account. Deploy an organization in AWS Organizations. Invite each existing AWS account to join the organization. Ensure that each account accepts the invitation.
- B. Configure each AWS account's email address to be aws+@example.com so that account management email messages and invoices are sent to the same place.
- C. Deploy AWS IAM Identity Center (AWS Single Sign-On) in the management account. Connect IAM Identity Center to the Azure Active Directory. Configure IAM Identity Center for automatic synchronization of users and groups.
- D. Deploy an AWS Managed Microsoft AD directory in the management account. Share the directory with all other accounts in the organization by using AWS Resource Access Manager (AWS RAM).
- E. Create AWS IAM Identity Center (AWS Single Sign-On) permission sets. Attach the permission sets to the appropriate IAM Identity Center groups and AWS accounts.
- F. Configure AWS Identity and Access Management (IAM) in each AWS account to use AWS Managed Microsoft AD for authentication and authorization.

 **gd1** Highly Voted 3 months ago

Selected Answer: ACE

Yes ACE - A for a new Management account: C for SSO; E for permissions to IAM

upvoted 5 times

 **ggrodsckiy** Most Recent 2 months ago

Correct ACE.

upvoted 1 times

 **Piccaso** 2 months, 2 weeks ago

Selected Answer: ACE

D must be wrong.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: ACE

ACE IT!

upvoted 1 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: ACE

this question scored an ACE

upvoted 1 times

 **SkyZeroZx** 2 months, 4 weeks ago

Selected Answer: ACE

A) Creating a master account to manage organizations on AWS and invite them sounds like a good idea and is recommended.

B) Has no sense

C) In AWS Single Sign On adding Azure AD as trust sounds like a good idea and it is the usual way to do it as well as creating users and groups

D) Create an AD in AWS and share it? it doesn't make sense because there already exists one in azure which we will use

E) Creating the corresponding permission set and attaching it to the groups that were created usually makes sense.

F) again an AD created in AWS is not necessary because it already exists in Azure and you do not want to have another one again

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: ACE

ACE - Management account, AWS SSO with Azure AD and permission sets

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: ACE

Yes ACE - A for a new Management account: C for SSO; E for permissions to IAM
upvoted 1 times

 **PhuocT** 3 months ago

Selected Answer: ACE

A, C and E
upvoted 1 times

 **MoussaNoussa** 3 months ago

ACE is the right answer
upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: ACE

Correct Answer is ACE
upvoted 1 times

Question #262

Topic 1

A company wants to manage the costs associated with a group of 20 applications that are infrequently used, but are still business-critical, by migrating to AWS. The applications are a mix of Java and Node.js spread across different instance clusters. The company wants to minimize costs while standardizing by using a single deployment methodology.

Most of the applications are part of month-end processing routines with a small number of concurrent users, but they are occasionally run at other times. Average application memory consumption is less than 1 GB, though some applications use as much as 2.5 GB of memory during peak processing. The most important application in the group is a billing report written in Java that accesses multiple data sources and often runs for several hours.

Which is the MOST cost-effective solution?

- A. Deploy a separate AWS Lambda function for each application. Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs.
- B. Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling. Monitor services and hosts by using Amazon CloudWatch.
- C. Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have sufficient resources. Monitor each AWS Elastic Beanstalk deployment by using CloudWatch alarms.
- D. Deploy a new Amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancers. Scale cluster size based on a custom metric set on instance memory utilization. Purchase 3-year Reserved Instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group.

 **nexus2020** Highly Voted  3 months ago

Selected Answer: B

Hours = lambda out

Reserve instance max size = D out

C: beanstalk still use EC2, if beanstalk = each application, it could be each app get its own EC2, which will cost more than the ECS on EC2 in B. So B is cheaper

upvoted 7 times

 **softarts** Most Recent  1 month, 1 week ago

Selected Answer: B

B 100% sure

upvoted 1 times

 **ggrodskiy** 2 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

B since the emphasis is on cost, no operational overhead. containers should be a bit more cost-effective as they are more granular per app
a: hours-> no lambda

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B is correct.

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: B

B for sure

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: B

A is incorrect due to lambda 15mins constraint

B is Correct

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

Question #263

Topic 1

A solutions architect needs to review the design of an Amazon EMR cluster that is using the EMR File System (EMRFS). The cluster performs tasks that are critical to business needs. The cluster is running Amazon EC2 On-Demand Instances at all times for all task, primary, and core nodes. The EMR tasks run each morning, starting at 1:00 AM. and take 6 hours to finish running. The amount of time to complete the processing is not a priority because the data is not referenced until late in the day.

The solutions architect must review the architecture and suggest a solution to minimize the compute costs.

Which solution should the solutions architect recommend to meet these requirements?

- A. Launch all task, primary, and core nodes on Spot Instances in an instance fleet. Terminate the cluster, including all instances, when the processing is completed.
- B. Launch the primary and core nodes on On-Demand Instances. Launch the task nodes on Spot Instances in an instance fleet. Terminate the cluster, including all instances, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
- C. Continue to launch all nodes on On-Demand Instances. Terminate the cluster, including all instances, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
- D. Launch the primary and core nodes on On-Demand Instances. Launch the task nodes on Spot Instances in an instance fleet. Terminate only the task node instances when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.

 **FunkyFresco** 20 hours, 26 minutes ago

Selected Answer: B

I will go with B.
upvoted 1 times

 **cmoreira** 3 weeks, 2 days ago

Selected Answer: B

Agreed with santi.
From EMR best practices, Treat all clusters as transient resources.
https://aws.github.io/aws-emr-best-practices/reliability/best_practices/
upvoted 1 times

 **774dayo** 3 weeks, 3 days ago

Selected Answer: B

bbbbbbbbbb
upvoted 1 times

 **Gabehcoud** 3 weeks, 5 days ago

Selected Answer: D

The cluster needs to be present later at the day to serve the data that was processed. So I choose D.
upvoted 3 times

 **aviathor** 4 weeks, 1 day ago

Selected Answer: D

The problem statement says:
"The EMR tasks run each morning, starting at 1:00 AM. and take 6 hours to finish running. The amount of time to complete the processing is not a priority because *the data is not referenced until late in the day.*"

So later in the day, clients will be using the cluster to read data. Therefore my understanding is that core and primary nodes need to be available, but the task nodes can be terminated once the tasks have finished their daily run.

upvoted 3 times

 **SK_Tyagi** 1 month ago

Selected Answer: B

If the core, master nodes had to be running, RI would have been a better choice over On-Demand. Here all nodes need to be terminated
upvoted 1 times

 **vn_thanhung** 3 weeks, 3 days ago

you think need terminate manage node?
upvoted 1 times

 **chico2023** 1 month, 2 weeks ago

Selected Answer: B

Option B. Pretty for what NikkyDicky correctly put in his comment.

upvoted 2 times

 **Asds** 1 month, 3 weeks ago

Selected Answer: B

Option B provides the most cost-effective approach by combining On-Demand Instances for critical nodes with Spot Instances for non-critical task nodes. Additionally, using Compute Savings Plans further optimizes the cost structure for the primary and core node instances

upvoted 1 times

 **ggorodskiy** 2 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

B, not D... minimize means shutdown all. no point of having an idle cluster incur costs

1. data stored through EMRFS on s3 may be referenced directly using s3 APIs
2. it don't take long to launch a (smaller) cluster if it's needed for referencing. then shut it down again
3. not even clear from the documentation task nodes can be scaled down without affecting core nodes
4. savings plan does not mean no cost for idle instances, just less cost

upvoted 4 times

 **vn_thanhaltung** 3 weeks, 3 days ago

you think need terminate manage node?

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: D

Option D provides a cost-effective solution while ensuring the cluster's critical tasks are completed within the desired timeframe

Option B suggests launching primary and core nodes on On-Demand Instances, launching task nodes on Spot Instances, and terminating the entire cluster, including all instances when processing is completed. Although using Spot Instances for task nodes can save costs, terminating the entire cluster would result in longer delays for accessing the data later in the day.

upvoted 4 times

 **santi1975** 2 months ago

Option B.

EMRFS allows you to access its content from a S3 bucket transparently (so decoupling computer from storage). The cluster can be terminated, with all its results safely stored in a S3 bucket... Not sure why it "would result in longer delays for accessing the data later". Please check:

https://aws.github.io/aws-emr-best-practices/reliability/best_practices/

upvoted 3 times

 **itsmeSuren** 2 months, 4 weeks ago

Selected Answer: D

Option D - This is the most cost effective working solution.

Not Option B - This is also a workable solution, but it will be expensive than D. So D is the best option.

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: D

Correct Answer is D. In B it has no sense to terminate primary instance if we have already purchase a saving plan.

upvoted 2 times

 **nexus2020** 2 months, 4 weeks ago

Selected Answer: B

If the question is asking about which is the highest availability option, then D.

But the question is asking about which is the cheapest, therefore B. B might not be the best, but does fit for the requirement (min cost).

regarding the delay on starting instances, instance scheduler can be used to start the instance at defined time before 1AM.

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: D

D - the cluster is used all the time, EMR is used between 1AM and 7AM.

B - doesn't make sense. Why would you terminate on-demand instances if you already paid for the savings plan.

upvoted 4 times

 **nexus2020** 2 months, 4 weeks ago

compute savings plan \$ amount is mentioned, so we can not assume the savings plan is very big and we can leave the on-demand instances running when there is no load. if savings plan is \$10, then when on-demand running it cost \$20, then it make sense to turn them off when the tasks are done, as \$10 savings plan will not cover the \$20 on-demand cost.

Key word in B: turn off when "the processing is completed".no point to keep things running when work is done

upvoted 1 times

 **rxhan** 2 months, 3 weeks ago

you turn off the task node when complete and use again in the morning, its critical

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: D

Option D provides a cost-effective solution while ensuring the cluster's critical tasks are completed within the desired timeframe

Option B suggests launching primary and core nodes on On-Demand Instances, launching task nodes on Spot Instances, and terminating the entire cluster, including all instances when processing is completed. Although using Spot Instances for task nodes can save costs, terminating the entire cluster would result in longer delays for accessing the data later in the day.

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: B

GPT: EMR cluster is composed of one master node, core nodes, and optional task nodes. The master node manages the cluster and runs the YARN ResourceManager service, JobHistory Server, and the Hadoop MapReduce and Spark schedulers. Core nodes are managed by the master node and run the YARN NodeManager daemon and the Hadoop Distributed File System (HDFS) DataNode daemon. Task nodes are optional and can be added to a cluster to perform tasks, but do not contain the HDFS DataNode daemon.

Because the master and core nodes are critical for the functioning of the EMR cluster, they should be run on On-Demand Instances to ensure they do not get terminated due to Spot Instance price fluctuations.

upvoted 1 times

Question #264

Topic 1

A company has migrated a legacy application to the AWS Cloud. The application runs on three Amazon EC2 instances that are spread across three Availability Zones. One EC2 instance is in each Availability Zone. The EC2 instances are running in three private subnets of the VPC and are set up as targets for an Application Load Balancer (ALB) that is associated with three public subnets.

The application needs to communicate with on-premises systems. Only traffic from IP addresses in the company's IP address range are allowed to access the on-premises systems. The company's security team is bringing only one IP address from its internal IP address range to the cloud. The company has added this IP address to the allow list for the company firewall. The company also has created an Elastic IP address for this IP address.

A solutions architect needs to create a solution that gives the application the ability to communicate with the on-premises systems. The solution also must be able to mitigate failures automatically.

Which solution will meet these requirements?

- A. Deploy three NAT gateways, one in each public subnet. Assign the Elastic IP address to the NAT gateways. Turn on health checks for the NAT gateways. If a NAT gateway fails a health check, recreate the NAT gateway and assign the Elastic IP address to the new NAT gateway.
- B. Replace the ALB with a Network Load Balancer (NLB). Assign the Elastic IP address to the NLB. Turn on health checks for the NLB. In the case of a failed health check, redeploy the NLB in different subnets.
- C. Deploy a single NAT gateway in a public subnet. Assign the Elastic IP address to the NAT gateway. Use Amazon CloudWatch with a custom metric to monitor the NAT gateway. If the NAT gateway is unhealthy, invoke an AWS Lambda function to create a new NAT gateway in a different subnet. Assign the Elastic IP address to the new NAT gateway.
- D. Assign the Elastic IP address to the ALB. Create an Amazon Route 53 simple record with the Elastic IP address as the value. Create a Route 53 health check. In the case of a failed health check, recreate the ALB in different subnets.

 **AMohanty** 1 month ago

Isn't NAT Gateway AWS managed
Why do we need to check if NAT GW is healthy ?
upvoted 2 times

 **ggrodsckiy** 2 months ago

Correct C.
upvoted 1 times

 **study_aws1** 2 months, 1 week ago

All seemed good for option C) till I encountered this sentence - "The company's security team is bringing only one IP address from its internal IP address range to the cloud." - Please note internal IP not external IP. Which seems to imply there is a connectivity between on-premises & Cloud (either through Site-to-Site VPN or DX), though not explicitly mentioned in the question.

