



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.

Correct Answer: A*Community vote distribution*

A (80%)

D (20%)

robertohyena Highly Voted 1 year, 3 months ago

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

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

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

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

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

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

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

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

upvoted 59 times

awsylum 1 year, 10 months ago

In your link, you missed this sentence:

"The most reliable, performant and low-cost approach is to share and associate private hosted zones directly to all VPCs that need them." You share the PHZ via the Shared Services VPC. You use the .2 DNS Resolver Address in each VPC to connect to the PHZ in the shared services VPC for domain resolution.

upvoted 3 times

alexkro 1 year, 9 months ago

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

upvoted 1 times

zhangyu20000 Highly Voted 3 years ago

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

upvoted 10 times

2pk Most Recent 2 weeks, 1 day ago

Selected Answer: A

A is the correct answer.

Because you should look at other sites which has these questions are available for free rather spend a fortune here. s c r i b d for example.

upvoted 1 times

 **EzKkk** 3 months, 2 weeks ago

Selected Answer: A

- For PHZ, you have to associate VPCs so it could resolve the domain
 - On-prem should be able to resolve PHZ => Need inbound endpoint
 - Use Shared Service VPC to host inbound endpoint and use Transit Gateway to manage P2P connection => Scalable solution
- upvoted 2 times

 **Ilapsiwala** 3 months, 3 weeks ago

Selected Answer: A

A: Private hosted zone should be associated with all VPCs for them to resolve cloud.example.com. Route 53 inbound resolver for on-prem to connect to route53.

No C & D: The PHZ is only associated with the shared services VPC, so other VPCs won't resolve cloud.example.com (PHZ lookups don't traverse TGW).

No B: B: Uses an EC2 conditional forwarder—adds latency, single points of failure, and admin overhead vs. the managed Resolver. Not "highest performance."

upvoted 2 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: A

Associating the private hosted zone with all VPCs ensures native name resolution inside AWS without cross-VPC resolution challenges.

Route 53 inbound resolver allows on-premises DNS servers to query Route 53 Private Hosted Zones over the Direct Connect link.

Transit Gateway connects all VPCs and on-premises to the shared services VPC hosting the inbound resolver.

This setup offers high performance and low complexity.

upvoted 2 times

 **SofieneGh** 8 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

 **CBMAN** 8 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **diazed** 8 months, 2 weeks ago

Selected Answer: A

A is correct.

upvoted 1 times

 **pekomari** 9 months, 1 week ago

Selected Answer: A

529問を全て行った結果合格できました！体感80%ほど似た問題があったので頑張ってください！

upvoted 2 times

 **mssc** 9 months, 3 weeks ago

Selected Answer: A

I have just taken the exam and 75 percent of the questions were from here. Prepare well for these Questions. Good Luck!

upvoted 3 times

 **FlyingHawk** 10 months, 3 weeks ago

Selected Answer: A

On-premises systems should be able to resolve and connect to cloud.example.com, it is inbound resolver, C is incorrect.

All VPCs will need to associate their private zones to the Transit Gateway, associated only the shared VPC with TGW forces all the DNS query from other VPCs forward to shared VPC, add the latency. D is incorrect

upvoted 1 times

 **pk0619** 1 year ago

Selected Answer: A

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.

upvoted 1 times

 **jrheen** 1 year, 1 month 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/>

upvoted 1 times

 **TariqKipkemei** 1 year, 2 months ago

Selected Answer: 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.
upvoted 1 times

 **to_to** 1 year, 2 months ago

Selected Answer: D

- 1-1. Private hosted zone One Account -> 2 Account PHZ is not Equals.
 - 1-2. VPCs in Private hosted zone
 - 2. On-Premise -> AWS Domain Name Query [Route 53 Resolver]
 - 3. Private hosted zone - Route 53 Resolver
- upvoted 1 times

 **to_to** 1 year, 2 months ago

Route 53 Resolver : inbound

upvoted 1 times

 **to_to** 1 year, 2 months ago

When I organized it slowly, I decided that it was "A" because it was attributed to an account, not a VPC.

upvoted 1 times

 **veds85** 1 year, 2 months ago

Selected Answer: A

"All VPCs and only need inbound Resolver"
upvoted 1 times

Question #2

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

Which solution will meet these requirements?

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

Correct Answer: C*Community vote distribution*

C (96%)	2%
---------	----

 **robertohyena** Highly Voted 3 years ago

C.
<https://docs.aws.amazon.com/apigateway/latest/developerguide/dns-failover.html>
 upvoted 16 times

 **leehjworking** 2 years, 8 months ago

Step1 - set up resources - Route 53 failover DNS records for the domain names
 upvoted 4 times

 **c73bf38** Highly Voted 1 year, 3 months 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 11 times

 **princajen** Most Recent 5 months, 3 weeks ago

Selected Answer: C
 Deploy a redundant stack (API Gateway + Lambda) in a second Region.

Uses Route 53 failover records, which allow DNS to direct traffic to a primary endpoint and automatically fail over to a secondary endpoint if the primary becomes unhealthy.

Enables health checks, ensuring failover is automatic and based on actual service availability.

Converts DynamoDB tables to global tables, ensuring data replication across Regions for consistency.
 upvoted 1 times

 **teeee123** 10 months, 1 week ago

Selected Answer: C
 I think C
 upvoted 1 times

 **TariqKipkemei** 1 year, 2 months ago

Selected Answer: C
 Failover routing policy – Use when you want to configure active-passive failover.
 upvoted 1 times

 **masetromain** 1 year, 3 months 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

 **Sarutobi** 1 year, 3 months 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 3 times

 **princajen** 11 months, 2 weeks ago

Multivalue is used for load balancing, not failover.

upvoted 1 times

 **edder** 1 year, 3 months ago

Selected Answer: B

The answer is B.

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

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

D: The global function is meaningless.

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

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

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

upvoted 1 times

 **ninomfr64** 1 year, 3 months ago

Selected Answer: C

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

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

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

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

upvoted 3 times

 **atirado** 1 year, 3 months ago

Selected Answer: C

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

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

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

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

upvoted 5 times

 **higashikumi** 1 year, 3 months ago

Selected Answer: C

To achieve automatic failover for the weather API, the company should deploy a duplicate API Gateway and Lambda functions in a secondary AWS region, then configure a Route 53 failover record that points to both endpoints. This failover record, combined with health checks, will automatically redirect traffic to the secondary region if the primary one fails. Additionally, converting DynamoDB tables to global tables ensures data availability in both regions, allowing the secondary API to function seamlessly during a failover.

upvoted 3 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **Helpnose** 1 year, 6 months ago

Selected Answer: D

The changes of A and C are too much, breaking the original security design.

B is wrong because answer B doesn't mention deny SCP on root level is changed. Allow on OU will not win because when allow and deny the same service, explicit deny always wins for the sake of security concerns.

upvoted 1 times

 **lighthouse85** 1 year, 7 months ago

Selected Answer: C

C, failover health

upvoted 2 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C

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

upvoted 1 times

 **MoTOne** 1 year, 9 months ago

Selected Answer: C

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

upvoted 3 times

 **abeb** 2 years, 1 month ago

C is correct

upvoted 1 times

Question #3

A company uses AWS Organizations with a single OU named Production to manage multiple accounts. All accounts are members of the Production OU. Administrators use deny list SCPs in the root of the organization to manage access to restricted services. The company recently acquired a new business unit and invited the new unit's existing AWS account to the organization. Once onboarded, the administrators of the new business unit discovered that they are not able to update existing AWS Config rules to meet the company's policies. Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?

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

Correct Answer: D*Community vote distribution*

D (64%)

B (30%)

5%

 **Snip** Highly Voted 3 years 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 52 times

 **robertohyena** Highly Voted 3 years 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 20 times

 **satya89** Most Recent 2 weeks, 4 days ago

Selected Answer: B

Option A involves removing organization-wide SCPs, which would create a security risk across all accounts.

Option C suggests converting from deny lists to allow lists, which would be a significant change to the organization's security model and potentially disruptive.

Option D involves moving the root SCP to the Production OU, which could leave the organization vulnerable at the root level and create inconsistent policy application.

Therefore, Option B represents the best solution that allows temporary access for the required changes while maintaining the organization's security posture with minimal long-term maintenance requirements.

upvoted 1 times

 **hess** 2 months, 2 weeks ago

Selected Answer: D

D is correct, as the root policy needs to be moved

upvoted 1 times

 **pkr3003** 2 months, 3 weeks ago

Selected Answer: B

 Why Option B Works (Official Logic)

AWS documentation (see Organizing AWS Accounts

) explicitly recommends using OUs for different life cycle or operational stages, such as sandbox, onboarding, production, etc.:

"You can group accounts into OUs that share common requirements. For example, you might have an OU for sandbox accounts that have fewer restrictions."

Therefore:

Creating an Onboarding OU with a more permissive SCP allows temporary relaxation of restrictions (like AWS Config updates).

Once configuration is complete, you can move the account back under the Production OU, where the standard deny-list SCPs apply.

This method avoids altering the root-level SCPs, thus keeping governance intact for existing accounts.

It also avoids additional long-term maintenance—no permanent policy changes, just a temporary OU for onboarding.

upvoted 2 times

 EzKkk 3 months, 1 week ago

Selected Answer: C

- 1, Root uses deny list
- 2, New accounts can't update Config
- 1 + 2 => Root is denying Config
- => Migrate to Root use allow so we can update Config
- => Onboard accounts
- => C

upvoted 1 times

 nayeh 5 months ago

Selected Answer: B

B is correct answer.

Question states "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." -> Hence, it's TEMPORARY onboarding issue, which is resolved by temporary OU. Once resolved, we are good to move to Production (original) OU.

Also, question states that "allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance" --> Hence, we don't want to change SCP from Root so that later on we can onboard as many OU as we need

upvoted 4 times

 princajen 5 months, 3 weeks ago

Selected Answer: D

By moving the restrictive SCP from root > Production OU, you free the Onboarding OU from that restriction.

Onboarding OU can have a permissive SCP that allows AWS Config actions.

Once setup is done, move the account to Production OU where root-level restrictions (now at Production OU) resume.

Preserves existing policies, avoids long-term complexity.

upvoted 1 times

 MasterVivek 6 months ago

Selected Answer: B

Explanation:

The company uses deny list SCPs at the root level, which means all accounts, including newly added ones, are subject to those restrictions. The new account needs temporary access to AWS Config actions to update rules, but the current SCPs are blocking that.

Option B allows for a temporary and isolated change:

By creating a separate Onboarding OU, you can apply a more permissive SCP just for that OU.

Once the necessary AWS Config changes are made, the account can be moved to the Production OU, where the standard restrictions apply.

This approach avoids modifying root-level SCPs or converting the entire policy model, which would introduce long-term maintenance overhead.

upvoted 2 times

 kvin97 6 months, 2 weeks ago

Selected Answer: D

Answer: D

But it needs to say deny list policy is moved back to the root level, after AWS config process.

upvoted 1 times

 calcinator423 7 months, 1 week ago

Selected Answer: B

Here's my take, and let me know if its wrong.

D is wrong because it suggests moving the Root SCP. This is extremely dangerous and generally not advisable, but it also implies that the Root SCP disallows AWS Config changes, which would imply previous administrators also could not change AWS Config. This is an assumption, so I would go with B.

upvoted 1 times

 MarkM1 7 months, 1 week ago

Selected Answer: B

B

A: Removing root-level SCPs would loosen security controls across all accounts and increase the risk of misconfiguration. Also, using

Service Catalog doesn't solve the issue of updating existing AWS Config rules.

C: Converting from deny list to allow list SCPs across the whole organization is a major change, hard to manage, and could unintentionally block many services. It's not recommended unless you're planning a full org-wide shift.

D: Moving the root SCP to the Production OU changes the scope of restrictions — the root SCP applies to all accounts by default. Moving it to a child OU limits its coverage, which introduces long-term security and management risks.

upvoted 1 times

 **Cps0** 1 year ago

Selected Answer: C

the question test knowledge about allow /denied inherit. all ou under root with 'deny' can't allow. So B is fail. C , D is correct but D is less operation.

upvoted 1 times

 **hspc_** 1 year ago

Selected Answer: D

For a permission to be allowed for a specific account, there must be an explicit Allow statement at every level from the root through each OU in the direct path to the account (including the target account itself).