In such a case, NAT gateway with Public subnet will not help. Option B) will become a viable solution in this case.

upvoted 1 times

 **chikorita** 1 month ago

Elastic IPs itself are public
whether you choose B or C
Option C is perfect for this use-case unless you associate ALB as target for NLB
upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C
C makes some sense
upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C
C - single NAT if only one Elastic IP is available.
upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: C
option C provides the most appropriate solution by using a single NAT gateway, monitoring its health with CloudWatch, and invoking a Lambda function to create a new NAT gateway if necessary.
upvoted 1 times

✉  **shree2023** 3 months ago

Selected Answer: C

C is the answer single NAT is needed

upvoted 1 times

✉  **PhuocT** 3 months ago

I think it's C.

upvoted 1 times

✉  **bhanus** 3 months ago

Selected Answer: C

I go with C

A is incorrect because you dont need 3 nat gateways

B does not make sense to replace ALB

D - you cannot assign elastic ip to ALB

upvoted 2 times

✉  **gd1** 3 months ago

A NAT (Network Address Translation) Gateway enables instances in a private subnet to connect to the internet or other AWS services but prevents the internet from initiating a connection with those instances. By using a single NAT gateway with the provided Elastic IP address, all outbound traffic will appear to come from the single, whitelisted IP address that the company allows.

upvoted 2 times

✉  **psyx21** 3 months, 1 week ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #265

Topic 1

A company uses AWS Organizations to manage more than 1,000 AWS accounts. The company has created a new developer organization. There are 540 developer member accounts that must be moved to the new developer organization. All accounts are set up with all the required information so that each account can be operated as a standalone account.

Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization? (Choose three.)

- A. Call the MoveAccount operation in the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization.
- B. From the management account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.
- C. From each developer account, remove the account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.
- D. Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration.
- E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's management account to send invitations to the developer accounts.
- F. Have each developer sign in to their account and confirm to join the new developer organization.

✉  **SmileyCloud** Highly Voted 3 months ago

Selected Answer: BEF

B - Remove
E - Invite
F - Verify
<https://repost.aws/knowledge-center/organizations-move-accounts>
upvoted 6 times

✉  **Khannas** 1 month, 1 week ago

Excellent Explanation
upvoted 2 times

✉  **khksoma** Most Recent 2 months ago

BEF is correct.
<https://aws.amazon.com/blogs/mt/aws-organizations-moving-an-organization-member-account-to-another-organization-part-1/#:~:text=Moving%20an%20account%20between%20organizations,and%20services%20continue%20to%20operate.>
upvoted 1 times

✉  **ggrodsckiy** 2 months ago

correct BEF.
upvoted 1 times

✉  **Jonalb** 2 months, 2 weeks ago

Selected Answer: BEF
its BEF
upvoted 1 times

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

Selected Answer: BEF
its BEF
upvoted 1 times

✉  **nexus2020** 3 months ago

Selected Answer: BEF
remove from org, invite from org, verify from individual. BEF
upvoted 1 times

✉  **gd1** 3 months ago

Selected Answer: BEF
GPT 4.0 corrected BEF are the answers. A is not feasible.
upvoted 2 times

✉  **gd1** 3 months ago

Selected Answer: AEF

GPT: In AWS Organizations, moving an account to a new organization is a two-step process. First, the account has to be removed from the old organization. This can be done using the MoveAccount operation from the old organization's management account (Option A). Second, the account has to be invited to the new organization. The new organization's management account should use the InviteAccountToOrganization operation to send an invitation to the account (Option E). Finally, to accept the invitation to join a new organization, the account owner (in this case, each developer) must sign in to their account and accept the invitation (Option F).

upvoted 1 times

 **gd1** 3 months ago

GPT corrected BEF are the answers.

upvoted 2 times

 **i_am_robot** 3 months ago

Selected Answer: ABF

To move an account between organizations, you need to remove the account from the current organization (using RemoveAccountFromOrganization) and then the individual account holders must accept an invitation to join the new organization (using the MoveAccount operation and then manually confirming the invitation to join the new organization).

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: BEF

A is incorrect not an option to MoveOperation not across org
B - remove account from org

E - Invite the dev account
F - Confirm

upvoted 1 times

 **PhuocT** 3 months ago

B, E, and F, I think

upvoted 1 times

 **Jackhemo** 3 months ago

Selected Answer: BDE

olabiba.ai says BDE

upvoted 1 times

 **rxhan** 1 month, 3 weeks ago

olabiba.ai is wrong

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: BEF

I go with BEF

<https://aws.amazon.com/blogs/mt/aws-organizations-moving-an-organization-member-account-to-another-organization-part-1/>
The above doc clearly says "Moving an account between organizations requires you to remove the account from an organization, making the account standalone, and then you accepting an invite to join another organization"

A is incorrect as per above statement

B Correct

C is incorrect because individual account cannot remove itself from an organization. This operation must be performed by the management account of the organization.

D is incorrect because there is NO need for placeholder

E is correct . The management account should INVITE its member account

F is correct - The member account should ACCEPT invitation

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: BDE

Correct Answer is BDE

upvoted 1 times

Question #266

Topic 1

A company's interactive web application uses an Amazon CloudFront distribution to serve images from an Amazon S3 bucket. Occasionally, third-party tools ingest corrupted images into the S3 bucket. This image corruption causes a poor user experience in the application later. The company has successfully implemented and tested Python logic to detect corrupt images.

A solutions architect must recommend a solution to integrate the detection logic with minimal latency between the ingestion and serving.

Which solution will meet these requirements?

- A. Use a Lambda@Edge function that is invoked by a viewer-response event.
- B. Use a Lambda@Edge function that is invoked by an origin-response event.
- C. Use an S3 event notification that invokes an AWS Lambda function.
- D. Use an S3 event notification that invokes an AWS Step Functions state machine.

 **i_am_robot** Highly Voted 3 months ago

Selected Answer: C

The requirement here is to catch and deal with the corruption at the time of ingestion. Hence, the logical place to put the check would be where the ingestion is actually happening, which is when the image is put into the S3 bucket. Amazon S3 can be configured to send an event notification when a new object is created (i.e., put into the bucket). This event can then trigger a Lambda function that uses the Python logic to check the image for corruption. This way, you are catching and dealing with any issues as soon as the image is ingested.

upvoted 6 times

 **NikkyDicky** Most Recent 2 months, 2 weeks ago

Selected Answer: C

its a C

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: C

Take care of corrupted images as soon as they get uploaded to S3

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: C

D is for more complex and multiple sets of Lambda.

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: C

A&B is too late, D is unnecessary

C is correct

upvoted 2 times

 **PhuocT** 3 months ago

C is correct.

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #267

Topic 1

A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application. The instances that run in the Auto Scaling group are constantly changing because of scaling events.

When the company deploys new application code versions, the company installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group. The application is set to go live within the next 24 hours.

What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?

- A. Configure Amazon EventBridge to invoke an AWS Lambda function when a new EC2 instance is launched into the Auto Scaling group. Code the Lambda function to associate the EC2 instances with the CodeDeploy deployment group.
- B. Write a script to suspend Amazon EC2 Auto Scaling operations before the deployment of new code. When the deployment is complete, create a new AMI and configure the Auto Scaling group's launch template to use the new AMI for new launches. Resume Amazon EC2 Auto Scaling operations.
- C. Create a new AWS CodeBuild project that creates a new AMI that contains the new code. Configure CodeBuild to update the Auto Scaling group's launch template to the new AMI. Run an Amazon EC2 Auto Scaling instance refresh operation.
- D. Create a new AMI that has the CodeDeploy agent installed. Configure the Auto Scaling group's launch template to use the new AMI. Associate the CodeDeploy deployment group with the Auto Scaling group instead of the EC2 instances.

 **Ganshank** 4 weeks ago

D as per this rather old blog post - <https://aws.amazon.com/blogs/devops/under-the-hood-aws-codedeploy-and-auto-scaling-integration/>
upvoted 1 times

 **aviathor** 4 weeks ago

It seems really unnecessary to have to install an app on the fly during scale-out of an ASG. Just launching the EC2 instances from a pre-installed AMI is so much faster, and removes sources of error.

I am a little frustrated never to have encountered AWS Image Builder in a question, or in course material...

upvoted 1 times

 **aviathor** 4 weeks ago

<https://dev.to/aws-builders/how-to-create-a-custom-ami-with-image-pipeline-and-automate-its-creation-using-ec2-image-builder-108m>
upvoted 1 times

 **Simon523** 4 weeks, 1 day ago

Selected Answer: D

AWS CodeDeploy is a deployment service that enables developers to automate the deployment of applications to instances and to update the applications as required.

upvoted 1 times

 **rxhan** 1 month, 3 weeks ago

Selected Answer: D

Bake AMI with agent already installed

upvoted 1 times

 **achillestasan** 2 months, 1 week ago

Selected Answer: C

D is not correct since it is considering about the code change.

upvoted 1 times

 **rxhan** 1 month, 3 weeks ago

CodeBuild cant create a new AMI?

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: D

It's a D

upvoted 1 times

 **SmileyCloud** 3 months ago

D - correct. You want the agent baked in the AMI.

upvoted 2 times

 **Alabi** 3 months ago

Selected Answer: D

This solution automates the deployment process by creating a new Amazon Machine Image (AMI) with the CodeDeploy agent installed. The Auto Scaling group's launch template is then updated to use this new AMI. By associating the CodeDeploy deployment group with the Auto Scaling group, CodeDeploy will automatically deploy the application to any new instances launched by the Auto Scaling group.

This approach eliminates the need to manually install the CodeDeploy agent on new instances and associate them with the deployment group. It simplifies the deployment process and reduces operational overhead by leveraging the automation capabilities of CodeDeploy and the Auto Scaling group.

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: D

GPT: This option provides the least amount of operational overhead by associating the CodeDeploy deployment group with the Auto Scaling group rather than individual EC2 instances. This enables any new instances launched by the Auto Scaling group to be automatically included in deployments, eliminating the need for manual intervention or additional automation to add new instances to the deployment group. The creation of an AMI with the CodeDeploy agent pre-installed ensures that all new instances launched by the Auto Scaling group will have the necessary components to participate in CodeDeploy deployments.

upvoted 3 times

 **psyx21** 3 months, 1 week ago

Selected Answer: D

Correct Answer is D

upvoted 2 times

Question #268

Topic 1

A company has a website that runs on four Amazon EC2 instances that are behind an Application Load Balancer (ALB). When the ALB detects that an EC2 instance is no longer available, an Amazon CloudWatch alarm enters the ALARM state. A member of the company's operations team then manually adds a new EC2 instance behind the ALB.

A solutions architect needs to design a highly available solution that automatically handles the replacement of EC2 instances. The company needs to minimize downtime during the switch to the new solution.

Which set of steps should the solutions architect take to meet these requirements?

- A. Delete the existing ALB. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Attach the existing EC2 instances to the Auto Scaling group.
- B. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALB. Attach the existing EC2 instances to the Auto Scaling group.
- C. Delete the existing ALB and the EC2 instances. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Wait for the Auto Scaling group to launch the minimum number of EC2 instances.
- D. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALB. Wait for the existing ALB to register the existing EC2 instances with the Auto Scaling group.

 **SK_Tyagi** 1 month ago

Selected Answer: B

Deleting the ALB will increase downtime, so A & C eliminated. B & D are similar but D suggests wait for ALB to register EC2 instances, again causing delay so eliminated

upvoted 3 times

 **ggrodsckiy** 2 months ago

Correct B

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

its a B

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B - correct. Attach the EC2s

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

New AS Group - assign to existing ALB and attach EC2s to new Scaling group.

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: B

New AS Group - assign to existing ALB and attach EC2s to new Scaling group.

upvoted 2 times

 **i_am_robot** 3 months ago

Selected Answer: B

Auto Scaling groups are designed to ensure that you are running your desired number of Amazon EC2 instances. It also can automatically replace any instances that fail or are unhealthy based on health checks. You can specify the minimum, maximum, and desired number of instances in your Auto Scaling group. By attaching a new launch template to the Auto Scaling group, the Auto Scaling group knows what configuration to use for the new instances it launches.

There's no need to delete the existing ALB as suggested in options A and C. The ALB is still functional and will work with the newly created Auto Scaling group. You can directly attach the Auto Scaling group to the existing ALB.

upvoted 3 times

 **psyx21** 3 months, 1 week ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

Question #269

Topic 1

A company wants to optimize AWS data-transfer costs and compute costs across developer accounts within the company's organization in AWS Organizations. Developers can configure VPCs and launch Amazon EC2 instances in a single AWS Region. The EC2 instances retrieve approximately 1 TB of data each day from Amazon S3.

The developer activity leads to excessive monthly data-transfer charges and NAT gateway processing charges between EC2 instances and S3 buckets, along with high compute costs. The company wants to proactively enforce approved architectural patterns for any EC2 instance and VPC infrastructure that developers deploy within the AWS accounts. The company does not want this enforcement to negatively affect the speed at which the developers can perform their tasks.

Which solution will meet these requirements MOST cost-effectively?

- A. Create SCPs to prevent developers from launching unapproved EC2 instance types. Provide the developers with an AWS CloudFormation template to deploy an approved VPC configuration with S3 interface endpoints. Scope the developers' IAM permissions so that the developers can launch VPC resources only with CloudFormation.
- B. Create a daily forecasted budget with AWS Budgets to monitor EC2 compute costs and S3 data-transfer costs across the developer accounts. When the forecasted cost is 75% of the actual budget cost, send an alert to the developer teams. If the actual budget cost is 100%, create a budget action to terminate the developers' EC2 instances and VPC infrastructure.
- C. Create an AWS Service Catalog portfolio that users can use to create an approved VPC configuration with S3 gateway endpoints and approved EC2 instances. Share the portfolio with the developer accounts. Configure an AWS Service Catalog launch constraint to use an approved IAM role. Scope the developers' IAM permissions to allow access only to AWS Service Catalog.
- D. Create and deploy AWS Config rules to monitor the compliance of EC2 and VPC resources in the developer AWS accounts. If developers launch unapproved EC2 instances or if developers create VPCs without S3 gateway endpoints, perform a remediation action to terminate the unapproved resources.

 **Sweetedad** 3 weeks, 4 days ago

Why not D?

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

C works

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - let the devs choose what they want but they still adhere to standards. Service catalog does that.

upvoted 1 times

 **SkyZeroXz** 3 months ago

Selected Answer: C

C is correct. Service catalog solves all issues.

S3 Gateway endpoint more cost effective with data transfer in VPC on AWS

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: C

C is correct. Service catalog solves all issues.

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: C

C is the effective way.

A is incorrect because it can allow users to create resources that are defined outside of CloudFormation

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #270

Topic 1

A company is expanding. The company plans to separate its resources into hundreds of different AWS accounts in multiple AWS Regions. A solutions architect must recommend a solution that denies access to any operations outside of specifically designated Regions.

Which solution will meet these requirements?

- A. Create IAM roles for each account. Create IAM policies with conditional allow permissions that include only approved Regions for the accounts.
- B. Create an organization in AWS Organizations. Create IAM users for each account. Attach a policy to each user to block access to Regions where an account cannot deploy infrastructure.
- C. Launch an AWS Control Tower landing zone. Create OUs and attach SCPs that deny access to run services outside of the approved Regions.
- D. Enable AWS Security Hub in each account. Create controls to specify the Regions where an account can deploy infrastructure.

 **Gabehcoud** 1 month ago

my bad, "attach a policy to each user" its a tedious tasks. ignore my previous message.

upvoted 1 times

 **Gabehcoud** 1 month ago

can someone please detail why the answer cannot be B?

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

its a C

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

AWS Org, Control Tower and SCPs.

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: C

C for sure

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: C

Control Tower with SCP (deny) solves the issues

upvoted 2 times

 **bhanus** 3 months ago

Selected Answer: C

C is the answer

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #271

Topic 1

A company wants to refactor its retail ordering web application that currently has a load-balanced Amazon EC2 instance fleet for web hosting, database API services, and business logic. The company needs to create a decoupled, scalable architecture with a mechanism for retaining failed orders while also minimizing operational costs.

Which solution will meet these requirements?

- A. Use Amazon S3 for web hosting with Amazon API Gateway for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use Amazon Elastic Container Service (Amazon ECS) for business logic with Amazon SQS long polling for retaining failed orders.
- B. Use AWS Elastic Beanstalk for web hosting with Amazon API Gateway for database API services. Use Amazon MQ for order queuing. Use AWS Step Functions for business logic with Amazon S3 Glacier Deep Archive for retaining failed orders.
- C. Use Amazon S3 for web hosting with AWS AppSync for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use AWS Lambda for business logic with an Amazon SQS dead-letter queue for retaining failed orders.
- D. Use Amazon Lightsail for web hosting with AWS AppSync for database API services. Use Amazon Simple Email Service (Amazon SES) for order queuing. Use Amazon Elastic Kubernetes Service (Amazon EKS) for business logic with Amazon OpenSearch Service for retaining failed orders.

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

C

A would work with Lambda/SQS vs ECS/SQS

upvoted 1 times

 **SkyZeroZx** 2 months, 4 weeks ago

Selected Answer: C

S3 + Appsync DB API (Manged service) and SQS and Deal letter queue for failed orders

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - You don't use "Amazon SQS long polling for retaining failed orders"

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: C

Option C combines Amazon S3 for web hosting, AWS AppSync for database API services, and AWS Lambda for business logic. This combination provides a decoupled and scalable architecture. Using Amazon SQS for order queuing ensures reliable message delivery, and utilizing an SQS dead-letter queue allows for retaining failed orders. This solution meets the requirements of the scenario while minimizing operational costs

upvoted 2 times

 **nexus2020** 3 months ago

Selected Answer: C

C is a good answer, but is it the cheapest? hard to tell

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: A

Checking a bit more for AWS AppSync - AWS AppSync enables developers to connect their applications and services to data and events with secure, serverless and high-performing GraphQL and Pub/Sub APIs. GraphQL is an open-source query language that describes how a client should request information through an API

I don't believe this is the intent of the exercise here by saying "Database API"

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: C

S3 + Appsync DB API (Manged service) and SQS and Deal letter queue for failed orders

upvoted 2 times

 **MoussaNoussa** 3 months ago

Correct Answer is C

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #272

Topic 1

A company hosts a web application on AWS in the us-east-1 Region. The application servers are distributed across three Availability Zones behind an Application Load Balancer. The database is hosted in a MySQL database on an Amazon EC2 instance. A solutions architect needs to design a cross-Region data recovery solution using AWS services with an RTO of less than 5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west-2, and has configured Amazon Route 53 health checks and DNS failover to us-west-2.

Which additional step should the solutions architect take?

- A. Migrate the database to an Amazon RDS for MySQL instance with a cross-Region read replica in us-west-2.
- B. Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2.
- C. Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment.
- D. Create a MySQL standby database on an Amazon EC2 instance in us-west-2.

 **vjp_training** 1 month, 1 week ago

Selected Answer: B

B is correct. RTO of A is Usually minutes, not sure will be less than 5p

<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html>

upvoted 2 times

 **softarts** 1 month, 2 weeks ago

Selected Answer: B

but A also meet requirement actually according to <https://aws.amazon.com/blogs/database/how-to-choose-the-best-disaster-recovery-option-for-your-amazon-aurora-mysql-cluster/>

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

B for Baurora

upvoted 2 times

 **shree2023** 3 months ago

Selected Answer: B

B global database is correct

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: B

B- Aurora provides the minimum RTO and RPO (1 min)

upvoted 3 times

 **bhanus** 3 months ago

Selected Answer: B

B Aurora is the right choice

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

Question #273

Topic 1

A company is using AWS Organizations to manage multiple accounts. Due to regulatory requirements, the company wants to restrict specific member accounts to certain AWS Regions, where they are permitted to deploy resources. The resources in the accounts must be tagged, enforced based on a group standard, and centrally managed with minimal configuration.

What should a solutions architect do to meet these requirements?

- A. Create an AWS Config rule in the specific member accounts to limit Regions and apply a tag policy.
- B. From the AWS Billing and Cost Management console, in the management account, disable Regions for the specific member accounts and apply a tag policy on the root.
- C. Associate the specific member accounts with the root. Apply a tag policy and an SCP using conditions to limit Regions.
- D. Associate the specific member accounts with a new OU. Apply a tag policy and an SCP using conditions to limit Regions.

 **ggrodskiy** 2 months ago

Correct D.

upvoted 1 times

 **Don2021** 2 months, 2 weeks ago

Selected Answer: D

D will only apply to the specific account in the new OU while C will apply SCP to the whole accounts with the organization

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: D

easy D

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: D

D - Correct. SCPs applied to OU.

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: D

D is correct

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: D

OU and SCP to have Tags and regions denied

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: D

Correct Answer is D

upvoted 1 times

Question #274

Topic 1

A company has an application that generates reports and stores them in an Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.

Which set of actions will immediately remediate the security issue without impacting the application's normal workflow?

- A. Create an AWS Lambda function that applies a deny all policy for users who are not authenticated. Create a scheduled event to invoke the Lambda function.
- B. Review the AWS Trusted Advisor bucket permissions check and implement the recommended actions.
- C. Run a script that puts a private ACL on all of the objects in the bucket.
- D. Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket.

 **rxhan** 1 month, 3 weeks ago

Script is never AWS answers
upvoted 2 times

 **ggrodsckiy** 2 months ago

Correct D.
Uses the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket. This would immediately block public access to the files in the S3 bucket without affecting the application's normal workflow. The application can still generate signed URLs to allow users to download their reports. The IgnorePublicAcls setting ignores any public ACLs on objects in this bucket and any objects that are added to this bucket in the future.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: D
its a D
upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: D
D - yank the cable from the switch. Check this -> <https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html>
upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: D
D is the most appropriate solution as it directly addresses the security issue by using the Block Public Access feature in Amazon S3. By setting the IgnorePublicAcls option to TRUE, it ensures that public access to the bucket and its objects is blocked, preventing unauthorized downloads. This solution is immediate, doesn't require modifying the application code or workflow, and provides an effective security control.
upvoted 1 times

 **easystoo** 3 months ago

d-d-d-d-d
upvoted 1 times

 **nexus2020** 3 months ago

IF the purpose is block pre-signed URL access to bucket, none of the options will work.

If we are just blocking non pre-signed URL access, then both C and D will work.

Correct me if I am wrong here.

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: C
C indeed
upvoted 1 times

 **gd1** 3 months ago

Selected Answer: D
Amazon S3 Block Public Access provides settings for access points, buckets, and accounts to help you manage public access to Amazon S3 resources. By default, new buckets, access points, and objects don't allow public access, but users or applications can modify bucket policies or object permissions to allow public access. S3 Block Public Access settings override these public access settings. You can use S3 Block Public Access to block existing public access, whether specified by an ACL or a policy, and to ensure that public access isn't granted to newly created

items. Using signed URLs to grant temporary access to the S3 objects is a secure way to share files. It allows the company to continue using their current workflow without affecting its users while also maintaining the privacy and security of the files in the bucket.

upvoted 2 times

 **PhuocT** 3 months ago

Selected Answer: D

D - Block Public Access feature in Amazon S3 to set the IgnorePublicAcls

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #275

Topic 1

A company is planning to migrate an Amazon RDS for Oracle database to an RDS for PostgreSQL DB instance in another AWS account. A solutions architect needs to design a migration strategy that will require no downtime and that will minimize the amount of time necessary to complete the migration. The migration strategy must replicate all existing data and any new data that is created during the migration. The target database must be identical to the source database at completion of the migration process.

All applications currently use an Amazon Route 53 CNAME record as their endpoint for communication with the RDS for Oracle DB instance. The RDS for Oracle DB instance is in a private subnet.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Create a new RDS for PostgreSQL DB instance in the target account. Use the AWS Schema Conversion Tool (AWS SCT) to migrate the database schema from the source database to the target database.
- B. Use the AWS Schema Conversion Tool (AWS SCT) to create a new RDS for PostgreSQL DB instance in the target account with the schema and initial data from the source database.
- C. Configure VPC peering between the VPCs in the two AWS accounts to provide connectivity to both DB instances from the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account.
- D. Temporarily allow the source DB instance to be publicly accessible to provide connectivity from the VPC in the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account.
- E. Use AWS Database Migration Service (AWS DMS) in the target account to perform a full load plus change data capture (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint.
- F. Use AWS Database Migration Service (AWS DMS) in the target account to perform a change data capture (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint.

 **SmileyCloud** Highly Voted  3 months ago

Selected Answer: ACE

ace - correct
 b - AWS SCT can't create RDS
 d - never make anything publicly accessible even if temporary
 f - you need initial data, not just changes
 upvoted 6 times

 **ggrodsckiy** Most Recent  2 months ago

Correct ACE.
 upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: ACE

ACE it
 upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: ACE

ACE are correct
 B is incorrect because SCT cannot create RDS instance
 upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: ACE

<https://docs.aws.amazon.com/dms/latest/sbs/chap-oracle-postgresql.migration-process.data-migration.html>
 upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: ACE

ACE is correct
 upvoted 1 times

 **gd1** 3 months ago

Selected Answer: ACE

A. Use SCT; C- Peering; E - DMS with full and change

upvoted 1 times

 **PhuocT** 3 months ago

A, C and E

upvoted 1 times

 **jubileu84** 3 months ago

Correct Answer is ACE

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: ACE

ACE are correct

B is incorrect because SCT cannot create RDS instance

upvoted 3 times

 **MoussaNoussa** 3 months ago

Correct Answer is ACE

upvoted 3 times

 **psyx21** 3 months, 1 week ago

Selected Answer: BEF

Correct Answer is BEF

upvoted 1 times

Question #276

Topic 1

A company has implemented an ordering system using an event-driven architecture. During initial testing, the system stopped processing orders. Further log analysis revealed that one order message in an Amazon Simple Queue Service (Amazon SQS) standard queue was causing an error on the backend and blocking all subsequent order messages. The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds. A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages.

Which step should the solutions architect take to meet these requirements?

- A. Increase the backend processing timeout to 30 seconds to match the visibility timeout.
- B. Reduce the visibility timeout of the queue to automatically remove the faulty message.
- C. Configure a new SQS FIFO queue as a dead-letter queue to isolate the faulty messages.
- D. Configure a new SQS standard queue as a dead-letter queue to isolate the faulty messages.

 **ggrodskiy** 2 months ago

Correct D.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: D

it's a D

upvoted 1 times

 **rxhan** 2 months, 3 weeks ago

Selected Answer: D

The dead-letter queue of a FIFO queue must also be a FIFO queue. Similarly, the dead-letter queue of a standard queue must also be a standard queue.

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: D

It's D - can't be C because the queue is standard queue.

"The dead-letter queue of a FIFO queue must also be a FIFO queue. Similarly, the dead-letter queue of a standard queue must also be a standard queue."

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

upvoted 4 times

 **Jonalb** 3 months ago

Selected Answer: C

Configuring a new SQS standard queue as a dead-letter queue (option D) is not the best choice in this scenario because a standard queue does not provide the strict ordering and exactly-once processing semantics needed for isolating faulty messages. The use of a FIFO queue ensures that the ordering of messages is preserved, which is crucial for troubleshooting and analysis.