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

upvoted 1 times

 **masetromain** 1 year, 3 months ago

Yes, in option D, the solution is to create a temporary OU named Onboarding for the new account. By creating a new OU for the new account, it allows for a new set of permissions and policies to be applied to this account, separate from the existing Production OU.

Once the new OU is created, an SCP is applied to it to allow AWS Config actions. This SCP allows the new account to make necessary adjustments to AWS Config without being blocked by the existing policies at the root level of the organization.

Then, the root SCP that is blocking these actions is moved to the Production OU, where it will continue to block these actions for all other accounts that are members of the Production OU.

Finally, once the necessary adjustments are made, the new account can be moved to the Production OU, where it will be subject to the existing policies and restrictions.

upvoted 4 times

 **masetromain** 2 years, 11 months ago

This approach is the correct solution because it allows the new account to make necessary adjustments to AWS Config while still adhering to the company's policies, and it does not introduce additional long-term maintenance. The new account will be only in the new OU temporarily, and the SCP blocking AWS Config actions will only be in the root temporarily.

upvoted 1 times

 **c73bf38** 1 year, 3 months ago

The best option to allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance would be option D:

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.

This solution involves creating a temporary OU named Onboarding for the new account and applying an SCP to the Onboarding OU that allows AWS Config actions. The organization's root SCP should be moved to the Production OU, and the new account should be moved to the Production OU when the adjustments to AWS Config are complete. This approach allows the administrators of the new account to make changes to AWS Config rules while maintaining the current policies in the Production OU.

upvoted 1 times

 **Ajani** 1 year, 3 months ago

Please note Question Constraint: Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?

Strategies for using SCPs

You can configure the service control policies (SCPs) in your organization to work as either of the following:

A deny list – actions are allowed by default, and you specify what services and actions are prohibited

An allow list – actions are prohibited by default, and you specify what services and actions are allowed.

upvoted 1 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.

Correct Answer: C*Community vote distribution*

C (96%)	4%
---------	----

 **robertohyena** Highly Voted 3 years 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 29 times

 **c73bf38** Highly Voted 1 year, 3 months 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 18 times

 **princajen** Most Recent 5 months, 3 weeks ago

Selected Answer: C

Aurora Auto Scaling for Replicas is valid and helps scale read-heavy workloads.

Sticky sessions are needed since the application is stateful.

Application Load Balancer supports both round robin and sticky sessions.

This ensures horizontal scaling of the app tier while maintaining a consistent user experience.

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: C

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

upvoted 2 times

 **masetromain** 1 year, 3 months 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

 **ninomfr64** 1 year, 3 months ago

Selected Answer: C

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

Thus C is correct

upvoted 3 times

 **atirado** 1 year, 3 months ago

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

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

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

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

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

upvoted 3 times

 **amministrazione** 1 year, 3 months ago

D. Enable Aurora Scaling for Aurora writers. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.

upvoted 1 times

 **Bereket** 1 year, 6 months ago

Selected Answer: C
C, Enable Aurora Auto Scaling for Aurora Replicas
upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C
C, Enable Aurora Auto Scaling for Aurora Replicas
upvoted 1 times

 **MoTOne** 1 year, 9 months ago

Selected Answer: C
Single writer: In an Aurora PostgreSQL DB cluster, there is only one writer instance at a time. All write operations, such as INSERT, UPDATE, and DELETE statements, are directed to the writer instance.
upvoted 4 times

 **GNB2024** 1 year, 10 months ago

Selected Answer: C
It's C
upvoted 1 times

 **liux99** 1 year, 12 months ago

B, D are distractor, as there is no writer replica in aurora autoscale.
NLB does not support sticky session so A is out. The answer is C.
upvoted 2 times

rhinozD 1 year, 10 months ago

NLB Sticky Session: <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#sticky-sessions>
upvoted 2 times

 **abeb** 2 years, 1 month ago

C Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the round robin routing and sticky session
upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: C
Aurora - AS only for read replicas. NLB doesn't support the least outstanding requests or round-robin algorithms, only flow hash is supported.
upvoted 1 times

 **ansgohar** 2 years, 3 months ago

Selected Answer: C

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

upvoted 1 times

 **rsn** 2 years, 3 months ago

Selected Answer: A

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

upvoted 2 times

 **Ganshank** 2 years, 3 months ago

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

Your call.

upvoted 3 times

Question #5

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

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

Which solution will meet these requirements?

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

Correct Answer: A*Community vote distribution*

A (37%)	D (28%)	C (19%)	Other
---------	---------	---------	-------

 **EricZhang** Highly Voted 3 years 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 64 times

 **RyGuy2025** 10 months, 4 weeks ago

If you read the solution - it does not reference a CloudFront Function, it references a Cloud Front Distribution, which is not the same. That is why B is the best answer.

upvoted 1 times

 **RyGuy2025** 10 months, 4 weeks ago

Where the function is integrated - it is already past the ALB.

upvoted 1 times

 **vn_thanhung** 2 years, 4 months 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 13 times

 **masetromain** Highly Voted 3 years ago

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

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

upvoted 32 times

 **vn_thanhung** 2 years, 4 months ago

Agree D

upvoted 5 times

 **nynomfr64** 2 years ago

Agree on D, but also CloudFront Function can manipulate headers

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cloudfront-functions.html#:~:text=cache%20hit%20ratio.-,Header%20manipulation,-%E2%80%93%20You%20can%20insert>

upvoted 3 times

 **apk123457890** Most Recent 3 weeks, 2 days ago

Selected Answer: D

D is the correct answer because -

The company needs serverless and the ability to modify response headers based on User-Agent.

Lambda@Edge is the only option that allows you to inspect and modify response headers at the edge before sending them to the client.

CloudFront provides global distribution and caching, and ALB can route requests to the correct Lambda function.

This approach replicates the on-premises behavior (removing headers for older devices) but in a fully managed, scalable, serverless way.
upvoted 1 times

 **jhxetc** 1 month ago

Selected Answer: A

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

A CloudFront Function is capable of modifying both response and request header content. Since this question mentions nothing about "global" or "low latency" or any of those keywords, it would be best to assume least cost to get the job done.

B. Is incorrect because modifying the default gateway response is going to mess with that header for everything and we only want it on the old devices.

C. Is incorrect because HTTP API does not support response template mapping - only REST API supports that. Had it said response parameters, I would be tempted to go for C.

D. Works - but is overkill and likely slower in the long run. Again, read the docs:

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

upvoted 1 times

 **ysyau** 1 month, 2 weeks ago

Selected Answer: D

A CloudFront Function running on a viewer response event does NOT receive the original request object.

It only receives the response object.

So you can do:

- Add headers
- Remove headers
- Edit headers

But you CANNOT say:

"Check User-Agent from the request, then modify the response."

Because on a viewer response event, CloudFront Functions don't have the User-Agent anymore. That context is gone.

Lambda@Edge is different. On a viewer response event, Lambda@Edge still gets both:

- event.request
- event.response

upvoted 1 times

 **Chris_W_1234** 2 months, 3 weeks ago

Selected Answer: C

The question states the company wants to implement serverless technologies. ALB is not serverless, API gateway is. Mapping templates allow for modifying response headers based on certain input values.

See <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-override-request-response-parameters.html>

upvoted 2 times

 **EzKkk** 3 months, 1 week ago

Selected Answer: C

I think either one is good, but the customer wanted to implement modernize their infrastructure via serverless. New infrastructure should also be compatible with older devices, at the same time provide latest feature to newer devices. So, C is the best option because:

- It's serverless
- It uses conditional response mapping which only removes problematic headers if response is going to older devices

upvoted 4 times

 **Clive97** 3 months, 2 weeks ago

Selected Answer: C

A. Incorrect. Involves Application Load Balancer, which is not needed

B. Incorrect. REST API gateway responses allow some header customization, but they are not dynamic per User-Agent.

C. HTTP API supports response transformations (mapping templates). Can dynamically remove headers based on request data (like User-Agent). Also, it directly invokes Lambda functions. Fully serverless, clean, simplest architecture.

D. Incorrect. Introduces an ALB unnecessarily.

upvoted 3 times

 **Ilapsiwala** 3 months, 3 weeks ago

Selected Answer: C

Not A & D: ALB is not serverless (it's managed but not serverless). CloudFront Functions can only run on viewer request/response events, not origin response, and have very limited capabilities (can't manipulate response headers deeply).

Not B: REST API has default gateway responses customization, but those only affect error responses from API Gateway itself (like 403, 429). They do not let you manipulate normal Lambda integration responses.

C: HTTP APIs support integration response mapping, where you can transform/modify headers before sending them back to the client. 100% serverless (API Gateway + Lambda).

Can use User-Agent condition to remove headers selectively.

upvoted 2 times

 **Murtuza** 3 months, 4 weeks ago

Selected Answer: D

Despite the fast performance of CloudFront Functions, they are not the right tool for this job due to a critical technical limitation. The official AWS documentation confirms that a CloudFront Function triggered by a viewer response event cannot access the original request headers, including the User-Agent.

upvoted 2 times

 **Jamesbomba007** 4 months, 1 week ago

Selected Answer: C

- A. Not optimal, since we already have lambda, an ALB is not needed.
- B. REST-API can invoke Lambda directly, though, gateway responses only modify HTTP error responses (403, 500), it doesn't strip arbitrary headers in normal Lambda responses.
- C. Is correct:
HTTP API supports response mapping.
you can inspect headers (like User-Agent) and modify outgoing responses.
Direct integration with Lambda (no ALB needed).
Fully serverless
Matches the requirement exactly (strip headers before response leaves API Gateway).
- D. Overkill, and again the use of ALB is not needed, Lambda is deployed.

upvoted 1 times

 **475ded6** 4 months, 1 week ago

Selected Answer: C

(HTTP API + Lambda) is fully serverless. ALB is not serverless.
Using Lambda@Edge is overkill with higher operational cost, harder to set up.

upvoted 2 times

 **Kp002** 4 months, 3 weeks ago

Selected Answer: D

Lambda@Edge runs in the CloudFront edge locations and can modify responses before they are sent to the client — perfect for removing or rewriting headers based on the User-Agent.

upvoted 1 times

 **beeri** 4 months, 3 weeks ago

Selected Answer: D

Lambda@Edge function is AWS recommended

upvoted 1 times

 **percolate792** 5 months, 3 weeks ago

Selected Answer: D

Option D because
CloudFront Functions only support the following event types:
viewer-request
viewer-response
BUT:

In the viewer-response phase, CloudFront Functions are read-only.
You cannot modify or remove headers in the response — you can only read them.
From AWS docs:
Viewer response events are read-only. You can't change the headers or the body of the response.

upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: D

Lambda@Edge is the only option that can inspect the request (User-Agent) and modify the response (remove headers) at the edge, fulfilling all functional and architectural requirements.

upvoted 1 times

 **0dc6cac** 6 months, 1 week ago

Selected Answer: B

There is no way A or D are the answers here....ALB + lambda target groups are NOT SERVERLESS...also we don't know the exact nature of the application, it might not be efficient or even possible to use ALB + lambda, if it involves API keys or some complex routing mechanism. AWS would NEVER prefer that we use ALB + lambda TGs to do something like this.

I'd say B is most likely the answer.

upvoted 1 times

Question #6

Topic 1

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

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

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

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

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

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

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

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

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

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

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

Correct Answer: C

Community vote distribution

C (65%)

D (33%)

 **robertohyena**  1 year, 3 months ago

Answer: C & D

Source:

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

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example4.html>
upvoted 34 times

 **higashikumi**  1 year, 3 months 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 19 times

 **EzKkk**  3 months, 1 week ago

Selected Answer: C

C&D

This is a classic P2P communication in AWS, basically, origin must allows others to access its resources and others must allows said actions themselves

upvoted 1 times

 **dsatizabal** 3 months, 3 weeks ago

Selected Answer: C

Just tested and only C works, not sure why the question asks for two :S

upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: C

C &D

This explicitly grants access to User_DataProcessor in Account B.

This is how cross-account access is granted using bucket policies.

This is a valid IAM user policy that allows the user to attempt S3 actions on the external bucket.
Needed in addition to the bucket policy in Account A.

upvoted 1 times

 **anhadenpp** 8 months, 1 week ago

Selected Answer: D

Answer : CD

Detail : <https://docs.aws.amazon.com/res/latest/ug/S3-buckets-cross-account-access.html>

upvoted 1 times

 **DhirajBansal** 1 year, 1 month ago

Selected Answer: C

This policy will give access to User in B account for Bucket in A account.

upvoted 1 times

 **Jorkaef** 1 year, 1 month ago

The correct combination of steps for this scenario are:

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

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

Here's why these are the correct steps:

Step C: The bucket policy in Account A (the retail company) needs to explicitly allow access to the IAM user from Account B (the business partner). This policy grants the necessary permissions to User_DataProcessor from Account B to access the S3 bucket in Account A.

Step E: In Account B (the business partner's account), the IAM user User_DataProcessor needs to be granted permissions to access S3 resources. This IAM policy allows the user to perform the necessary S3 actions.

upvoted 3 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: C

C & D.

In Account A, set the S3 bucket policy to allow only 'User_DataProcessor' from Account B access.

In Account B, set the permissions of User_DataProcessor to allow access to S3 bucket in Account A.
upvoted 1 times

85b5b55 1 year, 2 months ago

Answer: C & D

upvoted 1 times

atirado 1 year, 3 months ago

Selected Answer: C

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

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

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

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

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

upvoted 1 times

amministrazione 1 year, 3 months ago

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

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

upvoted 1 times

dEgYnIDA 1 year, 5 months ago

Selected Answer: D

The question says Choose two. The answer is C & D.

upvoted 1 times

kpcert 1 year, 6 months ago

Selected Answer: C

Ans C and D

2 Options have to be selected

upvoted 1 times

kpcert 1 year, 6 months ago

Ans - C and D

2 Options have to be selected

upvoted 1 times

MoTOne 1 year, 9 months ago

Selected Answer: C

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

upvoted 1 times

Dgix 1 year, 10 months ago

C and D.

upvoted 1 times

Question #7

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

Which solution will meet these requirements MOST cost-effectively?

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

Correct Answer: B*Community vote distribution*

B (71%)	A (24%)	3%
---------	---------	----

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

Selected Answer: B

B. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto scaled Amazon Elastic Container Service (Amazon ECS) clusters with the Fargate launch type to handle the expected load. Deploy tasks from the ECR images. Configure two separate Application Load Balancers to direct traffic to the ECS clusters.
 This option meets the requirement of using a serverless architecture by utilizing the Fargate launch type for the ECS clusters, which allows for automatic scaling of the containers based on the expected load. It also allows for separate deployments for production and testing by configuring separate ECS clusters and Application Load Balancers for each environment. This option also minimizes operational complexity by utilizing ECS and Fargate for the container orchestration and scaling.

upvoted 23 times

  **zhangyu20000** Highly Voted 3 years ago

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

upvoted 17 times

  **masetromain** 3 years ago

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

upvoted 3 times

  **anita_student** 2 years, 10 months ago

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

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

upvoted 5 times

  **Kirkster** 11 months, 2 weeks ago

10 GB is ENORMOUS for a container image. Even most Windows Server OS container images (which won't work in Lambda anyway) are smaller than that, and it's very very rare to see a Linux container image over ~1 GB (typically they are a few hundred MB)

upvoted 1 times

  **zhangyu20000** 3 years ago

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

upvoted 3 times

  **anita_student** 2 years, 10 months ago

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

upvoted 5 times

  **Kirkster** 11 months, 2 weeks ago

Of course you can run web applications from Lambda, with API Gateway (or Lambda HTTP URL) in front of it. You have to refactor a little, unless you're using ASP.NET Core, which can run nearly unmodified in Lambda using the Amazon.Lambda.AspNetCoreServer package.

upvoted 1 times

✉ **yuyuyuyu** 2 years, 12 months ago

I do not think A is the right answer.
Because image must be upload to the ECR.
upvoted 4 times

✉ **EzKkk** [Most Recent] 3 months, 1 week ago

Selected Answer: A

Cheapest and full serverless

upvoted 1 times

✉ **475ded6** 4 months, 1 week ago

Selected Answer: A

Option A is the most cost-effective and best meets the requirements because:

It uses AWS Lambda with container images, providing a fully serverless architecture for microservices.
API Gateway routes requests to separate production and testing Lambda functions, ensuring distinct environments.
upvoted 1 times

✉ **Jennie95** 4 months, 1 week ago

Selected Answer: B

"To create a Lambda function from a container image, build your image locally and upload it to an Amazon Elastic Container Registry (Amazon ECR) repository."

<https://docs.aws.amazon.com/lambda/latest/dg/images-create.html>

Thus A is not correct so must be B

upvoted 1 times

✉ **dzhuang** 4 months, 2 weeks ago

Selected Answer: A

The Point is in the question: The company needs to refactor the application as microservices that run on containers. sure A
upvoted 1 times

✉ **aszd** 4 months, 3 weeks ago

Selected Answer: A

💡 Why A is correct for SAP-C02:
Lambda does support container images up to 10 GB
→ This is official AWS functionality:
<https://docs.aws.amazon.com/lambda/latest/dg/images-create.html>

You don't need ECS or ECR (explicitly) in the answer
→ AWS Lambda can pull container images from Amazon ECR, which is implied.

The exam doesn't test whether the image is in ECR — only that you can deploy containers to Lambda, which is true.

"Most cost-effective" and "serverless" are the key exam keywords
→ Lambda has zero idle cost, no infra to manage, and automatic scaling
→ ECS/EKS/Fargate introduce ALBs, networking, cluster logic = more cost and complexity

You can run web apps in Lambda
→ Especially with API Gateway in front
→ Even frameworks like ASP.NET Core can run with slight adaptation
upvoted 2 times

✉ **percolate792** 5 months, 3 weeks ago

Selected Answer: B

Appropriate answer is B

upvoted 1 times

✉ **princajen** 5 months, 3 weeks ago

Selected Answer: A

While both A and B are valid real-world solutions, A is more aligned with:

Cost-effectiveness
Simplicity
AWS exam preference for serverless-first solutions
Container support with Lambda
upvoted 2 times

✉ **BIKEBUG** 5 months, 3 weeks ago

Selected Answer: A

AWS Lambda now supports container images (up to 10 GB), so you can package your microservices as containers and run them serverlessly. As per the needs in the question, it ticks the boxes of low operational complexity and low cost. However there is one catch. Lambda can be used only for runtimes <=15 min. So if the containerised applications need to run > 15min per invocation, then option B. Since the questions doesn't specifically talk about any timing, i would stick with A

upvoted 2 times

 **sasivarenan** 6 months, 1 week ago

Selected Answer: B

A is definitely no for hosting web applications, web applications typically make multiple HTTP requests where stick session are required which is not supported by API Gateway. So B looks perfect

upvoted 1 times

 **0dc6cac** 6 months, 2 weeks ago

Selected Answer: A

I think it's A, you can upload docker images to lambda, and it's serverless. I don't think ECS can count as serverless in this case.

upvoted 1 times

 **ThanhNgao** 5 months, 2 weeks ago

Fargate is serverless

upvoted 1 times

 **rhuanca** 6 months, 3 weeks ago

Selected Answer: A

looks like now since 2020 lambda support container images

https://aws.amazon.com/blogs/aws/new-for-aws-lambda-container-image-support/?utm_source=chatgpt.com

upvoted 2 times

 **SBoksh** 7 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/lambda/latest/dg/images-create.html>

upvoted 1 times

 **zhen234** 10 months, 3 weeks ago

Selected Answer: A

most cost-effective and least operational overhead

upvoted 1 times

 **Kirkster** 11 months, 2 weeks ago

Selected Answer: B

I was initially torn between A and B, but answer A says to upload the container image to Lambda, which isn't possible - to use a container with Lambda, you still upload the image to ECR. Answer D (Beanstalk) isn't the most cost-effective for running containers.

So between B and C (ECS vs EKS), ECS has less operational overhead, and also doesn't require the master node to be running, which means ECS will likely be very slightly cheaper, and have less operational work.

upvoted 1 times

 **fbukevin** 12 months ago

Selected Answer: B

At the time I consider B & C without doubt. But finally consider to migration efforts, I choose B. I don't really consider the cost between B & C.

upvoted 1 times

Question #8

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

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

What should a solutions architect recommend to meet these requirements?

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

Correct Answer: B

Community vote distribution

B (100%)

 **masetromain** Highly Voted 3 years ago

Selected Answer: B

I go with B

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

upvoted 19 times

 **masetromain** 2 years, 11 months ago

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

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

upvoted 17 times

 **princajen** Most Recent 5 months, 3 weeks ago

Selected Answer: B

Goal: Failover from primary Region to backup Region in under 15 minutes, cost-effectively.

Multi-tier app, running on EC2 behind an ALB, with Auto Scaling.

RDS Multi-AZ in primary, with a read replica in backup Region.

Route 53 is used for DNS-based routing to the app endpoint.

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: B

Option B is the least costly active-passive strategy

upvoted 1 times

 **Untamables** 1 year, 3 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

 **higashikumi** 1 year, 3 months 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

 **atirado** 1 year, 3 months ago

Selected Answer: B

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

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

Option C - This option implements an active-active strategy

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

upvoted 4 times

 **GreyBox1** 1 year, 3 months ago

Selected Answer: B

B is right.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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

upvoted 1 times

 **Bereket** 1 year, 6 months ago

Selected Answer: B

Correct answer B

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: B

B for sure

upvoted 1 times

 **Vaibs099** 1 year, 11 months ago

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

upvoted 1 times

 **ftaws** 1 year, 11 months ago

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

upvoted 1 times

 **rhinozD** 1 year, 10 months ago

What about RDS failover?

You need lambda to promote read replica.

upvoted 1 times

 **ninomfr64** 2 years ago

Selected Answer: B

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

upvoted 1 times

 **jainparag1** 2 years, 1 month ago

Selected Answer: B

B satisfies all the requirements.
upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: B
Health check is a metric, hence alarms can be executed, and alarms are integrated with SNS, SNS integrated with lambda. This sounds weird, but it will work.
upvoted 1 times

 **ansgohar** 2 years, 3 months ago

Selected Answer: B
B. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Configure Route 53 with a health check that monitors the web application and sends an Amazon Simple Notification Service (Amazon SNS) notification to the Lambda function when the health check status is unhealthy. Update the application's Route 53 record with a failover policy that routes traffic to the ALB in the backup Region when a health check failure occurs.
upvoted 2 times

 **dimitry_khan_arc** 2 years, 4 months ago

Selected Answer: B
Health check+SNS. This does not need to have active-active which satisfy the requirement.
upvoted 1 times

Question #9

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

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

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

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

Correct Answer: ADF

Community vote distribution

ADF (98%)

✉️  **masetromain** [Highly Voted] 3 years ago

Selected Answer: ADF

I go with ADF
<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html>
 upvoted 18 times

✉️  **spencer_sharp** 3 years ago

Why C is wrong?
 upvoted 3 times

✉️  **Karamen** 2 years, 4 months ago

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

✉️  **masetromain** 2 years, 11 months ago

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

✉️  **God_Is_Love** 2 years, 10 months ago

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

✉️  **dtha1002** 2 years, 7 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** 1 year, 3 months ago

- A. Using an Elastic Load Balancer (ELB) to distribute traffic across multiple EC2 instances can help ensure that the application remains available in the event that one of the instances becomes unavailable. By configuring the instances as part of an Auto Scaling group with a minimum capacity of two instances, you can ensure that there is always at least one healthy instance to handle traffic.
- D. Modifying the DB instance to create a Multi-AZ deployment that extends across two availability zones can help ensure that the database remains available in the event of a failure. In the event of a failure, traffic will automatically be directed to the secondary availability zone, reducing the amount of downtime.
- F. Creating a replication group for the ElastiCache for Redis cluster and enabling Multi-AZ can help ensure that the in-memory data store remains available in the event of a failure. This will allow traffic to be automatically directed to the secondary availability zone, reducing the amount of downtime.

upvoted 11 times

✉ EzKkk Most Recent 3 months, 1 week ago

Selected Answer: ADF

ADF

- A, ELB to distribute traffic, 2 instances mean no downtime
- B, DB across AZ so if one AZ fail, another will be active to receive traffic
- F, Same idea with B

upvoted 1 times

✉ EzKkk 3 months, 1 week ago

Sorry, it's D not B

upvoted 1 times

✉ princajen 5 months, 3 weeks ago

Selected Answer: ADF

To increase high availability and fault tolerance for a critical application running on EC2, ElastiCache, and RDS, you must ensure recovery and redundancy across all three tiers.