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: C

C

its a C

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: D

It's D - can't be C because the queue is standard queue.

"The dead-letter queue of a FIFO queue must also be a FIFO queue. Similarly, the dead-letter queue of a standard queue must also be a standard queue."

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

upvoted 2 times

 **SkyZeroZx** 3 months ago

Selected Answer: D

D dead letter queu

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: D

D indeed
C incorrect FIFO will slow down the process
upvoted 1 times

 **gd1** 3 months ago

Selected Answer: D
SQS - dead letter queue is designed for failures and needs to be addressed by the developers. We use it all teh time.
upvoted 1 times

 **i_am_robot** 3 months ago

Selected Answer: D
Amazon Simple Queue Service (SQS) allows you to set up Dead-Letter Queues (DLQs) to isolate messages that can't be processed correctly. This option is useful when you want to set aside and isolate messages that can't be processed (consumed) successfully to examine them later. When using standard queues, the DLQ should also be a standard queue.
upvoted 1 times

 **PhuocT** 3 months ago

Yep, D.
upvoted 1 times

 **jubileu84** 3 months ago

D is the right answer
upvoted 1 times

 **MoussaNoussa** 3 months ago

D is the right answer
upvoted 2 times

 **planedefiler** 3 months ago

DLQ for Standard Queue should be Standard DLQ
upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C
Correct Answer is C
upvoted 1 times

Question #277

Topic 1

A company has automated the nightly retraining of its machine learning models by using AWS Step Functions. The workflow consists of multiple steps that use AWS Lambda. Each step can fail for various reasons, and any failure causes a failure of the overall workflow.

A review reveals that the retraining has failed multiple nights in a row without the company noticing the failure. A solutions architect needs to improve the workflow so that notifications are sent for all types of failures in the retraining process.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Create an Amazon Simple Notification Service (Amazon SNS) topic with a subscription of type "Email" that targets the team's mailing list.
- B. Create a task named "Email" that forwards the input arguments to the SNS topic.
- C. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": ["States.ALL"] and "Next": "Email".
- D. Add a new email address to Amazon Simple Email Service (Amazon SES). Verify the email address.
- E. Create a task named "Email" that forwards the input arguments to the SES email address.
- F. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": ["States.Runtime"] and "Next": "Email".

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: ABC

simple as ABC

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: ABC

ABC is the right answer

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: ABC

ABC

D, E - SES - not good

F - States.runtime, doesn't catch all errors

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: ABC

"notifications are sent for all types of failures in the retraining process" - that means States.ALL. The rest is common sense.

<https://docs.aws.amazon.com/step-functions/latest/dg/concepts-error-handling.html>

upvoted 3 times

 **gd1** 3 months ago

Selected Answer: ABC

From GPT 4 now - Changed to ABC - A to create SNS, Create a task named "Email" that forwards the input arguments to the SNS topic.C for Errorr- F is bad since "States.Runtime" is not correct.

upvoted 2 times

 **shree2023** 3 months ago

Selected Answer: ABC

ABC is correct

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: ACE

GPT 4.0 is more accurate than 3.5. But has a limit. A is to create SNS; C to create a Task -This step adds error handling to the states in the workflow. If any step fails, the workflow will transition to the "Email" task to send a notification. E. Create a task named "Email" that forwards the input arguments to the SNS email address. E This step creates an AWS Lambda function or an AWS Step Functions task that sends an email notification using the SNS topic created in step A.

upvoted 1 times

 **i_am_robot** 3 months ago

Selected Answer: ABC

In AWS Step Functions, each state reports heartbeat failure, timeout failure, and all other types of failures. Therefore, to catch all errors, the solutions architect should add a Catch field to all Task, Map, and Parallel states with a statement of "ErrorEquals": ["States.ALL"], and "Next": "Email".

Then, a task named "Email" can be created to forward the input arguments to an SNS topic that sends notifications to the team's email.

upvoted 1 times

 **PhuocT** 3 months ago

A, B and C

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: ABC

ABC are right

DE are incorrect because SES cannot be used here. SES can be good for Bulk/Marketing emails

F is incorrect because the error type "States.Runtime" doesn't catch all types of errors. The question asks "notifications are sent for all types of failures"

upvoted 2 times

 **MoussaNoussa** 3 months ago

ABC is the right answer

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: ACF

Correct Answer is ACF

upvoted 1 times

Question #278

Topic 1

A company plans to deploy a new private intranet service on Amazon EC2 instances inside a VPC. An AWS Site-to-Site VPN connects the VPC to the company's on-premises network. The new service must communicate with existing on-premises services. The on-premises services are accessible through the use of hostnames that reside in the company.example DNS zone. This DNS zone is wholly hosted on premises and is available only on the company's private network.

A solutions architect must ensure that the new service can resolve hostnames on the company.example domain to integrate with existing services.

Which solution meets these requirements?

- A. Create an empty private zone in Amazon Route 53 for company.example. Add an additional NS record to the company's on-premises company.example zone that points to the authoritative name servers for the new private zone in Route 53.
- B. Turn on DNS hostnames for the VPC. Configure a new outbound endpoint with Amazon Route 53 Resolver. Create a Resolver rule to forward requests for company.example to the on-premises name servers.
- C. Turn on DNS hostnames for the VPC. Configure a new inbound resolver endpoint with Amazon Route 53 Resolver. Configure the on-premises DNS server to forward requests for company.example to the new resolver.
- D. Use AWS Systems Manager to configure a run document that will install a hosts file that contains any required hostnames. Use an Amazon EventBridge rule to run the document when an instance is entering the running state.

 **bhanus** Highly Voted 3 months ago

Selected Answer: B

Outbound resolver endpoints will let you query your onprem DNS
Inbound resolver endpoints will let your onprem DNS server to query the AWS VPC DNS server
upvoted 5 times

 **gd1** 3 months ago

Option B leverages Amazon Route 53 Resolver to handle DNS resolution between the VPC and the on-premises network. By turning on DNS hostnames for the VPC, the EC2 instances will have DNS resolution capabilities. Setting up an outbound endpoint with Route 53 Resolver enables the VPC to resolve DNS queries for external domains. Creating a Resolver rule specifically for the company.example domain allows forwarding of requests for that domain to the on-premises name servers.

upvoted 2 times

 **SK_Tyagi** Most Recent 1 month ago

Selected Answer: B

bhanus explanation spot on
upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

B for sure
upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: B

b
its a B
upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B - Outbound.
<https://catalog.us-east-1.prod.workshops.aws/workshops/b4a4be0e-d4f9-4ff5-af82-ebfb86dbe46a/en-US/4-route-53-resolvers-with-active-directory/endpoints>
upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: B

Outbound resolver endpoints will let you query your onprem DNS

Inbound resolver endpoints will let onprem DNS query the AWS default DNS server of VPC (.2)

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: B

Correct Answer is B

upvoted 2 times

Question #279

Topic 1

A company uses AWS CloudFormation to deploy applications within multiple VPCs that are all attached to a transit gateway. Each VPC that sends traffic to the public internet must send the traffic through a shared services VPC. Each subnet within a VPC uses the default VPC route table, and the traffic is routed to the transit gateway. The transit gateway uses its default route table for any VPC attachment.

A security audit reveals that an Amazon EC2 instance that is deployed within a VPC can communicate with an EC2 instance that is deployed in any of the company's other VPCs. A solutions architect needs to limit the traffic between the VPCs. Each VPC must be able to communicate only with a predefined, limited set of authorized VPCs.

What should the solutions architect do to meet these requirements?

- A. Update the network ACL of each subnet within a VPC to allow outbound traffic only to the authorized VPCs. Remove all deny rules except the default deny rule.
- B. Update all the security groups that are used within a VPC to deny outbound traffic to security groups that are used within the unauthorized VPCs.
- C. Create a dedicated transit gateway route table for each VPC attachment. Route traffic only to the authorized VPCs.
- D. Update the main route table of each VPC to route traffic only to the authorized VPCs through the transit gateway.

 **ggrodsckiy** 2 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

it's a C

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - Correct. Static routes on TGW.

upvoted 2 times

 **nexus2020** 3 months ago

Selected Answer: C

The wording for C is bad though, if ec2 in one VPC can communicate to another EC2 in any VPC, then TGW is the one linking them together, aka TGW already has a route table.

Now, creating a new route table? so the TGW will not look at the old route table? bad wording though

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: C

C is correct

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: C

C is correct. Option C suggests creating a dedicated transit gateway route table for each VPC attachment. This allows fine-grained control over the routing of traffic between VPCs. By creating separate route tables, the architect can specify the allowed routes for each VPC attachment and limit traffic to only the authorized VPCs. This approach ensures that communication between VPCs is restricted and provides a secure and controlled network environment.

upvoted 4 times

 **MoussaNoussa** 3 months ago

C is the right answer

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C

Correct Answer is C

upvoted 2 times

Question #280

Topic 1

A company has a Windows-based desktop application that is packaged and deployed to the users' Windows machines. The company recently acquired another company that has employees who primarily use machines with a Linux operating system. The acquiring company has decided to migrate and rehost the Windows-based desktop application to AWS.

All employees must be authenticated before they use the application. The acquiring company uses Active Directory on premises but wants a simplified way to manage access to the application on AWS for all the employees.

Which solution will rehost the application on AWS with the LEAST development effort?

- A. Set up and provision an Amazon Workspaces virtual desktop for every employee. Implement authentication by using Amazon Cognito identity pools. Instruct employees to run the application from their provisioned Workspaces virtual desktops.
- B. Create an Auto Scaling group of Windows-based Amazon EC2 instances. Join each EC2 instance to the company's Active Directory domain. Implement authentication by using the Active Directory that is running on premises. Instruct employees to run the application by using a Windows remote desktop.
- C. Use an Amazon AppStream 2.0 image builder to create an image that includes the application and the required configurations. Provision an AppStream 2.0 On-Demand fleet with dynamic Fleet Auto Scaling policies for running the image. Implement authentication by using AppStream 2.0 user pools. Instruct the employees to access the application by starting browser-based AppStream 2.0 streaming sessions.
- D. Refactor and containerize the application to run as a web-based application. Run the application in Amazon Elastic Container Service (Amazon ECS) on AWS Fargate with step scaling policies. Implement authentication by using Amazon Cognito user pools. Instruct the employees to run the application from their browsers.

 **chico2023** 1 month, 2 weeks ago

Selected Answer: C

Answer: C - Don't even think in any other option. It's AppStream what they need to provision.

upvoted 1 times

 **ggrodsckiy** 2 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

it's C, so Linux desktops can access via browser

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - Correct. AppStream is what is Citrix XenDesktop.

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: C

Amazon Cognito identity pools does not support AD. however WorkSpace is a right choise forthis use case though.

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: C

C for sure

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: C

C is correct answer

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: C

Option C leverages Amazon AppStream 2.0, a fully managed application streaming service. With AppStream 2.0, you can create an image that includes the Windows-based desktop application and the required configurations.

upvoted 3 times

 **PhuocT** 3 months ago

C seems correct answer.
upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: C
C
Use appstream
upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: B
Correct Answer is B
upvoted 1 times

 **Alabi** 3 months ago

Stop putting wrong answers in every question
upvoted 8 times

Question #281

Topic 1

A company is collecting a large amount of data from a fleet of IoT devices. Data is stored as Optimized Row Columnar (ORC) files in the Hadoop Distributed File System (HDFS) on a persistent Amazon EMR cluster. The company's data analytics team queries the data by using SQL in Apache Presto deployed on the same EMR cluster. Queries scan large amounts of data, always run for less than 15 minutes, and run only between 5 PM and 10 PM.

The company is concerned about the high cost associated with the current solution. A solutions architect must propose the most cost-effective solution that will allow SQL data queries.

Which solution will meet these requirements?

- A. Store data in Amazon S3. Use Amazon Redshift Spectrum to query data.
- B. Store data in Amazon S3. Use the AWS Glue Data Catalog and Amazon Athena to query data.
- C. Store data in EMR File System (EMRFS). Use Presto in Amazon EMR to query data.
- D. Store data in Amazon Redshift. Use Amazon Redshift to query data.

 **ggrodsckiy** 2 months ago

Correct B

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

it's a B

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: B

Clasic ServerLess

S3 Datalake

Glue for ETL

Athena for Query

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B - S3 , GDC and Athena for sure is the cheapest.

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: B

Storing the data in Amazon S3 is a cost-effective solution compared to running a persistent EMR cluster with HDFS.

The AWS Glue Data Catalog provides a centralized metadata repository for organizing and cataloging data in S3.

Amazon Athena is a serverless query service that allows you to run SQL queries directly against data in S3 without the need for a dedicated cluster or infrastructure.

By using Amazon Athena, you only pay for the queries you run, which aligns with the requirement of cost-effectiveness.

upvoted 2 times

 **shree2023** 3 months ago

Selected Answer: B

B is most cost effective

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: B

S3 with Glue and Athena will do the trick

upvoted 1 times

 **PhuocT** 3 months ago

Selected Answer: B

B could be the answer

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: B

B is the answer

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

Question #282

Topic 1

A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into details of AWS Billing and Cost Management. There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging. Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS instances.

Which strategy should the solutions architect provide to meet these requirements?

- A. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources.
- B. Use an AWS Config rule to alert the finance team of untagged resources. Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account role.
- C. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID. Use SCPs to restrict resource creation that do not have the cost center and project ID on the resource.
- D. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources. Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project ID on the resource.