upvoted 1 times

✉ teeee123 10 months, 1 week ago

Selected Answer: ADF

ADF try it

upvoted 1 times

✉ TariqKipkemei 1 year, 1 month ago

Selected Answer: ADF

Key words: each piece of the infrastructure must be healthy and must be in an active state, can automatically recover = Auto Scaling group and Multi-AZ deployment

upvoted 1 times

✉ higashikumi 1 year, 3 months 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

✉ marszalekm 1 year, 11 months ago

There isn't such a thing like "Auto Scaling group for the ElastiCache for Redis", there is a "Replication Group"

upvoted 2 times

✉ Maja1 1 year, 3 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 4 times

✉ atirado 1 year, 3 months ago

Selected Answer: ADF

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

Option B - No such thing as EC2 Unlimited Mode

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

Option D - Provides a place to fail over to

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

Option F - Provides a place to fail over to

Choose A, D, F

upvoted 2 times

✉  **eboehm** 1 month ago

Apparently there is a such thing as unlimited mode... but it doesn't solve availability... its for performance on T family instances
upvoted 1 times

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

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.
D. Modify the DB instance to create a Multi-AZ deployment that extends across two Availability Zones.
F. Create a replication group for the ElastiCache for Redis cluster. Enable Multi-AZ on the cluster.
upvoted 1 times

✉  **joshnort** 1 year, 7 months ago

Selected Answer: ADF

Satisfies the High Availability requirement on the EC2 instance, Amazon RDS for MariaDB DB instance, and ElastiCache for Redis cluster
upvoted 1 times

✉  **gofavad926** 1 year, 9 months ago

Selected Answer: ADF

ADF, as mentioned in the other comments
upvoted 1 times

✉  **DmitriKonnovNN** 1 year, 11 months ago

"The infrastructure can automatically recover from failure with the least possible downtime",
to me this sounds rather resilient than highly-available, since it focuses on MTTR but not explicitly on up-time.
upvoted 1 times

✉  **severlight** 2 years, 1 month ago

Selected Answer: ADF

obvious
upvoted 1 times

✉  **ansgohar** 2 years, 3 months ago

Selected Answer: ADF

A, D, F
upvoted 1 times

✉  **NikkyDicky** 2 years, 6 months ago

Selected Answer: ADF

it's of course ADF
upvoted 1 times

✉  **Parimal1983** 2 years, 6 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** 2 years, 7 months ago

ADF will meet the described provisions
upvoted 1 times

Question #10

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

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

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

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

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

Correct Answer: AE*Community vote distribution*

AE (90%) 7%

 **Raj40** Highly Voted 3 years ago

A & E
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GeneratingCustomErrorResponse.html#custom-error-pages-procedure>
 upvoted 37 times

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

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

Option B - This option requires a lot of set up

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

Option D - This option requires a lot of set up

Option E - This option helps: Shows a custom error page when the error occurs
 upvoted 11 times

 **mellefinho** Most Recent 2 months ago

Selected Answer: AE
 A & E
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GeneratingCustomErrorResponse.html#custom-error-pages-procedure>
 upvoted 1 times

 **EzKkk** 3 months, 1 week ago

Selected Answer: AC
 The key here is LEAST OPERATIONAL OVERHEAD so A&E is definitely out of the question because in order for this to work, you have to reconfigure the behavior of CloudFront, create OAC for the distribution to work with a specific error code. It's very complex.

On the other hand, A&C is much more straight forward, the idea is Route 53 will do the health check with the requested resource i.e CloudFront distribution and trigger failover record if the distribution is unhealthy.

upvoted 1 times

 **Chris_W_1234** 2 months, 3 weeks ago

The scenario states that the application immediately and successfully loads when the user refreshes the browser. A health check such as in C would direct users to the error page for a longer period of time, until future health checks have succeeded again. Until then, ALL users will receive error pages. In effect, you will make the user experience worse.

upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: AE

Amazon S3 to host the custom error page (cheap, serverless)

Amazon CloudFront to intercept 502 responses from the ALB and redirect users to the custom error page

upvoted 1 times

 **5e8c031** 6 months, 1 week ago

Selected Answer: AE

Any answer consisting of modifying the ALB forwarding rules because it will modify the behaviour of the system for all users, even those who did not get a HTTP 502. Any answer involving Route 53 will not work because it supposes that the DNS cache on clients expires before it takes effect, and it will effect all users, even those who did not get a HTTP 502.

Using a CloudFront custom error page is the only workable option that will serve the custom error page only in the event of a HTTP 502

upvoted 1 times

 **ausl** 7 months, 3 weeks ago

Selected Answer: AE

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

upvoted 1 times

 **teeee123** 10 months, 1 week ago

Selected Answer: AE

Maybe A and E

upvoted 1 times

 **hoef03** 1 year, 2 months ago

Selected Answer: AC

AC, because for E to work, another s3 origin needs to be created, (OAI when not static website), and a behaviour for the path routing to the error html.. Also unclear what the "DNS record modification" is made for.

upvoted 1 times

 **Parimal1983** 1 year, 3 months ago

Selected Answer: AE

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

upvoted 2 times

 **Sarutobi** 1 year, 3 months ago

Selected Answer: AE

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

upvoted 5 times

 **dev112233xx** 1 year, 3 months ago

Selected Answer: AE

A&E are the correct answers imo

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. Create an Amazon S3 bucket. Configure the S3 bucket to host a static webpage. Upload the custom error pages to Amazon S3.
E. Add a custom error response by configuring a CloudFront custom error page. Modify DNS records to point to a publicly accessible web page.

upvoted 1 times

 **agatim** 1 year, 5 months ago

Selected Answer: AC

Option A - Allow us to expose a error page with low effort.

Option B - Requires a lot of set up

Option C - Allow us to redirect all the traffic to our error page exposed by S3 in case of errors.

Option D - requires a lot of set up

Option E - Custom Error Pages in CloudFront refers to the same Origin (in our case the Load Balancer) so it does not work with all the other answers.

So correct answer are A and C

upvoted 2 times

 **roger8t8** 1 year, 6 months ago

A & E

<https://aws.amazon.com/blogs/aws/custom-error-pages-and-responses-for-amazon-cloudfront/>

upvoted 1 times

 **azhar3128** 1 year, 6 months ago

I think it is wordplay. Option A says to upload "error pages", which will be an overhead for creating a page for each error and unnecessary. that's where C & E are correct

upvoted 4 times

 **shmoeee** 11 months, 3 weeks ago

my exact thoughts. Why not use already available pages

upvoted 1 times

 **iulian0585** 1 year, 7 months ago

Selected Answer: AE

A and E according to AWS documentation:

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

upvoted 1 times

Question #11

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

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

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

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

Correct Answer: BD*Community vote distribution*

BD (83%)

Other

 **masetromain** Highly Voted 3 years ago

Selected Answer: BD

I go with BD

upvoted 29 times

 **masetromain** 2 years, 11 months ago

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

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

upvoted 16 times

 **8693a49** 1 year, 5 months ago

Note that B says it enables sharing from the management account, but the infrastructure team must use the infrastructure account to manage the network", so there is nothing to share from the management account. Also, options D and E also enable resource sharing (you don't need to enable it from the management account, other accounts can enable resource sharing too).

VPCs can't talk to each other by default. You need to do something to 'glue' them together in a larger network.

upvoted 2 times

 **Kirkster** 11 months, 2 weeks ago

In this case, there is actually only one VPC - the one in the infrastructure account. Users in other accounts deploy to subnets in that account, as those subnets are shared using resource sharing, as outlined in this blog:

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

upvoted 1 times

 **razguru** Highly Voted 3 years 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 12 times

 **8693a49** 1 year, 5 months ago

There are multiple VPCs because each account must have at least one.

upvoted 4 times

 **Chris_W_1234** 2 months, 3 weeks ago

Not true. You can delete the default VPC in an account. The scenario mentions there is only one VPC, the one in the infra account, and that VPC gets shared with the other, "regular" accounts.

upvoted 1 times

 **aszd** Most Recent 4 months, 3 weeks ago

Selected Answer: BD

Why A is not necessary in this scenario:
A transit gateway is useful if:

You have multiple VPCs to connect

You need centralized routing between VPCs

But in this scenario:

The question only talks about sharing one VPC from the infrastructure account

There's no requirement for VPC-to-VPC communication

upvoted 3 times

princajen 5 months, 3 weeks ago

Selected Answer: BD

RAM sharing across AWS Organizations (must be enabled once).

d. is how you share subnets so other can deploy resources into the VPC without managing networking.

upvoted 1 times

Curious76 7 months, 2 weeks ago

Selected Answer: AD

A. Create a transit gateway in the infrastructure account.

AWS Transit Gateway allows multiple accounts to connect to a single shared network efficiently.

AWS Resource Access Manager (RAM) lets the infrastructure team share subnets with other accounts.

upvoted 1 times

unbornfroyo 8 months, 1 week ago

Selected Answer: AD

A. Transit Gateway in Infrastructure Account

A transit gateway (TGW) allows centralized, scalable network connectivity between VPCs across accounts.

Hosting the TGW in the infrastructure account ensures centralized control of routing and traffic flow, while allowing other accounts to connect through attachments.

D. RAM Share of Subnets

Use AWS Resource Access Manager (RAM) in the infrastructure account to share subnets with specific AWS accounts or OUs in the organization.

This allows other accounts to launch resources (like EC2 instances) into shared subnets without being able to modify the network itself.

upvoted 1 times

Kirkster 11 months, 2 weeks ago

Selected Answer: BD

The transit gateway is a red herring. Creating a resource share and then sharing out subnets is described in this AWS blog:

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

To those who say there are multiple VPCs (one in each account), read the question more carefully - it never says that. It merely says that users in the other accounts need to be able to deploy resources to the shared subnets.

upvoted 1 times

_KBM 1 year ago

Selected Answer: AD

A. Create a transit gateway in the infrastructure account.

A transit gateway allows the infrastructure account to centralize the network and connect multiple VPCs across accounts. It serves as the backbone for communication between the accounts.

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.

Using AWS Resource Access Manager (RAM), you can share the subnets of the infrastructure account's VPC with other accounts in the organization, enabling individual accounts to create resources in those subnets while centralizing network management in the infrastructure account.

upvoted 1 times

wem 1 year ago

Selected Answer: AD

The following steps will meet the requirements for sharing a common network managed from the infrastructure account across multiple AWS accounts, with the least operational complexity and in line with best practices:

A. Create a transit gateway in the infrastructure account.

A transit gateway allows centralized routing and connectivity between multiple VPCs across different AWS accounts. This approach enables the infrastructure account to control network management while allowing other accounts to use the shared network.

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.

Using AWS Resource Access Manager (RAM) to share subnets from the infrastructure account allows individual accounts to create resources within those subnets. This aligns with the requirement that individual accounts can create resources but not manage the network.

upvoted 1 times

 **Heman31in** 1 year ago

Selected Answer: AD

Without Step A (transit gateway), the solution would lack a central mechanism for connecting VPCs across accounts, which is essential for a shared network. D because: AWS Resource Access Manager (RAM) allows you to share VPC subnets across accounts. By creating a resource share for specific subnets and associating it with the appropriate organizational units (OUs), individual accounts can launch resources in the shared subnets while the infrastructure account retains network control.

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: BD

Enable resource sharing from the AWS Organizations management account then, 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.

upvoted 1 times

 **Sin_Dan** 1 year, 2 months ago

The correct answer is A and D.
B is a wrong option.

While AWS Organizations is required to manage multiple accounts, enabling resource sharing through AWS RAM is done in the infrastructure account (where the VPC resides), not in the AWS Organizations management account. Resource sharing is configured via RAM in the account that owns the resources, not through Organizations directly.

upvoted 2 times

 **SkyZeroZx** 1 year, 3 months 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

 **sreed77** 1 year, 3 months ago

Selected Answer: BD

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

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

Here are the steps involved in implementing this solution:

Create a resource share in RAM in the infrastructure account.

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

Select each subnet to associate with the resource share.