 **ggrodsckiy** 2 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

C of course

upvoted 1 times

 **hexie** 2 months, 3 weeks ago

Selected Answer: C

C.

A will meet only 1 of the 2 points which is the Tag. A wont prevent it in the future.

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - Apply tags and prevent future untagged resources to be created with SCPs.

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: C

C , adicionally use SCP for denied not create resource without tag in the future

upvoted 1 times

 **Maria2023** 3 months ago

Selected Answer: C

Requirement "There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging." equals SCP, so answer C

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: C

C is correct.

A only takes care of existing resources not future resources

upvoted 2 times

 **gd1** 3 months ago

Selected Answer: A

Option A suggests using the Tag Editor feature in AWS Billing and Cost Management to tag existing resources. By using consistent tagging through cost allocation tags, the cost center and project ID can be defined and associated with the DynamoDB tables and RDS instances. Allowing 24 hours for tags to propagate ensures that the existing resources are appropriately tagged.

upvoted 1 times

 **PhuocT** 3 months ago

C makes sense, using SCP

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: C

C is correct use SCPs

upvoted 1 times

 **MoussaNoussa** 3 months ago

C is the right answer

upvoted 1 times

 **Don2021** 3 months ago

Why not C, C will take care of existing and SCP will ensure future resources are tagged

upvoted 3 times

 **psyx21** 3 months, 1 week ago

Selected Answer: A

Correct Answer is A

upvoted 1 times

Question #283

Topic 1

A company wants to send data from its on-premises systems to Amazon S3 buckets. The company created the S3 buckets in three different accounts. The company must send the data privately without the data traveling across the internet. The company has no existing dedicated connectivity to AWS.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a private VIF between the on-premises environment and the private VPC.
- B. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a public VIF between the on-premises environment and the private VPC.
- C. Create an Amazon S3 interface endpoint in the networking account.
- D. Create an Amazon S3 gateway endpoint in the networking account.
- E. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Peer VPCs from the accounts that host the S3 buckets with the VPC in the network account.

 **cmoreira** 3 weeks, 2 days ago

Selected Answer: AC

AC - DX+Interface endpoint.

Both gateway and interface endpoints will use aws backbone, so not internet. However, you cannot access a GW endpoint from onprem. Therefore needs interface (ENIs) endpoints.

upvoted 1 times

 **ggrodsckiy** 2 months, 1 week ago

Correct AC.

upvoted 1 times

 **Christina666** 2 months, 2 weeks ago

Selected Answer: AC

You can use two types of VPC endpoints to access Amazon S3: gateway endpoints and interface endpoints (by using AWS PrivateLink). A gateway endpoint is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network. Interface endpoints extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on-premises, or from a VPC in another AWS Region by using VPC peering or AWS Transit Gateway.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: AC

AC of course. see links below

upvoted 1 times

 **pupsik** 3 months ago

Selected Answer: AC

AC - links provided by other members provide very good explanation.

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: AC

AC - detailed steps under use case 2 -> <https://repost.aws/knowledge-center/s3-bucket-access-direct-connect>

upvoted 3 times

 **NETeng01** 3 months ago

Endpoint comparison: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>

upvoted 3 times

 **bhanus** 3 months ago

Thank you. Perfect explanation

upvoted 1 times

 **Mekala** 3 months ago

Selected Answer: AC

AC - Access from on-prem is using S3 Interface Endpoint + Private VIF.

<https://aws.amazon.com/blogs/networking-and-content-delivery/secure-hybrid-access-to-amazon-s3-using-aws-privatelink/>

upvoted 2 times

✉ **shree2023** 3 months ago

Selected Answer: AC

Seems AC

upvoted 1 times

✉ **gd1** 3 months ago

Selected Answer: AC

Amazon S3: interface VPC endpoint and gateway VPC endpoint. Difference :

When you configure an interface VPC endpoint, an elastic network interface (ENI) with a private IP address is deployed in your subnet. An Amazon EC2 instance in the VPC can communicate with an Amazon S3 bucket through the ENI and AWS network. Using the interface endpoint, applications in your on-premises data center can easily query S3 buckets over AWS Direct Connect or Site-to-Site VPN. Interface endpoint supports a growing list of AWS services. Consult our documentation to find AWS services compatible with interface endpoints powered by AWS PrivateLink.

upvoted 1 times

✉ **Jackhemo** 3 months ago

Selected Answer: A

olabiba.ai says A,C.

Keep in mind However, gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway. For those scenarios, you must use an interface endpoint. <https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

upvoted 1 times

✉ **bhanus** 3 months ago

Selected Answer: AD

A - private VIF will keep traffic private between onprem and aws

D - S3 ONLY supports gateway endpoints. Gateway endpoints can be utilized to access Amazon S3 and Amazon DynamoDB services privately.

C is WRONG because S3 does not support interface VPC endpoint

upvoted 1 times

✉ **bhanus** 2 months, 3 weeks ago

AC is the answer. Thanks NETeng01 for below doc. Perfect explanation on Gateway vs Interface endpoint

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>

upvoted 1 times

✉ **bhanus** 3 months ago

Changing to AC. Thanks Mekala for the documentation reference

<https://aws.amazon.com/blogs/networking-and-content-delivery/secure-hybrid-access-to-amazon-s3-using-aws-privatelink/>

upvoted 1 times

✉ **planedefiler** 3 months ago

Selected Answer: AC

AC is good

upvoted 1 times

✉ **Don2021** 3 months ago

AC because A will get the content to VPC and you can use S3 interface to share within other accounts.

upvoted 2 times

✉ **psyx21** 3 months, 1 week ago

Selected Answer: CE

CE is the correct option

upvoted 1 times

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

f... u..

upvoted 2 times

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

9 times out of 10 is the wrong answer. gotta be on purpose

upvoted 1 times

Question #284

Topic 1

A company operates quick-service restaurants. The restaurants follow a predictable model with high sales traffic for 4 hours daily. Sales traffic is lower outside of those peak hours.

The point of sale and management platform is deployed in the AWS Cloud and has a backend that is based on Amazon DynamoDB. The database table uses provisioned throughput mode with 100,000 RCU and 80,000 WCU to match known peak resource consumption.

The company wants to reduce its DynamoDB cost and minimize the operational overhead for the IT staff.

Which solution meets these requirements MOST cost-effectively?

- A. Reduce the provisioned RCU and WCU.
- B. Change the DynamoDB table to use on-demand capacity.
- C. Enable Dynamo DB auto scaling for the table.
- D. Purchase 1-year reserved capacity that is sufficient to cover the peak load for 4 hours each day.

 **Arnaud92** 3 weeks, 6 days ago

Selected Answer: D

When it's predictable i go for reserved capacity that have up to 77% cost reduction. <https://aws.amazon.com/dynamodb/reserved-capacity/>. I'll go for D.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

its C for predictable scaling

upvoted 1 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: C

C - Autoscaling. "In addition, you can leverage auto-scaling to adjust the table's capacity based on the application's utilization, thereby enforcing cost optimization measures. It is a good fit for workloads with predictable traffic." <https://www.finout.io/blog/how-to-optimize-usage-and-reduce-dynamodb-pricing>

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - Autoscaling. "In addition, you can leverage auto-scaling to adjust the table's capacity based on the application's utilization, thereby enforcing cost optimization measures. It is a good fit for workloads with predictable traffic." <https://www.finout.io/blog/how-to-optimize-usage-and-reduce-dynamodb-pricing>

upvoted 3 times

 **shree2023** 3 months ago

Selected Answer: C

C is correct answer with predictable pattern auto scaling is good enough and not on demand

upvoted 2 times

 **Don2021** 3 months ago

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

upvoted 2 times

 **gd1** 3 months ago

C is correct A, B and D do not meet needs.

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C

C is the correct Option

upvoted 1 times

Question #285

Topic 1

A company hosts a blog post application on AWS using Amazon API Gateway, Amazon DynamoDB, and AWS Lambda. The application currently does not use API keys to authorize requests. The API model is as follows:

- GET /posts/{postId}: to get post details
- GET /users/{userId}: to get user details
- GET /comments/{commentId}: to get comments details

The company has noticed users are actively discussing topics in the comments section, and the company wants to increase user engagement by making the comments appear in real time.

Which design should be used to reduce comment latency and improve user experience?

- A. Use edge-optimized API with Amazon CloudFront to cache API responses.
- B. Modify the blog application code to request GET/comments/{commentId} every 10 seconds.
- C. Use AWS AppSync and leverage WebSockets to deliver comments.
- D. Change the concurrency limit of the Lambda functions to lower the API response time.

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

C. websockets ==realtime

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - Correct. <https://advancedweb.hu/real-time-data-with-appsync-subscriptions/>

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: C

Option C (Use AWS AppSync and leverage WebSockets to deliver comments) is the most appropriate solution for real-time comments. AWS AppSync is a fully managed service that simplifies real-time data synchronization and offline capabilities for applications. It supports WebSockets, which enables real-time communication between clients and the server. By leveraging AppSync and WebSockets, the comments can be delivered instantly to users as they are posted, reducing comment latency and improving user engagement.

upvoted 2 times

 **shree2023** 3 months ago

Selected Answer: C

C is correct others are not real time and cost effective

upvoted 2 times

 **gd1** 3 months ago

Selected Answer: C

AWS AppSync is a managed service that uses GraphQL to make it easy for applications to get exactly the data they need. With AppSync, you can build scalable applications, including those requiring real-time updates, on a range of data sources such as NoSQL data stores, relational databases, HTTP APIs, and your custom data sources with AWS Lambda.

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #286

A company manages hundreds of AWS accounts centrally in an organization in AWS Organizations. The company recently started to allow product teams to create and manage their own S3 access points in their accounts. The S3 access points can be accessed only within VPCs, not on the internet.

What is the MOST operationally efficient way to enforce this requirement?

- A. Set the S3 access point resource policy to deny the s3>CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- B. Create an SCP at the root level in the organization to deny the s3>CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- C. Use AWS CloudFormation StackSets to create a new IAM policy in each AWS account that allows the s3>CreateAccessPoint action only if the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- D. Set the S3 bucket policy to deny the s3>CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

B. SCP for scale

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B - Since you have 100s of accounts. If it was a single account, then A.

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 2 times

 **softarts** 1 month, 1 week ago

don't think there is so called "S3 access point resource policy" no matter it is 1 or 100 accounts. it is either identity or bucket resource policy

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

B is correct SCP at Org level

upvoted 2 times

 **shree2023** 3 months ago

Selected Answer: B

B is correct SCP at Org level

upvoted 2 times

 **gd1** 3 months ago

Selected Answer: B

SCP is a type of policy that you can use to manage permissions in your organization, allowing you to control AWS service actions across multiple AWS accounts. By creating the SCP at the root level, you ensure that all accounts within the organization are subjected to this policy. This is an efficient way to enforce the requirement across all accounts as it requires a single policy change instead of individual changes in every account.

upvoted 2 times

 **PhuocT** 3 months ago

Selected Answer: B

B

when the question mention AWS Organizations, use SCP always the good choice.

upvoted 2 times

 **MoussaNoussa** 3 months ago

of course answer B

upvoted 1 times

 **Don2021** 3 months ago

B - This approach ensures centralized policy management and consistent enforcement across all AWS accounts within the organization. It avoids the need for configuring bucket policies or access point resource policies in each individual account, making it operationally efficient.

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: A

Correct Answer is A

upvoted 1 times

✉ **rxhan** 1 month, 3 weeks ago

yeah be careful, you skewing the numbers on the vote, we are trying to help others.

upvoted 2 times

✉ **Alabi** 3 months ago

Why do you always provide wrong answers? Please do your research before making a comment, as you're misleading others

upvoted 5 times

✉ **PhuocT** 3 months ago

you always provided wrong answer, not sure if you do that on purpose.

upvoted 7 times

Question #287

Topic 1

A solutions architect must update an application environment within AWS Elastic Beanstalk using a blue/green deployment methodology. The solutions architect creates an environment that is identical to the existing application environment and deploys the application to the new environment.

What should be done next to complete the update?

- A. Redirect to the new environment using Amazon Route 53.
- B. Select the Swap Environment URLs option.
- C. Replace the Auto Scaling launch configuration.
- D. Update the DNS records to point to the green environment.

 **ggorodskiy** 2 months, 1 week ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

its a B

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: B

B

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B - Look at the link, step 5 -> <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: B

B. Select the Swap Environment URLs option.

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: B

B to swap from blue to green

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: B

AWS Elastic Beanstalk provides a Swap Environment URLs option for performing a blue/green deployment. This operation swaps the CNAME records of two environments, thus rerouting traffic from the original environment (blue) to the new environment (green).

upvoted 4 times

 **bhanus** 3 months ago

Selected Answer: B

B elastic beanstalk has Swap Environment URLs feature

<https://docs.aws.amazon.com/whitepapers/latest/blue-green-deployments/swap-the-environment-of-an-elastic-beanstalk-application.html>

upvoted 2 times

 **MoussaNoussa** 3 months ago

B of course

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

Question #288

Topic 1

A company is building an image service on the web that will allow users to upload and search random photos. At peak usage, up to 10,000 users worldwide will upload their images. The will then overlay text on the uploaded images, which will then be published on the company website.

Which design should a solutions architect implement?