Assign permissions to the resource share.

upvoted 4 times

 **cnetthers** 1 year, 3 months ago

I would go BD

When you share a subnet using AWS Resource Access Manager (RAM) with another AWS account, the resources within that shared subnet can communicate with each other and with the resources in the account that owns the subnet. However, for outbound network connectivity to other VPCs, on-premises networks, or the internet, you need to set up additional networking components.

upvoted 1 times

 **cnetthers** 1 year, 3 months ago

2. Inter-VPC Communication:

o If the resources in the shared subnet need to communicate with resources in another VPC (either within the same AWS account or in

a different AWS account), you can use VPC Peering or a Transit Gateway.

o VPC Peering: Establish a peering connection between the VPCs and update the route tables accordingly.

o Transit Gateway: Create a Transit Gateway, attach both VPCs to the Transit Gateway, and configure the necessary route tables and Transit Gateway route tables.

upvoted 1 times

✉ **cnethe** 1 year, 6 months ago

3. On-Premises Connectivity:

o If the resources in the shared subnet need to communicate with an on-premises network, you can use AWS Direct Connect or a Site-to-Site VPN.

o These connections can be routed through a Transit Gateway for more scalable and manageable network architecture.

upvoted 1 times

✉ **cnethe** 1 year, 6 months ago

Here's a breakdown of different scenarios and the required setup:

1. Internet Access:

o If you need resources in the shared subnet to access the internet, ensure that the subnet is a public subnet with an associated Internet Gateway (IGW) and appropriate route table entries.

o The account that owns the VPC will typically manage the IGW and the route tables.

upvoted 1 times

✉ **shaaam80** 1 year, 3 months ago

Selected Answer: BD

Answer - B & D.

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

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

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

upvoted 3 times

✉ **Sin_Dan** 1 year, 2 months ago

How do you think the Accounts got subnets without VPCs?

upvoted 1 times

✉ **severlight** 1 year, 3 months ago

Selected Answer: BD

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

upvoted 2 times

✉ **mattfaz** 1 year, 2 months ago

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

upvoted 1 times

✉ **8693a49** 1 year, 5 months ago

You don't share a prefix list, you associate it with the shared resource (which here is a TGW). The way you do it is you add the prefixes to the route tables inside the account's VPCs. The prefixes will point towards the TGW. This makes the network traffic destined to other account go through the TGW into these accounts based on the TGW routing table. The TGW routing table can only be controlled from the infrastructure account.

upvoted 2 times

Question #12

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

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

Which solution meets these requirements?

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

Correct Answer: A*Community vote distribution*

A (92%)	8%
---------	----

 **Raj40** Highly Voted 3 years ago

Selected Answer: A

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

upvoted 20 times

 **masetromain** Highly Voted 3 years ago

Selected Answer: A

I go with A

upvoted 8 times

 **masetromain** 2 years, 11 months ago

A. Create an AWS PrivateLink interface VPC endpoint. Connect this endpoint to the endpoint service that the third-party SaaS application provides. Create a security group to limit the access to the endpoint. Associate the security group with the endpoint. This solution uses AWS PrivateLink, which creates a secure and private connection between the company's VPC and the third-party SaaS application VPC, without the traffic traversing the internet. The use of a security group and limiting access to the endpoint service conforms to the principle of least privilege.

upvoted 11 times

 **EzKkk** Most Recent 3 months, 1 week ago

Selected Answer: A

Honestly, I think this is a badly phrased question because it doesn't provide any information regarding the SaaS other than "API" endpoint which could be public RESTful API endpoint to be called over the internet or PrivateLink VPC endpoint. In order to answer this question, we have to make a lot of speculations and rule out incorrect answers rather than finding a correct one. Option B is used for hybrid cloud setup so it's false. Option C require a P2P connection which couldn't be done because we don't own the VPC in which SaaS resides. Option D reverse the role of our infrastructure and SaaS provider, now we are the provider and SaaS is the consumer. Therefore, the only option left is A.

upvoted 2 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: A

Use AWS PrivateLink to connect securely and privately to the SaaS app without traversing the internet -- with fine-grained security group control to maintain least privilege.

upvoted 1 times

 **2aldous** 1 year, 3 months ago

Selected Answer: A

Access SaaS products through AWS PrivateLink is the answer.

upvoted 1 times

 **SkyZeroZx** 1 year, 3 months ago

Selected Answer: A

Create an AWS PrivateLink interface VPC endpoint.

upvoted 1 times

NikkyDicky 1 year, 3 months ago

Selected Answer: A

it s a

upvoted 1 times

cattle_rei 1 year, 3 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

shaaam80 1 year, 3 months ago

Selected Answer: A

Answer - A.

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

AWS Private Link VPC endpoint to access the SaaS application.

upvoted 1 times

atirado 1 year, 3 months ago

Selected Answer: A

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

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

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

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

upvoted 3 times

gofavad926 1 year, 3 months ago

Selected Answer: A

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

upvoted 1 times

amministrazione 1 year, 3 months ago

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

upvoted 1 times

severlight 2 years, 1 month ago

Selected Answer: A

obvious

upvoted 1 times

senthilsekaran 2 years, 1 month ago

Correct Answer : A

upvoted 1 times

task_7 2 years, 3 months 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 4 times

Jassybang_a 1 year, 10 months ago

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

upvoted 1 times

whenthan 2 years, 4 months 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

mfsec 2 years, 9 months ago

Selected Answer: A

Create an AWS PrivateLink interface VPC endpoint.

upvoted 1 times

Question #13

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

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

Correct Answer: A

Community vote distribution

A (100%)

✉  **masetromain**  3 years ago

Selected Answer: A

A is good

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

upvoted 15 times

✉  **masetromain** 2 years, 11 months ago

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

upvoted 15 times

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

Selected Answer: A

Use AWS Systems Manager for patch automation and compliance reporting across EC2 and on-premises servers.

upvoted 1 times

✉  **TariqKipkemei** 1 year, 1 month ago

Selected Answer: A

Use AWS Systems Manager update, manage, and configure Amazon EC2 instances, edge devices, on-premises servers, and virtual machines (VMs).

upvoted 1 times

✉  **atirado** 1 year, 3 months ago

Selected Answer: A

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

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

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

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

upvoted 1 times

✉  **MoTOne** 1 year, 3 months ago

Selected Answer: A

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

upvoted 1 times

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

Selected Answer: A

obvious

upvoted 1 times

 **whenthan** 1 year, 3 months ago

Selected Answer: A

A is correct

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. Use AWS Systems Manager to manage patches on the on-premises servers and EC2 instances. Use Systems Manager to generate patch compliance reports.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A is the correct answer

upvoted 1 times

 **stevegod0** 2 years, 5 months ago

A is correct:

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

upvoted 1 times

 **cattle_rei** 2 years, 5 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** 2 years, 6 months ago

Selected Answer: A

yep - A

upvoted 1 times

 **EricZhang** 2 years, 7 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** 2 years, 7 months ago

Selected Answer: A

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

upvoted 2 times

 **2aldous** 2 years, 8 months ago

Selected Answer: A

Easy question :)

A is the answer.

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: A

Use AWS Systems Manager to manage patches

upvoted 1 times

 **kiran15789** 2 years, 9 months ago

Selected Answer: A

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

upvoted 1 times

Question #14

Topic 1

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

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

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

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

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

upvoted 14 times

 **rtgfdv3** Highly Voted 3 years ago

Selected Answer: B

<https://aws.amazon.com/blogs/infrastructure-and-automation/run-code-before-terminating-an-ec2-auto-scaling-instance/>
upvoted 8 times

 **princaben** Most Recent 5 months, 3 weeks ago

Selected Answer: B

Lifecycle hook pauses instance termination.

EventBridge detects the lifecycle event.

Lambda uses Systems Manager SendCommand to execute on the instance, copying logs to S3.

Once logs are copied, it sends CONTINUE to the Auto Scaling group.

Fully automated, graceful, and scales properly.

upvoted 1 times

 **pk0619** 1 year ago

Selected Answer: B

This is most accurate with redundancy as EventBridge can directly invoke SSM Document and you don't need Lambda function.
upvoted 1 times

 **Shanmahi** 1 year ago

Selected Answer: B

B using systems manager
upvoted 1 times

 **atirado** 1 year, 3 months ago

Selected Answer: B

Option A - This option might not work: Preventing ASG termination could create further trouble and there is no guarantee the script will run if the instance happens to be unhealthy

Option B - This option could work: Running the script from the SSM API guarantees the script will run, using EventBridge to capture the ASG termination event provides a perfect place to hook in the call to SSM which will also pause the termination until the script runs. Then CONTINUE allows the ASG termination to continue.

Option C - This option does not work because it does not solve the problem: Terminating instances within the 15 minute window causes log files to be lost.

Option D - This option might not work: It does not rely on EventBridge to detect the ASG termination event. It also could create further trouble because no other actions will be performed due to sending ABANDON though nothing is said about other actions in the question

upvoted 6 times

 **F_Eldin** 1 year, 3 months 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 3 times

 **gameoflove** 1 year, 3 months 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

 **cattle_rei** 1 year, 3 months 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

 **ansgohar** 1 year, 3 months ago

Selected Answer: B

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

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: B

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

upvoted 2 times

 **cattle_rei** 2 years, 4 months 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** 2 years, 4 months ago

Selected Answer: B

d is wrong, shouldn't be "ABANDON"

upvoted 2 times

 **NikkyDicky** 2 years, 6 months ago

Selected Answer: B

it's a B

upvoted 1 times

 **2aldous** 2 years, 8 months ago

Selected Answer: B

B.

Smart solution :)

upvoted 3 times

Question #15

Topic 1

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

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

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

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

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

Correct Answer: CE*Community vote distribution*

CE (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: CE

C and E are correct.

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

E. Associate a new VPC in Account B with a hosted zone in Account A. Delete the association authorization in Account A. This step is necessary because the association authorization needs to be removed in Account A after the association is done in Account B.

upvoted 37 times

 **kiran15789** Highly Voted 2 years, 9 months ago

Selected Answer: CE

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-associate-vpcs-different-accounts.html>
upvoted 12 times

 **princajen** Most Recent 5 months, 3 weeks ago

Selected Answer: CE

These steps will enable DNS resolution of db.example.com from EC2 instances in Account B via cross-account private hosted zone sharing.
upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: CE

Associate the new VPC in Account B with the hosted zone in Account A, delete the association authorization in Account A. Then create an authorization to associate the private hosted zone in Account A with the new VPC in Account B.
upvoted 1 times

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

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

CloudFloater 1 year, 3 months 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 5 times

whenthan 1 year, 3 months 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

liuliangzhou 1 year, 3 months ago

Selected Answer: CE

A account's DNS Zone authorization is associated with B's VPC, and after B's VPC is associated with A's Private Zone, A's authorization permission is deleted for security reasons.

upvoted 1 times

amministrazione 1 year, 3 months ago

- C. Create an authorization to associate the private hosted zone in Account A with the new VPC in Account B.
- E. Associate a new VPC in Account B with a hosted zone in Account A. Delete the association authorization in Account A.

upvoted 1 times

7f6aef3 1 year, 8 months ago

Selected Answer: CE

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

upvoted 1 times

8608f25 1 year, 10 months ago

Selected Answer: CE

Correct answers

upvoted 1 times

8608f25 1 year, 3 months ago

Explanation:

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

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

upvoted 4 times

8608f25 1 year, 10 months ago

Why the others are incorrect:

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

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

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

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

upvoted 3 times

atirado 2 years ago

Selected Answer: CE

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

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

Option C - This option contributes to the solution.

Option D - Breaks the company's architecture

Option E - This option contributes to the solution

upvoted 1 times

severlight 2 years, 1 month ago

Selected Answer: CE

obvious

upvoted 1 times

SfQ 2 years, 2 months ago

Selected Answer: CE

C and E are correct.

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

upvoted 1 times

Chainshark 2 years, 2 months ago

Why is B marked as correct?

upvoted 2 times

SfQ 2 years, 2 months ago

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

upvoted 2 times

NikkyDicky 2 years, 6 months ago

Selected Answer: CE

it's CE

upvoted 1 times

Jonalb 2 years, 6 months ago

Selected Answer: CE

ccccccccccccceeeeeeeeeeeeee

upvoted 1 times

Question #16

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

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

Correct Answer: C*Community vote distribution*

C (92%) 8%

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

Selected Answer: C

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

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

upvoted 30 times

 **spencer_sharp** Highly Voted 3 years ago

Selected Answer: C

No brainer

upvoted 9 times

 **mellefinho** Most Recent 1 month, 3 weeks ago

Selected Answer: C

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

upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: C

Move videos to Amazon S3

Set up CloudFront to serve them

Continue using EC2 + ALB + EFS for blog pages, but offload heavy static content (videos). to S3/CloudFront.

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: C

video ,unstructured content = Amazon S3

resolve buffering and timeout issues = Amazon CloudFront distribution

upvoted 1 times

 **ninomfr64** 1 year, 3 months ago

Selected Answer: C

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

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

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

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

upvoted 3 times

 **ninomfr64** 2 years ago

Also this follows AWS best practices to separate static content from dynamic content allowing for better scalability
upvoted 2 times

 **atirado** 1 year, 3 months ago

Selected Answer: C

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

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

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

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

upvoted 2 times

 **amministrazione** 1 year, 3 months ago

C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
upvoted 1 times

 **Bereket** 1 year, 6 months ago

Selected Answer: D

The most cost-efficient and scalable deployment that will resolve the issues for users, given the requirements and the described scenario, is:

D. Set up an Amazon CloudFront distribution for all site contents, and point the distribution at the ALB.
upvoted 2 times

 **Christophe_** 1 year, 10 months ago

Selected Answer: D

Option C - Does not support new content added later by users, does not accelerate site content

Option D - Accelerate site and videos, allow content added

upvoted 2 times

 **e4bc18e** 1 year, 9 months ago

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

upvoted 2 times

 **geekos** 2 years ago

Selected Answer: C

C is good

upvoted 1 times

 **abeb** 2 years, 1 month ago

C is good

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: C

obvious

upvoted 1 times

 **cattle_rei** 2 years, 3 months 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 years, 5 months ago

Selected Answer: D

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

upvoted 2 times

 **totopopo** 2 years, 5 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** 2 years, 6 months ago

C more cost efficient

upvoted 1 times

 **karim_arous** 2 years, 6 months ago

Selected Answer: C

C without a doubt

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.

Correct Answer: A

Community vote distribution

A (100%)

 **masetromain**  1 year, 3 months ago

Selected Answer: A

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

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

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

It also provides automatic failover and routing capabilities.

upvoted 26 times

 **anita_student** 2 years, 10 months ago

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

upvoted 9 times

 **AMohanty** 2 years, 3 months ago

Transit GW - connects both over Private VIF and Transit VIF

upvoted 1 times

 **masetromain** 2 years, 11 months ago

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

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

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

upvoted 17 times

 **Sarutobi** 2 years, 10 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 2 times

 **Sarutobi** 2 years, 10 months ago

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

upvoted 1 times

 **kz407**  1 year, 9 months ago

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

upvoted 6 times

 **EzKkk**  3 months ago

Selected Answer: A

The keyword is "expands into other Regions". DXGW is a global resource so you don't have to create one for each region, making it the only viable solution for scaling.

upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: A

Use a Direct Connect Gateway to:

Enable redundant connections.

Support multi-Region VPC connectivity.

Provide a future-proof, scalable architecture.

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: A

'must provide connectivity to other Regions through the same pair of Direct Connect connections'= Direct Connect gateway

upvoted 1 times

 **atirado** 1 year, 3 months ago

Selected Answer: A

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

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

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

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

upvoted 2 times

 **ninomfr64** 1 year, 3 months ago

Selected Answer: A

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

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

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

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

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

upvoted 6 times

 **arthurmeirelessm** 11 months, 1 week ago

Por que Direct Connect Gateway nao forneceria conectividade a outras regiões?

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **MoTOne** 1 year, 9 months ago

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

upvoted 1 times

 **KyleZheng** 1 year, 12 months ago

A

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

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: A

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

upvoted 3 times

 **severlight** 2 years, 1 month ago

Selected Answer: A
multiple regions - dx gateway
upvoted 1 times

 **AMohanty** 2 years, 3 months 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** 2 years, 4 months ago

Selected Answer: A
<https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/>
upvoted 1 times

 **NikkyDicky** 2 years, 6 months ago

Selected Answer: A
It's A.
D is not supported
upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: A
A
keyword === Direct Connect gateway
upvoted 1 times

 **gameoflove** 2 years, 7 months ago

Selected Answer: A
A. Is the Correct Option as Direct Connect Gateway with Private Virtual Interface will meet the requirement
upvoted 1 times

Question #18

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

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

Which solution meets these requirements?

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

Correct Answer: C*Community vote distribution*

C (84%)

Other

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

Selected Answer: C

This solution meets the requirements by using multiple managed services offered by AWS which can reduce the operational overhead. Hosting the web application in Amazon S3 would make it highly available, scalable and can handle variable traffic. The uploaded videos can be stored in S3 and processed using S3 event notifications that trigger a Lambda function, which calls the Amazon Rekognition API to categorize the videos. SQS can be used to process the event notifications and also it is a managed service. This solution eliminates the need to manage EC2 instances, EBS volumes and the custom software. Additionally, using Lambda function in this case, eliminates the need for managing additional servers to process the SQS queue which will reduce operational overhead.

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

upvoted 35 times

 **Chris_W_1234** 2 months, 3 weeks ago

Assuming the website is 100% static (could be SPA), A could work but the answer leaves out crucial aspects, like how the static website would upload the files to S3. Presigned URLs? Where would they come from? Half-baked answer IMO.

upvoted 1 times

 **Mahakali** 2 years, 3 months ago

Any explanation on option A ?

upvoted 1 times

 **AWSum1** 1 year, 3 months ago

ECS is managed to an extent, but the question fails to elaborate, no mention of fargate etc. There's unnecessary mentions of spot instances to confuse you. The web application has static content which can be hosted in S3 instead of ECS

upvoted 2 times

 **RaghavendraPrakash** Highly Voted 2 years, 8 months 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 14 times

 **gofavad926** 1 year, 9 months ago

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

upvoted 2 times

 **Arnaud92** 2 years, 3 months ago

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

upvoted 3 times

 **Boops** 2 years, 3 months ago

"The website contains static content"

Contains do not means that all the website is just static

upvoted 1 times

 **Six_Fingered_Jose** 2 years, 3 months ago

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

upvoted 10 times

 **jpa8300** 1 year, 12 months ago

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

upvoted 2 times

 **Kirkster** 11 months, 2 weeks ago

You absolutely can host a static website in Amazon S3, I do it all the time (you create DNS records pointing to the S3 bucket), although putting CloudFront in front of it would be better. S3 web hosting even allows custom 404 error pages, and selecting a default (index.html) page, etc.

upvoted 1 times

 **EzKkk** Most Recent 3 months ago

Selected Answer: C

Comparing C and D is very hard tbh, option C offers a fully managed service solution but it has way more overhead compared to option D. If you need further computation, let's say for a backend server, you will have to set up a Lambda function or a bunch of Lambda functions behind an API Gateway and you have to manually monitor it. Meanwhile, option D offers better flexibility and scalability since you're working with basically EC2 only which means your concern is regarding ONLY ONE component.

Both options offer somewhat right and somewhat wrong to the question so I will roll my dice C since I like a decoupled system :D

upvoted 2 times

 **generic_aws_dude** 3 months, 3 weeks ago

Selected Answer: B

This question is a bit weird for me. While it does say the website contains static content, it does not mean the web application can run in Cloudfront+S3. Let's say the web application that allows users to upload video is running on a JS framework using server-side rendering or it's a Spring Boot App. Some of the content maybe static but not all.

This is more of a "static" = S3 + Cloudfront mentality. Ugh, kinda set a bad precedent

upvoted 1 times

 **dsatizabal** 4 months ago

Selected Answer: D

How can we refuse the idea of using Beanstalk? S3 website is static and I guess limited, if we add other components we'd be adding overhead, we can have a dynamic site deployed over Beanstalk and in the same codebase we can have the listener or worker process for the SQS queue, this ensures a fully managed service that offers a variety of deployment options and monitoring tools and integrations

upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: C

Option C offers a modern, serverless, highly scalable, and cost-efficient architecture using fully managed AWS services that handle everything from video storage to processing and categorization, with minimal operational burden.

upvoted 1 times

 **Kirkster** 11 months, 2 weeks ago

Selected Answer: C

Answer A doesn't really address the operational burden, and the Spot instance stuff is a distractor. Answer C (hosting the static website in S3, along with the videos, and switching to Rekognition with S3 events) provides the most reduction in operational burden, and as a plus is also going to be the lowest-cost solution.

upvoted 1 times

 **Drake17** 1 year ago

Selected Answer: C

The Amazon Rekognition Video API facilitates the analysis of videos either stored in an Amazon S3 bucket or streamed via Amazon Kinesis Video Streams.

<https://docs.aws.amazon.com/rekognition/latest/dg/how-it-works-operations-intro.html>

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: C

'static website' = Amazon S3

'store videos' = Amazon S3

'video analysis' = Amazon Rekognition

'reduce operational overhead, managed service' = S3 events, AWS Lambda, Amazon SQS

upvoted 1 times

✉  **cudbyanc** 1 year, 3 months ago

Selected Answer: C

The answer is 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. Instead, Amazon S3 can host the web application, and store the uploaded videos, which can trigger S3 event notifications to send messages to the SQS queue. Then, an AWS Lambda function can process the messages in the SQS queue and use Amazon Rekognition API to categorize the videos. This approach also takes advantage of AWS-managed services, such as S3, SQS, and Lambda, which reduces operational overhead and dependency on third-party software.

upvoted 5 times

✉  **Bereket** 1 year, 3 months ago

Selected Answer: C

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.

Explanation:

Hosting the Web Application in Amazon S3:

Cost-effective and Scalable: Amazon S3 is a cost-effective and scalable solution for hosting static web content. It can handle variable traffic efficiently without the need to manage servers.

Static Content Hosting: Ideal for serving static content like HTML, CSS, JavaScript, and media files.

upvoted 1 times

✉  **kz407** 1 year, 3 months ago

Selected Answer: C

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

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

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

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

1. Move storage of files to S3.
2. Eliminate the BE codebase, revamp the FE codebase to rely entirely on AWS JS SDK and handle file uploads with that. Now you don't need to manage any compute resources at all.
3. Go about the rest of the solution.

upvoted 1 times

✉  **924641e** 1 year, 3 months ago

Selected Answer: C

The mention of static content really throws this question off and clearly the community thinks this as well. The argument of static website vs static content being the key to selecting D isn't really a strong argument but that doesn't exclude D from being a viable solution.

Operational overhead is minimized with Elastic Beanstalk and removes dependencies on third party tools/software.

upvoted 2 times

✉  **24Gel** 1 year, 9 months ago

thanks, this is the best explain

upvoted 1 times

✉  **grire974** 1 year, 3 months ago

Selected Answer: C

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

upvoted 1 times

✉  **grire974** 1 year, 11 months ago

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

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

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

upvoted 2 times

✉  **generic_aws_dude** 3 months, 3 weeks ago

Ok, this is the reason why C is correct. Rekognition API can't access files in EFS

upvoted 1 times

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

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.

upvoted 1 times

✉  **ff32d79** 1 year, 4 months ago

I saw this question in other question bank (owner of the questions) and it is A, reason is assuming is moving files back and forth cannot be static page, so it is A.

upvoted 1 times

 Helpnonsense 1 year, 6 months ago

Selected Answer: C

Only Answer C is the solution that covers all the requirements, where the videos are stored, how SQS messages are produced and consumed, how web app is hosted.

upvoted 1 times

Question #19

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

How can this be accomplished?

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

Correct Answer: B

Community vote distribution

B (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: B

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

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

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

upvoted 31 times

 **princajen** Most Recent 5 months, 3 weeks ago

Selected Answer: B

Option. B offers a safe, automated, and fast deployment and rollback strategy using native AWS tools designed for serverless applications. It dramatically reduces operational burden, risk, and downtime compared to manual or partially automated approaches.

upvoted 1 times

 **calcinator423** 7 months, 1 week ago

Selected Answer: B

A and D are just obviously wrong bc they said "reduce time to deploy" and cloudformation is very very slow.

B and C are effectively the same answer, but B uses automatic, serverless, managed architecture, and C is using manual CLI scripts and manual reverting. Generally, manual anything is discouraged.

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: B

keywords:

'Code deployment, reduce deployment time, rollback, serverless' = AWS Serverless Application Model, AWS CodeDeploy

upvoted 2 times

 **5up3rm4n** 1 year, 3 months 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 3 times

 **atirado** 1 year, 3 months ago

Selected Answer: B

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

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

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

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

upvoted 3 times

 **AWSum1** 1 year, 3 months ago

Selected Answer: B

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

Pretty much what the question wants

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **AwsZora** 1 year, 6 months ago

why not a?

upvoted 2 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: B

B, use SAM to deploy serverless applications on aws

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: B

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

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: B

obvious

upvoted 1 times

 **whenthan** 2 years, 4 months ago

Selected Answer: B

requirmeents :

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

upvoted 1 times

 **NikkyDicky** 2 years, 6 months ago

Selected Answer: B

B no do0ubt

upvoted 1 times

 **Jonalb** 2 years, 6 months ago

Selected Answer: B

100% B

upvoted 1 times

 **gameoflove** 2 years, 7 months ago

Selected Answer: B

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

 **2aldous** 2 years, 8 months 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

Question #20

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

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

Which solution will meet these requirements at the LOWEST cost?