- A. Store the uploaded images in Amazon Elastic File System (Amazon EFS). Send application log information about each image to Amazon CloudWatch Logs. Create a fleet of Amazon EC2 instances that use CloudWatch Logs to determine which images need to be processed. Place processed images in another directory in Amazon EFS. Enable Amazon CloudFront and configure the origin to be the one of the EC2 instances in the fleet.
- B. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to Amazon Simple Notification Service (Amazon SNS). Create a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) to pull messages from Amazon SNS to process the images and place them in Amazon Elastic File System (Amazon EFS). Use Amazon CloudWatch metrics for the SNS message volume to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the ALB in front of the EC2 instances.
- C. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to the Amazon Simple Queue Service (Amazon SQS) queue. Create a fleet of Amazon EC2 instances to pull messages from the SQS queue to process the images and place them in another S3 bucket. Use Amazon CloudWatch metrics for queue depth to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the S3 bucket that contains the processed images.
- D. Store the uploaded images on a shared Amazon Elastic Block Store (Amazon EBS) volume mounted to a fleet of Amazon EC2 Spot instances. Create an Amazon DynamoDB table that contains information about each uploaded image and whether it has been processed. Use an Amazon EventBridge rule to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to reference an Elastic Load Balancer in front of the fleet of EC2 instances.

 **ggrodskiy** 2 months, 1 week ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

its a C

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - no doubt, SQS and CloudFront for processed image retrieval

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: C

ALB – B is out

S3 is good enough, EFS and EBS are too much for image processing

upvoted 3 times

 **Alabi** 3 months ago

Selected Answer: C

Option C (Store the uploaded images in an S3 bucket and use S3 event notification with SQS queue) is the most suitable design. Amazon S3 provides highly scalable and durable storage for the uploaded images. Configuring S3 event notifications to send messages to an SQS queue allows for decoupling the processing of images from the upload process. A fleet of EC2 instances can pull messages from the SQS queue to process the images and store them in another S3 bucket. Scaling out the EC2 instances based on SQS queue depth using CloudWatch metrics ensures efficient utilization of resources. Enabling Amazon CloudFront with the origin set to the S3 bucket containing the processed images improves the global availability and performance of image delivery.

upvoted 3 times

 **SkyZeroZx** 3 months ago

Selected Answer: C

C without doubt

upvoted 1 times

 **shree2023** 3 months ago

Selected Answer: C

C indeed

upvoted 1 times

 **MoussaNoussa** 3 months ago

C without doubt

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #289

Topic 1

A company has deployed its database on an Amazon RDS for MySQL DB instance in the us-east-1 Region. The company needs to make its data available to customers in Europe. The customers in Europe must have access to the same data as customers in the United States (US) and will not tolerate high application latency or stale data. The customers in Europe and the customers in the US need to write to the database. Both groups of customers need to see updates from the other group in real time.

Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL replica of the RDS for MySQL DB instance. Pause application writes to the RDS DB instance. Promote the Aurora Replica to a standalone DB cluster. Reconfigure the application to use the Aurora database and resume writes. Add eu-west-1 as a secondary Region to the DB cluster. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.
- B. Add a cross-Region replica in eu-west-1 for the RDS for MySQL DB instance. Configure the replica to replicate write queries back to the primary DB instance. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.
- C. Copy the most recent snapshot from the RDS for MySQL DB instance to eu-west-1. Create a new RDS for MySQL DB instance in eu-west-1 from the snapshot. Configure MySQL logical replication from us-east-1 to eu-west-1. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.
- D. Convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster. Add eu-west-1 as a secondary Region to the DB cluster. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.

 **ggrodskiy** Highly Voted 2 months, 1 week ago

Correct D.

You cannot convert RDS MySQL to Aurora MySQL natively, but you can create an Aurora read replica of the RDS MySQL DB instance and then promote it to a standalone Aurora MySQL DB cluster <https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/> <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.html>. This is the first step of option A in the question. However, this option also requires pausing application writes and reconfiguring the application, which can cause downtime and data inconsistency. Therefore, option A is not the best solution for the given requirements. Option D is still the correct answer because it does not require pausing writes or reconfiguring the application, and it enables cross-Region replication and write forwarding for the database.

upvoted 7 times

 **nharaz** Most Recent 1 day, 12 hours ago

Selected Answer: D

Write forwarding is a feature of Aurora that allows writes to be directed to the primary cluster while maintaining read access to the replica cluster, ensuring data consistency and low latency.

upvoted 1 times

 **xav1er** 1 month ago

Selected Answer: A

It's clearly A , not any other option

upvoted 1 times

 **Asds** 1 month, 3 weeks ago

Selected Answer: A

A, 'cause of the conversion which is not possible

upvoted 2 times

 **Mom305** 2 months, 1 week ago

Selected Answer: A

The reason you create an Amazon Aurora MySQL Replica is because "replication lag between source DB instance and Aurora Read Replica approaches zero" , and here are the steps recommended and instructed as part of an AWS Workshop <https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/#:~:text=2.1%20-%20Open%20the%20Amazon%20RDS,choose%20Create%20Aurora%20read%20replica.>

upvoted 1 times

 **Zox42** 2 months, 2 weeks ago

Selected Answer: A

Answer A

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: A

A - <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Replica.html>

upvoted 2 times

 **hexie** 2 months, 3 weeks ago

Selected Answer: D
I'm going for D just because the doc I'll send below says its possible to do what A says, but its a read replica. A read replica doesn't perform operations itself, it's just for read purposes.

<https://aws.amazon.com/blogs/aws/new-create-an-amazon-aurora-read-replica-from-a-mysql-db-instance/>

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

ehh, that article describes A, not D

upvoted 1 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: A

<https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/>

upvoted 1 times

 **qwertyui0** 2 months, 3 weeks ago

Selected Answer: A

You cannot convert RDS MySQL to Aurora MySQL natively. Need to create a Aurora read replica first.

upvoted 1 times

 **javitech83** 2 months, 4 weeks ago

Selected Answer: A

I would go for A. D would be great but it would require some effort to I am not sure it's possible to convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster. Option A gives more details and is perfectly possible

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Replica.html>

upvoted 2 times

 **aviathor** 4 weeks ago

The Aurora read replica can be promoted to a stand-alone cluster.

upvoted 1 times

 **james55** 3 months ago

Selected Answer: A

I could be wrong but I can find documentation for A but not D.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Replica.html>

"Before you promote your Aurora read replica, stop any transactions from being written to the source MySQL DB instance, and then wait for the replica lag on the Aurora read replica to reach 0"

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: A

A - See step-by-step here -> <https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/>

upvoted 2 times

 **nexus2020** 3 months ago

Selected Answer: D

A seems to work as well, but D is more clear and direct, and does not involve pausing the DB.

For write forwarding : In an Amazon RDS DB cluster, write forwarding is a feature that allows write operations to be directed to the primary instance even when connecting to a reader instance. This helps ensure that write operations are always sent to the appropriate instance in the cluster.

PS: nowhere mentioned Aurora Global Database in the question, and Aurora Global Database is not the default behaviour of DB. so it is something you have to turn on and have it configured.

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: D

Option D is the recommended solution. By converting the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster, the company can add eu-west-1 as a secondary Region to the cluster, enabling low-latency access to the data in Europe. Write forwarding can be enabled on the DB cluster, allowing writes to be directed to the primary Region (us-east-1) and automatically forwarded to the secondary Region (eu-west-1). This ensures real-time updates and data consistency between the two Regions. By deploying the application in eu-west-1 and configuring it to use the Aurora MySQL endpoint in eu-west-1, customers in Europe will have access to the data with low latency and real-time updates.

upvoted 2 times

 **gd1** 3 months ago

Selected Answer: D

With Aurora Global Database, you can set up one primary region where the read-write operations take place, and up to five read-only secondary regions. In Aurora, you can use write forwarding, which allows Aurora MySQL DB clusters that are secondary clusters in an Aurora global

database to automatically forward write operations to the primary DB cluster and return the results of the operations back to your application.
upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: D

Correct Answer is D

upvoted 3 times

Question #290

Topic 1

A company is serving files to its customers through an SFTP server that is accessible over the internet. The SFTP server is running on a single Amazon EC2 instance with an Elastic IP address attached. Customers connect to the SFTP server through its Elastic IP address and use SSH for authentication. The EC2 instance also has an attached security group that allows access from all customer IP addresses.

A solutions architect must implement a solution to improve availability, minimize the complexity of infrastructure management, and minimize the disruption to customers who access files. The solution must not change the way customers connect.

Which solution will meet these requirements?

- A. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.
- B. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a VPC-hosted, internet-facing endpoint. Associate the SFTP Elastic IP address with the new endpoint. Attach the security group with customer IP addresses to the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.
- C. Disassociate the Elastic IP address from the EC2 instance. Create a new Amazon Elastic File System (Amazon EFS) file system to be used for SFTP file hosting. Create an AWS Fargate task definition to run an SFTP server. Specify the EFS file system as a mount in the task definition. Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB) in front of the service. When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server. Associate the Elastic IP address with the NLB. Sync all files from the SFTP server to the S3 bucket.
- D. Disassociate the Elastic IP address from the EC2 instance. Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hosting. Create a Network Load Balancer (NLB) with the Elastic IP address attached. Create an Auto Scaling group with EC2 instances that run an SFTP server. Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume. Configure the Auto Scaling group to automatically add instances behind the NLB. Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches. Sync all files from the SFTP server to the new multi-attach EBS volume.

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

B of course. need SG to whitelist IPs

upvoted 1 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: B

<https://repost.aws/knowledge-center/aws-sftp-endpoint-type>

upvoted 2 times

 **SkyZeroZx** 2 months, 3 weeks ago

Selected Answer: B

B

Question say " The EC2 instance also has an attached security group that allows access from all customer IP addresses."

B say "Attach the security group with customer IP addresses to the new endpoint"

Should be Security Group for working with security for customer

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: B

It's B. You can't attach elastic IP with A). -> <https://repost.aws/knowledge-center/aws-sftp-endpoint-type> - look at the table

upvoted 2 times

 **ozelllll** 3 months ago

Selected Answer: B

It's B: <https://repost.aws/knowledge-center/aws-sftp-endpoint-type>

upvoted 4 times

 **gd1** 3 months ago

Selected Answer: B

A is public access; the requirement says need Security Group with Ip addresses - B is correct

upvoted 1 times

 **Jackhemo** 3 months ago

Selected Answer: B

Olabiba.ai Says B:

Option B suggests disassociating the Elastic IP address from the EC2 instance and creating an Amazon S3 bucket for SFTP file hosting. An AWS Transfer Family server is then created and configured with a VPC-hosted, internet-facing endpoint. The SFTP Elastic IP address is associated with the new endpoint, and the security group with customer IP addresses is attached to the endpoint. The Transfer Family server is pointed to the S3 bucket, and all files from the SFTP server are synced to the S3 bucket.

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: A

Correct Answer is A

upvoted 2 times

 **rxhan** 1 month, 3 weeks ago

again wrong, dont be quick and wrong.

upvoted 2 times

Question #291

Topic 1

A company ingests and processes streaming market data. The data rate is constant. A nightly process that calculates aggregate statistics takes 4 hours to complete. The statistical analysis is not critical to the business, and data points are processed during the next iteration if a particular run fails.

The current architecture uses a pool of Amazon EC2 Reserved Instances with 1-year reservations. These EC2 instances run full time to ingest and store the streaming data in attached Amazon Elastic Block Store (Amazon EBS) volumes. A scheduled script launches EC2 On-Demand Instances each night to perform the nightly processing. The instances access the stored data from NFS shares on the ingestion servers. The script terminates the instances when the processing is complete.

The Reserved Instance reservations are expiring. The company needs to determine whether to purchase new reservations or implement a new design.

Which solution will meet these requirements MOST cost-effectively?

- A. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use a scheduled script to launch a fleet of EC2 On-Demand Instances each night to perform the batch processing of the S3 data. Configure the script to terminate the instances when the processing is complete.
- B. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price.
- C. Update the ingestion process to use a fleet of EC2 Reserved Instances with 3-year reservations behind a Network LoadBalancer. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price.
- D. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon Redshift. Use Amazon EventBridge to schedule an AWS Lambda function to run nightly to query Amazon Redshift to generate the daily statistics.

 **softarts** 1 month, 2 weeks ago

Selected Answer: B

A=> Use a scheduled script to launch a fleet of EC2 On-Demand wrong
 C=> Update the ingestion process to use a fleet of EC2 Reserved Instances wrong
 D=> lambda wrong
 upvoted 2 times

 **hglopes** 1 month, 2 weeks ago

Selected Answer: C

For a stable rate of ingestion I choose EC2 with 3yr reservation over Firehose & S3API costs. Using Spot instances for the low priority aggregation will lower the costs further
 upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

its a B
 upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: B

B - Correct. And only because of this -> " The statistical analysis is not critical to the business, and data points are processed during the next iteration if a particular run fails."
 Spot instances are not guaranteed and if the condition above was not there, than probably C.
 upvoted 3 times

 **easystoo** 3 months ago

b-b-b-b-b-b-b
 upvoted 2 times

 **gd1** 3 months ago

Selected Answer: B

S3 + Batch with SOT servers
 upvoted 2 times

 **Don2021** 3 months ago

Support B as answer. MOST cost effective
 upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: B

Correct Answer is B

upvoted 2 times

Question #292

Topic 1

A company needs to migrate an on-premises SFTP site to AWS. The SFTP site currently runs on a Linux VM. Uploaded files are made available to downstream applications through an NFS share.