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

Correct Answer: A*Community vote distribution*

A (58%)

D (40%)

 **tman22** Highly Voted 3 years ago

A - Glacier Deep Archive can't be used for web hosting, regardless if the company says retrieval time is no concern.
upvoted 43 times

 **tman22** 3 years 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 18 times

 **zhangyu20000** Highly Voted 3 years 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 23 times

 **apk123457890** Most Recent 3 weeks, 1 day ago

Selected Answer: D

D. S3 Glacier Deep Archive + Interface Endpoint

Glacier Deep Archive is the cheapest storage class in AWS for long-term archival.
Retrieval is slow (hours), but that's acceptable here.
Private access via S3 interface endpoint ensures no public exposure.
Website hosting is unnecessary but can be ignored if bucket policy restricts access.
Cost: Lowest among all options → Correct choice.
upvoted 1 times

 **jhxetc** 1 month ago

Selected Answer: D

D. Is the correct answer. The reason for configuring website hosting is so that DNS can be used with the intranet domain name, not to actually serve content as a website. This allows people to request the document and return when it is restored. It is by far the most cost effective option and frankly, whenever a question uses the terms "no concern on retrieval time," Glacier is the answer they are going for.
upvoted 1 times

 **eboehm** 1 month ago

Selected Answer: C

Its really interesting reading all of these answers. I honestly think this question is messed up or intended to really trick you. No one in all of these answers ever mention that if you use static web hosting you CANNOT connect it to an s3 interface endpoint. This makes C the only valid low cost option.
upvoted 1 times

 **b0969fd** 2 months, 1 week ago

Selected Answer: A

Ok, for those answering D, try to create an S3 bucket and "configure the S3 bucket to use the S3 Glacier Deep Archive storage class as default."

upvoted 1 times

 **OM_mero** 2 months, 3 weeks ago

Selected Answer: D

speed of retrieval are not concerns of the company, so defiantly it's D .

upvoted 1 times

 **arisa_seobomi** 3 months ago

Selected Answer: A

I tried it out.

I uploaded identical HTML files to an S3 bucket, specifying each storage class.

When using the Glacier storage class, I received a 403 error when accessing the web.

Therefore, the answer is the One Zone-Infrequent Access (S3 One Zone-IA) storage class, and option A is correct.

upvoted 3 times

 **seyik** 2 months, 3 weeks ago

Glacier and Glacier Deep Archive objects are not immediately readable. You must restore them before GET works. Hitting them via a website endpoint will return 403 until a restore completes.

upvoted 1 times

 **17Master** 3 months, 1 week ago

Selected Answer: D

No menciona appweb, pero si menciona "La disponibilidad y la velocidad de recuperación no son preocupaciones de la empresa".

upvoted 1 times

 **Nano6** 4 months, 2 weeks ago

Selected Answer: D

A (S3 One Zone-IA): More expensive than Glacier Deep Archive for long-term archival.

B (EFS One Zone-IA) & C (EBS sc1): Higher cost for large archival storage, unnecessary compute.

upvoted 1 times

 **strike3test** 5 months, 2 weeks ago

Selected Answer: D

Although option D mentions configuring the S3 bucket for website hosting, the key part is restricting access via an S3 VPC endpoint, ensuring data is not publicly exposed. The website hosting configuration can be ignored or omitted if only intranet access is required, or simply means enabling bucket policies for the intranet use

upvoted 1 times

 **strike3test** 5 months, 2 weeks ago

Selected Answer: A

There is no practical way to serve a website directly from Glacier Deep Archive storage class objects due to retrieval delays and costs.

upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: D

Even though Option D includes a technically incompatible feature (website hosting), the rest of the solution matches the requirements best - lowest cost, secure private access, and appropriate storage class.

upvoted 2 times

 **sergza888** 5 months, 4 weeks ago

Selected Answer: A

i liked D but it has "Configure the S3 bucket for website hosting." as part of the answer and that is a deal breaker You can not do it if you configured your Bucket as Glacier deep

upvoted 1 times

 **Kaps443** 6 months, 3 weeks ago

Selected Answer: A

All components work, supports website hosting, low cost

upvoted 1 times

 **thiagodotoli** 7 months, 1 week ago

Selected Answer: D

A questão não aborda hospedagem. A intranet já existe e fará a consulta no S3. Geralmente armazenamento MENOR custo e que não tenha tempo de recuperação a resposta é o Glaciar.

upvoted 1 times

 **calcinator423** 7 months, 1 week ago

Selected Answer: D

"speed of retrieval does not matter" = s3 glacier deep archive. Although S3 Glacier Deep Archive can't be used for website hosting, you also don't need it because you're accessing the documents via the S3 interface endpoint via the intranet.

upvoted 1 times

Question #21

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

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

Which solution will meet these requirements?

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

Correct Answer: A*Community vote distribution*

A (81%)

Other

 **masetromain**  2 years, 11 months ago

Selected Answer: A

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

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

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

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

upvoted 32 times

 **masetromain** 2 years, 11 months ago

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

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

upvoted 2 times

 **bititan**  2 years, 11 months ago

Selected Answer: A

A is has options for SAML and SCIM configuration with AD

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

D is openID based, MS AD would not support this

so I go with A

upvoted 14 times

 **trap** 2 years, 1 month ago

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

upvoted 3 times

 **trap** 2 years, 1 month ago

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

 **gonzjo52** 1 year, 8 months ago

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

 **princajen** Most Recent 5 months, 3 weeks ago

Selected Answer: A

Option A provides:

Centralized identity management with Active Directory.

Scalable access across AWS accounts using IAM Identity Center + ABAC.

Automated provisioning via SCIM.

Integration with existing VPN connectivity.

upvoted 1 times

 **Heman31in** 1 year ago

Selected Answer: A

SCIM v2.0 in the Context of AWS SSO and Active Directory

When using AWS IAM Identity Center (AWS SSO) with Active Directory, SCIM v2.0 is utilized to automatically provision and de-provision users and groups. This eliminates the need for manual user or group management and ensures that changes in your on-premises AD are reflected in AWS SSO.

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: A

keywords:

'Use active directory to sign in Aws accounts' = AWS IAM Identity Center (AWS Single Sign-On) , SAML 2.0
'conditional access to the accounts based on user groups and roles' = AWS IAM (ABAC)

upvoted 3 times

 **Ashu_0007** 1 year, 4 months ago

AWS IAM Identity Center + SAML

upvoted 1 times

 **Vaibs099** 1 year, 11 months ago

A is correct

Reasons -

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

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

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

upvoted 3 times

 **atirado** 2 years ago

Selected Answer: D

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

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

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

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

upvoted 2 times

 **ninomfr64** 2 years ago

Selected Answer: B

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

Now, with AWS IdC we need ADFS and while ADFS does not support SCIM, it is possible to still have your users and groups automatically synchronize with the IAM IDC by using the SCIM API and PowerShell as per <https://aws.amazon.com/blogs/modernizing-with-aws-identity-and-access-management-iam/>

aws/synchronize-active-directory-users-to-aws-iam-identity-center-using-scim-and-powershell/#:~:text=While%20ADFS%20does%20not%20support,the%20SCIM%20API%20and%20PowerShell.

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

upvoted 2 times

 **nynomfr64** 1 year, 11 months ago

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

upvoted 1 times

 **924641e** 2 years ago

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

upvoted 3 times

 **subupro** 2 years ago

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

upvoted 1 times

 **siasiasia** 2 years, 1 month ago

Selected Answer: C

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

upvoted 1 times

 **gonzjo52** 1 year, 8 months ago

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

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

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

upvoted 1 times

 **sizzla83** 2 years, 1 month ago

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

upvoted 1 times

 **nynomfr64** 2 years ago

Agree with you on B, but:

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

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

upvoted 1 times

 **enk** 2 years, 1 month ago

Selected Answer: A

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

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: A

federated IdP is required and access to multiple accounts

upvoted 1 times

 **trap** 2 years, 1 month ago

Answer A and B are wrong!!!

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

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

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

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

<https://help.okta.com/en-us/content/topics/directory/ad-agent-manage-users-groups.htm>
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_aws-accounts.html

upvoted 3 times

 **M4D3V1L** 2 years, 2 months ago

Selected Answer: A

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

upvoted 1 times

Question #22

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

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

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

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

Correct Answer: B*Community vote distribution*

B (77%)

A (22%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: B

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

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

upvoted 49 times

 **masetromain** 2 years, 11 months ago

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

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

upvoted 16 times

 **zhangyu20000** Highly Voted 2 years, 12 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

 **Chris_W_1234** Most Recent 2 months, 3 weeks ago

Selected Answer: B

Not A: Solution mentions descriptive error message when the scenario asks for errors not to be shown.

B: The problem is with PUT calls, which points to a bottleneck in DynamoDB. Throttling the high-use client will keep enough DynamoDB write capacity for all other low-use clients. Also, solution mentions that application handles 429 "without error" (presumably retries, just like A).

Not C: PUT calls can't be cached (or at least it doesn't make sense here).

Not D: The problem is with DynamoDB write capacity, not with Lambda functions not scaling up quickly enough.

upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: B

Use API Gateway throttling + usage plans to fairly distribute access and protect your system from high request rates by individual clients. Option B provides a targeted and scalable fix that meets both technical and business goals.

upvoted 1 times

 **HajaMydin** 7 months ago

Selected Answer: B

Why B is the best solution:

Problem Summary:

Increased errors during PUT requests.

Caused by a single client generating a high volume of requests.

The API is noncritical, and retries are acceptable.

Errors are affecting customer experience and API reputation.

Solution Breakdown:

API Gateway usage plans allow you to throttle requests by API key, limiting the impact of a noisy or abusive client.

Throttling results in HTTP 429 (Too Many Requests) responses.

Clients can be coded to recognize 429 responses and retry with backoff, which improves customer experience while maintaining control.

This approach protects backend systems like Lambda and DynamoDB from being overloaded.

upvoted 1 times

 **f3f4935** 8 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: B

keywords:

'A large number of the PUT requests' = API throttling

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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

upvoted 1 times

 **Ashu_0007** 1 year, 4 months ago

API gateway throttling

upvoted 1 times

 **Jason666888** 1 year, 4 months ago

Selected Answer: B

Key word: a large number of the PUT requests, one client

Seeing this will ring a bell on throttling on API Gateway. But normally you also need to make sure when the client side see "429 too many attempts", the app can capture that error code and show some reasonable error message(e.g. You have sent too many requests .Please try again later)

upvoted 2 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: B

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

upvoted 1 times

 **anubha.agrahari** 1 year, 9 months ago

Selected Answer: B

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

upvoted 1 times

 **duriselvan** 1 year, 10 months ago

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

upvoted 1 times

 **AimarLeo** 1 year, 10 months ago

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

upvoted 2 times

 **bjexamprep** 1 year, 11 months ago

Selected Answer: A

There is no evidence indicating the problem is with the throughput. If it is throughput, other clients will have similar problem.

And "the errors are displayed to customers and are causing damage to the API's reputation.", this means the solution should be able to reduce the error message showed on the client side, while, throttling the client will actually close the service for this particular client, which is against the "clients can tolerate retries of unsuccessful calls".

I vote A for this question.

upvoted 1 times

 **sarfraz_khan** 2 years ago

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

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

upvoted 1 times

 **atirado** 2 years ago

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

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

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

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

upvoted 2 times

Question #23

Topic 1

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

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

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

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

Correct Answer: A*Community vote distribution*

A (86%) 14%

 **sambb** Highly Voted 2 years, 10 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 if you can install a gateway in AWS, but Amazon would never advise this

upvoted 25 times

 **b3llman** 2 years, 4 months ago

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

 **Chainshark** 2 years, 2 months ago

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

 **dqwsmtwwvtgxwkvgcvc** 2 years, 4 months ago

There is one S3 file gateway

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

upvoted 1 times

 **Tofu13** 2 years, 3 months ago

<https://aws.amazon.com/blogs/storage/new-enhancements-for-moving-data-between-amazon-fsx-for-lustre-and-amazon-s3/>
 upvoted 3 times

 **chico2023** Highly Voted 2 years, 4 months 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 16 times

 **princajen** Most Recent 5 months, 3 weeks ago

Selected Answer: A

Option A delivers:

Massive cost savings (thanks to S3 Intelligent-Tiering and ephemeral FSx).