As part of the migration to AWS, a solutions architect must implement high availability. The solution must provide external vendors with a set of static public IP addresses that the vendors can allow. The company has set up an AWS Direct Connect connection between its on-premises data center and its VPC.

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

- A. Create an AWS Transfer Family server. Configure an internet-facing VPC endpoint for the Transfer Family server. Specify an Elastic IP address for each subnet. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.
- B. Create an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.
- C. Use AWS Application Migration Service to migrate the existing Linux VM to an Amazon EC2 instance. Assign an Elastic IP address to the EC2 instance. Mount an Amazon Elastic File System (Amazon EFS) file system to the EC2 instance. Configure the SFTP server to place files in the EFS file system. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.
- D. Use AWS Application Migration Service to migrate the existing Linux VM to an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon FSx for Lustre file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the FSx for Lustre endpoint instead.

 **grodskiy** 2 months, 1 week ago

Correct A.

upvoted 1 times

 **Jonalb** 2 months, 1 week ago

Selected Answer: A

AAAAAAAAAA

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: A

its an A.. static IPs

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: A

It's A. You can't have elastic IP with B.

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: A

A <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-sftp-server-to-aws-using-aws-transfer-for-sftp.html>

upvoted 1 times

 **Alabi** 3 months ago

Selected Answer: A

Option A suggests creating an AWS Transfer Family server and configuring an internet-facing VPC endpoint for it. By specifying an Elastic IP address for each subnet, the company can provide a set of static public IP addresses to external vendors. The Transfer Family server can be configured to place files into an Amazon Elastic File System (Amazon EFS) file system, which provides a scalable and highly available storage solution across multiple Availability Zones. This allows the company to maintain high availability for the SFTP site and its downstream applications without the need for manual intervention or additional operational overhead.

upvoted 1 times

 **gd1** 3 months ago

Selected Answer: A

A is correct for Pvt IP addresses.

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: A

A is correct

B is incorrect because for Publicly accessible endpoints for AWS Transfer Family you can't attach a static IP address. AWS provides IP addresses that are subject to change. IPs are provided via AWS Global Accelerator, which uses static Anycast IP addresses
<https://repost.aws/knowledge-center/aws-sftp-endpoint-type>

upvoted 3 times

 **bhanus** 3 months ago

Selected Answer: A

A is correct

In B there is NO mention of elasticIPs. the question asks "The solution must provide external vendors with a set of static public IP addresses that the vendors can allow"

upvoted 2 times

 **psyx21** 3 months, 1 week ago

Selected Answer: A

Correct Answer is A

upvoted 2 times

Question #293

Topic 1

A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group. The VPC architecture spans two Availability Zones (AZ) with a subnet in each that the Auto Scaling group is targeting. The VPC is connected to an on-premises environment and connectivity cannot be interrupted. The maximum size of the Auto Scaling group is 20 instances in service. The VPC IPv4 addressing is as follows:

VPC CIDR: 10.0.0.0/23 -

AZ1 subnet CIDR: 10.0.0.0/24 -

AZ2 subnet CIDR: 10.0.1.0/24 -

Since deployment, a third AZ has become available in the Region. The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime. Which solution will meet these requirements?

- A. Update the Auto Scaling group to use the AZ2 subnet only. Delete and re-create the AZ1 subnet using half the previous address space. Adjust the Auto Scaling group to also use the new AZ1 subnet. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Remove the current AZ2 subnet. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.
- B. Terminate the EC2 instances in the AZ1 subnet. Delete and re-create the AZ1 subnet using half the address space. Update the Auto Scaling group to use this new subnet. Repeat this for the second AZ. Define a new subnet in AZ3, then update the Auto Scaling group to target all three new subnets.
- C. Create a new VPC with the same IPv4 address space and define three subnets, with one for each AZ. Update the existing Auto Scaling group to target the new subnets in the new VPC.
- D. Update the Auto Scaling group to use the AZ2 subnet only. Update the AZ1 subnet to have half the previous address space. Adjust the Auto Scaling group to also use the AZ1 subnet again. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Update the current AZ2 subnet and assign the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.

 **YodaMaster** Highly Voted  2 months, 3 weeks ago

This question was painful to read.

upvoted 10 times

 **Blingy** Most Recent  4 days, 3 hours ago

The question though lol had to look for the difference in the options to remember the answer. When it comes to a “delete “

upvoted 1 times

 **Arnaud92** 3 weeks, 5 days ago

Selected Answer: D

D is easier, no need to delete the subnet. <https://docs.aws.amazon.com/vpc/latest/userguide/subnet-cidr-reservation.html>

upvoted 2 times

 **SK_Tyagi** 1 month ago

Selected Answer: A

Surely wasn't a 3 min ques. Thankfully they did not throw CIDR reservations into the mix

upvoted 3 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: A

A. can't update subnet

upvoted 2 times

 **Christina666** 2 months, 2 weeks ago

These answers are big pain to read

upvoted 4 times

 **SmileyCloud** 3 months ago

Selected Answer: A

A - Correct. You can't modify subnet as D says.

upvoted 2 times

✉ **nexus2020** 3 months ago

Selected Answer: A

D: "Update the AZ1 subnet" in D is not possible. you have to delete and recreate a subnet, there is no update option

B: service intrruption

C: is a joke.....

upvoted 4 times

✉ **Jackhemo** 3 months ago

Selected Answer: A

olabiba.ai says "A". Chatgpt kept bouncing between "B" & "D".

upvoted 1 times

✉ **bhanus** 3 months ago

Selected Answer: A

A is answer

upvoted 2 times

✉ **PhuocT** 3 months ago

yep, A is correct.

upvoted 2 times

✉ **jubileu84** 3 months ago

A is correct. <https://repost.aws/knowledge-center/vpc-ip-address-range>

upvoted 1 times

✉ **MoussaNoussa** 3 months ago

A is the correct answer

upvoted 1 times

✉ **psyx21** 3 months, 1 week ago

Selected Answer: D

Correct Answer is D

upvoted 1 times

✉ **nexus2020** 3 months ago

"Update the AZ1 subnet" in D is not possible. you have to delete and recreate a subnet, there is no update option

upvoted 2 times

✉ **Arnaud92** 3 weeks, 5 days ago

i think it's feasible (ndlr changing the cidr reservation: <https://docs.aws.amazon.com/vpc/latest/userguide/subnet-cidr-reservation.html>). So for me D can be easier to adopt.

upvoted 1 times

✉ **javitech83** 2 months, 3 weeks ago

psyx21 answer wrong on purpose

upvoted 1 times

Question #294

Topic 1

A company uses an organization in AWS Organizations to manage the company's AWS accounts. The company uses AWS CloudFormation to deploy all infrastructure. A finance team wants to build a chargeback model. The finance team asked each business unit to tag resources by using a predefined list of project values.

When the finance team used the AWS Cost and Usage Report in AWS Cost Explorer and filtered based on project, the team noticed noncompliant project values. The company wants to enforce the use of project tags for new resources.

Which solution will meet these requirements with the LEAST effort?

- A. Create a tag policy that contains the allowed project tag values in the organization's management account. Create an SCP that denies the cloudformation:CreateStack API operation unless a project tag is added. Attach the SCP to each OU.
- B. Create a tag policy that contains the allowed project tag values in each OU. Create an SCP that denies the cloudformation:CreateStack API operation unless a project tag is added. Attach the SCP to each OU.
- C. Create a tag policy that contains the allowed project tag values in the AWS management account. Create an IAM policy that denies the cloudformation:CreateStack API operation unless a project tag is added. Assign the policy to each user.
- D. Use AWS Service Catalog to manage the CloudFormation stacks as products. Use a TagOptions library to control project tag values. Share the portfolio with all OUs that are in the organization.

 **ggrodsckiy** 2 months, 1 week ago

Correct A.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: A

A. tag policy create in management account

upvoted 1 times

 **SkyZeroZx** 2 months, 4 weeks ago

Selected Answer: A

A) in management account for tag policy and SCP , Sounds Good

B) for each account ? more overhead

C) IAM for account in cloudformation ? is incorrect in this case

D) AWS Service Catalog ? why ? incorrect

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: A

A - Correct. You create an SCP with allowed tags in the root OU and then attach the SCP to all OUs.

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: A

AAAAAAAAAAAAAA

upvoted 1 times

 **bhanus** 3 months ago

Selected Answer: A

A is correct BUT I did NOT like the last line in option A. It says "Attach the SCP to each OU". Why should you attach SCP to each OU. Can't you just attach to RootOU so it gets inherited to child OUs

upvoted 4 times

 **SmileyCloud** 2 months, 3 weeks ago

The tags are different for each OU.

upvoted 1 times

 **jubileu84** 3 months ago

Correct Answer is A

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: A

A) Is correct in the master account of all organization use SCP is less overhead than B

B) is more overhead than A because in each OU create SCP

- C) IAM in all account is more overhead
D) is valid but not restrict other options o create with CLI or console the rest service without tags

Then A is correct

upvoted 3 times

 **Jackhemo** 3 months ago

Selected Answer: A

olabiba.ai says 'A'

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: A

Correct Answer is A

upvoted 1 times

 **bmdf** 3 months, 1 week ago

Selected Answer: A

What not use SCP?

upvoted 1 times

Question #295

Topic 1

An application is deployed on Amazon EC2 instances that run in an Auto Scaling group. The Auto Scaling group configuration uses only one type of instance.

CPU and memory utilization metrics show that the instances are underutilized. A solutions architect needs to implement a solution to permanently reduce the EC2 cost and increase the utilization.

Which solution will meet these requirements with the LEAST number of configuration changes in the future?

- A. List instance types that have properties that are similar to the properties that the current instances have. Modify the Auto Scaling group's launch template configuration to use multiple instance types from the list.
- B. Use the information about the application's CPU and memory utilization to select an instance type that matches the requirements. Modify the Auto Scaling group's configuration by adding the new instance type. Remove the current instance type from the configuration.
- C. Use the information about the application's CPU and memory utilization to specify CPU and memory requirements in a new revision of the Auto Scaling group's launch template. Remove the current instance type from the configuration.
- D. Create a script that selects the appropriate instance types from the AWS Price List Bulk API. Use the selected instance types to create a new revision of the Auto Scaling group's launch template.

 **SmileyCloud** Highly Voted 3 months ago

Selected Answer: C

It's C. You change the instance type/size in the launch template not the ASG. ASG can change the min/max size, not instance type.

upvoted 6 times

 **cmoreira** Most Recent 3 weeks, 2 days ago

Selected Answer: C

It could be B or C, but "LEAST number of configuration changes in the future" makes it C.

upvoted 1 times

 **aviathor** 4 weeks ago

Selected Answer: B

In the launch template, you can only select one instance type. You can however override the Launch Template in the ASG configuration and specify multiple instance types.

upvoted 1 times

 **softarts** 1 month, 1 week ago

Selected Answer: C

attribute-based instance types

upvoted 1 times

 **ggrodsckiy** 2 months, 1 week ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: B

its a B

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

ah, damn, clicked the wrong one.

It's a C! not B

upvoted 1 times

 **pupsik** 2 months, 4 weeks ago

Selected Answer: C

"with the LEAST number of configuration changes in the future?" means we need to use attribute-based instance types. Otherwise as new instance types get created, and older ones get retired, we need to re-configure launch config again.

upvoted 3 times

 **nexus2020** 3 months ago

Selected Answer: B

C: Application recommend to use X, but the real utilization is low, aka underutilized. so C is NOT addressing the cost saving part.

B would be the answer addressing the right sizing. utilization is also what AWS recommend to check when doing right sizing, such as using Trusted Advisor to see the under utilization, using compute optimizer, cloudwatch log, etc

upvoted 1 times

Alabi 3 months ago

Selected Answer: C

By using the information about the application's CPU and memory utilization, you can determine the CPU and memory requirements of the application.

In this solution, you create a new revision of the Auto Scaling group's launch template and specify the CPU and memory requirements in the template. This ensures that the new instances launched by the Auto Scaling group meet the application's requirements.

By removing the current instance type from the configuration, you ensure that only instances with the specified CPU and memory requirements are launched, effectively increasing utilization and optimizing costs.

This solution requires minimal configuration changes as you are primarily modifying the launch template with the updated CPU and memory requirements.

upvoted 1 times

easytoo 3 months ago

C-C-C-C-C-C-C

upvoted 1 times

Maria2023 3 months ago

Selected Answer: C

I vote for C because of the attribute-based instance type selection, available in the ASG configuration

upvoted 2 times

Maria2023 3 months ago

This might be available only for Spot instances though, needs to be confirmed

upvoted 1 times

ozelllll 3 months ago

Selected Answer: C

It's C: <https://aws.amazon.com/blogs/aws/new-attribute-based-instance-type-selection-for-ec2-auto-scaling-and-ec2-fleet/>

upvoted 2 times

skyhiker 1 month ago

Spot on with this link, thank you!

upvoted 1 times

rxhan 3 months ago

I am thinking so too, since Launch Templates are what AWS recommends. Launch Configs will be retired.

upvoted 1 times

gd1 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

psyx21 3 months, 1 week ago

Selected Answer: B

Correct Answer is B

upvoted 3 times

Question #296

Topic 1

A company implements a containerized application by using Amazon Elastic Container Service (Amazon ECS) and Amazon API Gateway. The application data is stored in Amazon Aurora databases and Amazon DynamoDB databases. The company automates infrastructure provisioning by using AWS CloudFormation. The company automates application deployment by using AWS CodePipeline.

A solutions architect needs to implement a disaster recovery (DR) strategy that meets an RPO of 2 hours and an RTO of 4 hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Set up an Aurora global database and DynamoDB global tables to replicate the databases to a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon CloudFront with origin failover to route traffic to the secondary Region during a DR scenario.
- B. Use AWS Database Migration Service (AWS DMS), Amazon EventBridge, and AWS Lambda to replicate the Aurora databases to a secondary AWS Region. Use DynamoDB Streams, EventBridge, and Lambda to replicate the DynamoDB databases to the secondary Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.
- C. Use AWS Backup to create backups of the Aurora databases and the DynamoDB databases in a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.
- D. Set up an Aurora global database and DynamoDB global tables to replicate the databases to a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.

 **finesse_999** Highly Voted  1 month, 1 week ago

I think the key here is to focus on the requirements. It is clearly stated that the requirement is that the strategy meet an RPO of 2 hours and an RTO of 4 hours. Even though option C is the most cost-effective, it is contingent on a few external factors, like the size of the data, the data change rate, etc., which cannot be assumed at the risk of breaching RPO and RTO requirements. So based on that, the most effective option is D.

upvoted 5 times

 **Explorer_30** Most Recent  3 weeks, 1 day ago

Answer is C for the RTO and RPO provided

upvoted 2 times

 **SK_Tyagi** 1 month ago

Selected Answer: C

<https://aws.amazon.com/blogs/database/cost-effective-disaster-recovery-for-amazon-aurora-databases-using-aws-backup/>

upvoted 3 times

 **chico2023** 1 month, 2 weeks ago

Selected Answer: C

Answer: C

Weird question. Sometimes I think there is no BEST answer and that they were created just to confuse people. Anyway, thinking on cost and the mentioned RPO and RTO, I would still go with C (if they were longer, it would be easier to choose among the questions).

upvoted 3 times

 **punj** 1 month, 2 weeks ago

Selected Answer: C

To implement C backups must be taken at the interval of 2 hours to satisfy RPO which might not be very efficient. D is efficient but costs slightly more.

upvoted 1 times

 **rxhan** 1 month, 3 weeks ago

Selected Answer: C

C and D are correct solutions

C is the answer as it is cost less <https://aws.amazon.com/blogs/database/cost-effective-disaster-recovery-for-amazon-aurora-databases-using-aws-backup/>

upvoted 1 times

 **grodskiy** 2 months, 1 week ago

Correct D.

upvoted 2 times

 **Piccaso** 2 months, 2 weeks ago

Selected Answer: D

I am not sure about that the C can satisfy requirement for RPO and RTO.

upvoted 1 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

what a bizarre question... no mention about failing over application components in answers..

looking at just the DBs and with RPO/RTO targets, C is the answer for cost-effective

upvoted 3 times

 **YodaMaster** 2 months, 3 weeks ago

Selected Answer: C

C is cheaper than D

upvoted 1 times

 **javitech83** 2 months, 3 weeks ago

Selected Answer: C

The most cost effective would be C. Although RPO of 2 hours will require a backup every 2 hours, but is cheaper than global databases

upvoted 1 times

 **pupsik** 2 months, 4 weeks ago

Selected Answer: C

"RTO of 4 hours" and "MOST cost effective" - use AWS Backup.

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: D

D - When you see DR, your best bet is Route53 and failover. In this case, global tables and regional GW API also contributes.

upvoted 1 times

 **CloudInfrastructures** 3 months ago

Selected Answer: C

Backup is cheaper and it probably fits in the RTO

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: C

Global table (D) cost more than using Backup (C)

upvoted 1 times

 **zhaogster** 3 months ago

C is correct

upvoted 3 times

 **SkyZeroZx** 3 months ago

Selected Answer: D

The answer is D.

This solution is the most cost-effective because it uses Amazon Aurora global databases and DynamoDB global tables to replicate the databases to a secondary AWS Region. This replication is done automatically and in real time, so the RPO is 0 seconds. The RTO is also low, because the secondary Region is already configured and ready to take over in the event of a disaster.

upvoted 3 times

 **SkyZeroZx** 3 months ago

The other solutions are more expensive because they require manual replication or backups. For example, solution B uses AWS DMS, DynamoDB Streams, EventBridge, and Lambda to replicate the databases to a secondary Region. This replication is not done in real time, so the RPO is greater than 0 seconds. The RTO is also higher, because the secondary Region must be manually configured and provisioned before it can be used.

Solution C uses AWS Backup to create backups of the databases in a secondary AWS Region. This solution has a lower RPO than solution B, because the backups can be restored to a point in time within the backup retention period. However, the RTO is still higher than solution D, because the backups must be restored manually before the databases can be used.

upvoted 2 times

 **javitech83** 2 months, 3 weeks ago

Option C RTO is higher, but the solution is cheaper and we need to select the most COST effective

upvoted 3 times

 **nexus2020** 3 months ago

Question is asking for RPO of 2 hours and an RTO of 4 hours. It is not asking which option provides the lowest RPO/RTO. It is asking which one costs less.

upvoted 3 times

Question #297

Topic 1

A company has a complex web application that leverages Amazon CloudFront for global scalability and performance. Over time, users report that the web application is slowing down.

The company's operations team reports that the CloudFront cache hit ratio has been dropping steadily. The cache metrics report indicates that query strings on some URLs are inconsistently ordered and are specified sometimes in mixed-case letters and sometimes in lowercase letters.

Which set of actions should the solutions architect take to increase the cache hit ratio as quickly as possible?

- A. Deploy a Lambda@Edge function to sort parameters by name and force them to be lowercase. Select the CloudFront viewer request trigger to invoke the function.
- B. Update the CloudFront distribution to disable caching based on query string parameters.
- C. Deploy a reverse proxy after the load balancer to post-process the emitted URLs in the application to force the URL strings to be lowercase.
- D. Update the CloudFront distribution to specify casing-insensitive query string processing.

 **ggrodskiy** 2 months, 1 week ago

Correct A.

upvoted 2 times

 **dkx** 2 months, 2 weeks ago

A. Yes, because Amazon CloudFront considers the case of parameter names and values when caching based on query string parameters , thus inconsistent query strings may cause CloudFront to forward mixed-cased/misordered requests to the origin.

Triggering a Lambda@Edge function based on a viewer request event to sort parameters by name and force them to be lowercase is the best choice.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/QueryStringParameters.html#query-string-parameters-optimizing-caching>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-cloudfront-trigger-events.html>

B. No, because this will exacerbate the caching issue by sending all query string parameters requests to the origin

C. No, because this won't help increase the cache hit ratio

D. No, because a CloudFront distribution specifies information about the origin/source of your content and how to track and manage content delivery.

upvoted 3 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: A

its an A

D would be nice if was supported

upvoted 1 times

 **SmileyCloud** 3 months ago

Selected Answer: A

A - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examples-normalize-query-string-parameters>

upvoted 2 times

 **SmileyCloud** 3 months ago

A - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examples-normalize-query-string-parameters>

upvoted 1 times

 **nexus2020** 3 months ago

Selected Answer: A

D is out: CloudFront distributions do not have built-in support for specifying a case-insensitive query string. By default, CloudFront treats query strings as case-sensitive, meaning that a URL with a different case in the query string parameter would be treated as a separate object and potentially result in a cache miss.

upvoted 1 times

 **SkyZeroZx** 3 months ago

Selected Answer: A

A , same questions this version 1

<https://www.examtopics.com/discussions/amazon/view/27789-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

 **gd1** 3 months ago

Selected Answer: A

A is the answer -to sort parameters by name and force them to be lowercase

upvoted 1 times

 **bhanus** 3 months ago

A

check for the example in the below documentation

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html>

upvoted 1 times

 **PhuocT** 3 months ago

A is answer

upvoted 1 times

 **psyx21** 3 months, 1 week ago

Selected Answer: A

Correct Answer is A

upvoted 1 times

Question #298

Topic 1

A company runs an ecommerce application in a single AWS Region. The application uses a five-node Amazon Aurora MySQL DB cluster to store information about customers and their recent orders. The DB cluster experiences a large number of write transactions throughout the day.

The company needs to replicate the data in the Aurora database to another Region to meet disaster recovery requirements. The company has an RPO of 1 hour.

Which solution will meet these requirements with the LOWEST cost?

- A. Modify the Aurora database to be an Aurora global database. Create a second Aurora database in another Region.
- B. Enable the Backtrack feature for the Aurora database. Create an AWS Lambda function that runs daily to copy the snapshots of the database to a backup Region.
- C. Use AWS Database Migration Service (AWS DMS). Create a DMS change data capture (CDC) task that replicates the ongoing changes from the Aurora database to an Amazon S3 bucket in another Region.
- D. Turn off automated Aurora backups. Configure Aurora backups with a backup frequency of 1 hour. Specify another Region as the destination Region. Select the Aurora database as the resource assignment.

 **YodaMaster** Highly Voted 2 months, 3 weeks ago

Selected Answer: C

Good luck for the exams. I know I'm gonna fail coz it takes me 3 hours just to read the questions. >:(
upvoted 10 times

 **SkyZeroZx** Highly Voted 2 months, 3 weeks ago

if you got far it means you are persistent, good luck on your exam
upvoted 5 times

 **kjcncjek** Most Recent 2 weeks, 4 days ago

its can't be D
You can't disable automated backups on Aurora. The backup retention period for Aurora is managed by the DB cluster.

so answer is C
upvoted 1 times

 **aviathor** 3 weeks, 6 days ago

Selected Answer: C

Although I also lean towards C, the problem is that I think the solution is not complete with only the CDC. We would also need a backup from which to recover the databases before applying the changes.
upvoted 1 times

 **longng0924** 1 month ago

Before considering the cost, please consider the ability of solution.

B. Backtrack feature is mainly use for solved incorrect data or configuration but don't clone to new DB, just roll-back to a PITR.

C. How can create a S3 as a target for DMS in other regions? It must be the same region with DMS.
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html#CHAP_Target.S3.Prerequisites

D. Cannot turn off automatic backup of Aurora, the automatic backup range is 1 to 35 days. Disable require 0 day but don't have any option which is 0 day.

So, the answer A is reasonable.

upvoted 1 times

 **aviathor** 3 weeks, 6 days ago

Who said DMS had to be configured in the source region? Actually it is recommended to configure DMS in the target region. So DMS to S3 it is! C
upvoted 1 times

 **softarts** 1 month, 2 weeks ago

Selected Answer: C

lean to C, but C doesn't backup the full data?
upvoted 1 times

 **breadops** 1 month, 3 weeks ago

Selected Answer: C

No RTO = C

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html

upvoted 1 times

 **khksoma** 1 month, 3 weeks ago

Prerequisites for using Amazon S3 as a target

Before using Amazon S3 as a target, check that the following are true:

The S3 bucket that you're using as a target is in the same AWS Region as the DMS replication instance you are using to migrate your data.

upvoted 1 times

 **aviathor** 3 weeks, 6 days ago

Yep, so you configure DMS in the target region.

upvoted 1 times

 **MegalodonBolado** 2 months ago

C looks more like a workaround than an architected solution. Also, I don't know how to confirm RPO < 1 hour if data amount wasn't provided.

Vote: A

upvoted 2 times

 **khksoma** 2 months ago

I dont think it can be C. Check the pre-req for S3 to be the target in this link.

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html

upvoted 2 times

 **ggrodsckiy** 2 months, 1 week ago

Correct A.

We have an RPO of 1 hour, which means you can tolerate losing up to 1 hour of data in case of a disaster. However, you also need to consider the cost and the recovery time objectives (RTO) of your solution. Using AWS DMS will cost more than using Aurora global database, and it will take longer to recover your data from S3 to a new database. Aurora global database will replicate your data to another Region with low latency, and it will allow you to fail over to the secondary DB cluster in minutes if the primary Region is unavailable. Therefore, Aurora global database is a better solution for your requirements.

upvoted 3 times

 **dkx** 2 months, 2 weeks ago

A. No, because this will create more database resources and the question is asking about 'replication of data', not 'replication of databases'

B. No, because a daily copy does not meet the RPO of 1 hour requirement

C. Yes, because using DMS CDC to replicate ongoing changes addresses the large number of write transactions throughout the day and the RPO of 1 hour requirement

D. No, because this just writes the active DB cluster's logs to a different region on an hourly basis.

Note, this question and answer choices are poorly worded.

upvoted 3 times

 **NikkyDicky** 2 months, 2 weeks ago

Selected Answer: C

best guess is C, since can't disable aurora backups and global DB is expensive

upvoted 1 times

 **NikkyDicky** 2 months, 3 weeks ago

Selected Answer: C

C would be a better, less costly option, given that there are no RTO requirements

upvoted 1 times

 **javitech83** 2 months, 3 weeks ago

Selected Answer: C

Correct is C. Is cheaper and we do not need a RTO, just RPO

upvoted 2 times

 **SmileyCloud** 3 months ago

Selected Answer: C

C - lowest cost. Otherwise A.

upvoted 1 times

 **javitech83** 2 months, 3 weeks ago

you are right, it does not state RTO so the cheaper is C

upvoted 1 times

 **Jonalb** 3 months ago

Selected Answer: A

AAAAAAAAAAAAAA

upvoted 2 times

 **nexus2020** 3 months ago

Why A is not the answer:

Global Database cost a lot more, and offer almost RPO in SECONDS, not 1 hour, so A would not meeting the 1 hour RPO and low cost.

C is the better choice.

upvoted 1 times