High Performance for compute-intensive workloads.

Scalability and simplicity using managed AWS services.

upvoted 1 times

 **diazed** 8 months, 2 weeks ago

Selected Answer: A

With our S3 objects imported into our Lustre file system, we can now lazy-load the files we need by simply reading the particular files. After a file is lazy-loaded, its contents are fully copied from S3 onto the Amazon FSx for Lustre file system, where it can be accessed with extremely low latency. I will go for A. <https://aws.amazon.com/blogs/storage/new-enhancements-for-moving-data-between-amazon-fsx-for-lustre-and-amazon-s3/>

upvoted 1 times

 **SIJUTHOMASP** 12 months ago

Selected Answer: D

I lean more towards D but I am not sure whether the Gateway is only intended for on-premise as few are mentioning here. If that is not the case then the right option is D.

upvoted 1 times

 **zaxxon** 1 year ago

Selected Answer: D

FSx for Lustre, is only for Linux where in the question is Linux noted. It's states only EC2 instance not which OS is on it!

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: A

'The job runs once monthly', 'cost reduction' = S3 Intelligent-Tiering storage class, lazy loading.

'Scalable file system', 'shared file system', 'data-intensive' = Amazon FSx for Lustre

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: A

By choosing Option A, the company can leverage the cost-effectiveness of Amazon S3 Intelligent-Tiering for storage and the high performance of Amazon FSx for Lustre for temporary file access, while minimizing the overall cost by creating and deleting the file system only when needed.

Option B (using Amazon EBS Multi-Attach) is not ideal because EBS volumes are designed for persistent storage, and attaching and detaching a large volume to multiple instances can be time-consuming and potentially disruptive.

Option C (using Amazon FSx for Lustre with batch loading) is less cost-effective than Option A because batch loading requires loading the entire 200 TB of data into the file system, which can be expensive and time-consuming.

Option D (using AWS Storage Gateway File Gateway) is not the most cost-effective solution because the File Gateway is designed for on-premises file storage integration and may not provide the same level of performance as FSx for Lustre for this data-intensive workload.

upvoted 2 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

A or D : confusion. I wish they can provide explanation about their answers when it is not the most voted one

upvoted 1 times

 **Helpnosense** 1 year, 6 months ago

I vote D instead A because the requirement in the question is "modifies the data on the shared file system" Fsx imported data from s3 and lost the relationship to s3 after import is done Without explicitly copy back to s3, the change stays on shared file system only. Answer A solution doesn't provide a step to copy the modification back to s3.

Storage gateway presents s3 storage to the OS as shared file system. Any modification on the shared file system will be automatically saved on s3.

upvoted 3 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A: Lazy loading is cost-effective because only a subset of data is used at every job
upvoted 1 times

 **kz407** 1 year, 9 months ago

Selected Answer: A

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

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

Compute resources are residing in AWS, so having Storage GW and File GW won't solve a thing.
As far as option B is concerned, it comes down to the limitations of EBS (such as the max block size, and max number of instance that can be attached etc). Also, attaching and detaching of the EBS volumes seems a bit complicated too. On top of that, EBS does not offer the cost optimizations offered by S3 Intelligent Tiering. The question clearly mentions that only a subset of the data will be used. Intelligent tiering ensures a substantial cost optimization over time.
Hence, the answer should be A.

upvoted 3 times

 **kspendli** 1 year, 9 months ago

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

upvoted 1 times

 **anubha.agrahari** 1 year, 9 months ago

Selected Answer: A

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

upvoted 2 times

 **atirado** 2 years ago

Selected Answer: A

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

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

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

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

upvoted 2 times

 **AimarLeo** 1 year, 11 months ago

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

upvoted 1 times

 **ninomfr64** 2 years ago

Not B because using EBS still involves EC2 instances that are expensive (the instances that host the shared file system run continuously).

Also, multi-attach is supported only for io1/oi2 EBS disk types that are expensive;

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

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

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

upvoted 1 times

Question #24

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

Assuming that resources are deployed in multiple Availability Zones in a single Region, which solution will meet these requirements?

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

Correct Answer: C*Community vote distribution*

C (96%)	4%
---------	----

 **God_Is_Love** Highly Voted  2 years, 10 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 14 times

 **masetromain** Highly Voted  2 years, 11 months ago

Selected Answer: C

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

upvoted 6 times

 **dsatizabal** Most Recent  4 months ago

Selected Answer: D

How could EC2 without ASG be more highly available than ECS?

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

keywords:

'TCP', 'fixed address', 'regional' = NLB

upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Answer is C

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: C

By choosing Option C, the company can meet the requirements of high availability, redundancy across Availability Zones, accessibility through a DNS name (my.service.com), and fixed IP address assignments that can be added to allow lists by other companies.

Option A is not suitable because it involves creating Elastic IP addresses for each EC2 instance, which can become difficult to manage and does not provide the desired DNS name accessibility.

Option B is not appropriate because it uses an Amazon ECS cluster with public IP addresses, which may not provide the desired fixed IP addresses for allow listing by other companies.

Option D is not the correct choice because it uses an Application Load Balancer (ALB), which is designed for HTTP/HTTPS traffic and may not be the best fit for a TCP-based service. Additionally, it involves creating public IP addresses for each host in the ECS cluster, which can be complex and may not provide the desired fixed IP addresses for allow listing.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **Ashu_0007** 1 year, 4 months ago

Ec2+NLB

upvoted 1 times

 **Alawi_Amazon_AWS** 1 year, 8 months ago

A looks ok

<https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/Strategies.html>

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C

C: NLB with elastic IPs

upvoted 1 times

 **Vaibs099** 1 year, 11 months ago

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

upvoted 1 times

 **sammyhaj** 1 year, 11 months ago

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

upvoted 1 times

 **Simon523** 2 years, 3 months ago

Selected Answer: C

Other option haven't mention multi AZ

upvoted 1 times

 **Christina666** 2 years, 5 months ago

Selected Answer: C

Static IP-> NLB

upvoted 1 times

 **NikkyDicky** 2 years, 6 months ago

Selected Answer: C

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

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: C

Create one Elastic IP address for each Availability Zone.

upvoted 2 times

 **AWS_Sam** 2 years, 7 months ago

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

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

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

upvoted 2 times

Question #25

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

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

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

Which solution will meet these requirements MOST cost-effectively?

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

Correct Answer: D*Community vote distribution*

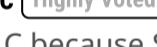
D (88%)

11%

 **_lasco_**  2 years, 10 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 27 times

 **joefromnc**  2 years, 4 months ago

Can not be C because Savings Plans require long term commitment.
upvoted 7 times

 **fifi1907**  4 months, 3 weeks ago

Selected Answer: A

no one vote A?
upvoted 1 times

 **generic_aws_dude** 3 months, 3 weeks ago

If anything with AWS, 3 AZ's are better 2 because of the keyword "high availability"
upvoted 1 times

 **BennyMao** 9 months, 3 weeks ago

Selected Answer: C

Savings Plans provide cost savings compared to On-Demand while ensuring predictable compute resources for scheduled jobs with tight SLAs. Balanced distribution of On-Demand and Spot Instances across AZs ensures redundancy and cost-effectiveness.
upvoted 1 times

 **TariqKipkemei** 1 year, 1 month ago

Selected Answer: D

keywords:
'65%, more than half of the instances must continue to meet SLAs' = On-demand instances with capacity reservations.
'cost-effectively' = spot instances.
upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.
upvoted 1 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: C

I vote C.

The 65% of scheduled jobs is the portion of the total work load. I don't believe it's SLA since SLA will be 99.99% or more. The jobs is hourly from 0.3 to 2 hours. There are 12 servers on prem. If the number of jobs per server can handle is N. Then to cover the worst situation that all the jobs run 2 hours, by given 12 servers and tight SLA, the number of hourly jobs is $12 / 2 = 6N$. Answer C has 6 servers and since the number of job per server is N then 6 server can handle $6N$ jobs match the hourly job number $6N$.

2 ec2 with saving plan + 2 spot instances is more cost effective than 3 ec2 with capacity plan(not saving a penny by capacity reservation plan) + 1 spot instance.

upvoted 2 times

 **Chris_W_1234** 2 months, 3 weeks ago

Scenario states no long-term commitment, which invalidates solution C with savings plan, which requires a commitment.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: D

D is more cost-effective than C

upvoted 2 times

 **atirado** 2 years ago

Selected Answer: D

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

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

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

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

upvoted 2 times

 **subupro** 2 years ago

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

upvoted 1 times

 **edder** 2 years, 1 month ago

Selected Answer: D

The answer is D.

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

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

C: No Savings Plan required.

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

upvoted 2 times

 **Russ99** 2 years, 4 months ago

Selected Answer: D

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

upvoted 3 times

 **ggrodsckiy** 2 years, 4 months ago

Correct C.

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

upvoted 4 times

 **joefrommc** 2 years, 4 months ago

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

upvoted 4 times

 **awsrd2023** 2 years, 5 months ago

Selected Answer: D

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

Ruling out Factors:

A. Only 2 AZ (low redundancy), all EC2 in capacity reservation (Not Cost effective as SLA requirement is in 65/35 ratio).

B. All 4 on-demand in 1 AZ (low redundancy), rest spot (Will effect tight SLA - is actually 35/65 instead of 65/35).

C. Savings Plan (Against no long term commitments requirement).

upvoted 3 times

 **NikkyDicky** 2 years, 6 months ago

Selected Answer: D

D

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

  **aca1** 2 years, 7 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** 2 years, 7 months ago**Selected Answer: C**

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

upvoted 1 times

Question #26

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

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

The application resources must be deployed through AWS CloudFormation.

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

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

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

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

Correct Answer: A

Community vote distribution

A (100%)

 **Untamables**  3 years 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 19 times

 **OnePunchExam** 2 years, 8 months 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 9 times

 **karma4moksha**  2 years, 7 months ago

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

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

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

upvoted 14 times

 **ftaws** 1 year, 11 months ago

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

upvoted 3 times

 **soulation** 10 months ago

Read it again more carefully: "offers managed rotation for master user credentials"

This is for application credential. Beside, even rotation for master has limitations:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-secrets-manager.html>

upvoted 1 times

 **princajen**  5 months, 3 weeks ago

Selected Answer: A

Secrets Manager is purpose-built for securely storing and rotating credentials.

Option A is the only one using native, integrated AWS services that meet all security, rotation, and automation requirements - with the lowest operational burden.

upvoted 2 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

Selected Answer: A

Secrets Manager (\$\$\$): Automatic rotation of secrets with AWS Lambda // SSM Parameter Store (\$): No secret rotation (can enable rotation using Lambda triggered by EventBridge) --> more overhead even if it is cheaper ==> Answer A

upvoted 1 times

 **ivarnarik1** 1 year, 7 months ago

Correct Answer: A

Cloudformation template::systems manager has no resource called: RotationSchedule. where as Cloudformation template::secrets manager Indeed has a resource called: RotationSchedule.

Therefore the correct answer is A only.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A is the correct answer

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: A

Option A is the most straightforward and provides the least amount of operational overhead because it leverages AWS Secrets Manager's native capabilities for secret rotation. This eliminates the need for custom rotation logic or external triggers for rotation, unlike the other options that either rely on AWS Systems Manager Parameter Store (which does not have built-in secret rotation capabilities like Secrets Manager) or require additional resources such as Amazon EventBridge or AWS AppSync for triggering rotations, which complicates the architecture and increases operational overhead.

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

upvoted 3 times

 **AimarLeo** 1 year, 10 months ago

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

upvoted 4 times

 **atirado** 2 years ago

Selected Answer: A

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

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

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

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

upvoted 4 times

 **shaaam80** 2 years ago

Selected Answer: A

Answer A. Password rotation -> Secrets Manager

upvoted 1 times

 **whenthan** 2 years, 3 months 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** 2 years, 4 months ago

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

upvoted 2 times

 **chico2023** 2 years, 4 months ago

Selected Answer: A

Answer: A

upvoted 1 times

 **NikkyDicky** 2 years, 6 months ago

Selected Answer: A

it's n A

upvoted 1 times

 **rtguru** 2 years, 7 months ago

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

upvoted 1 times

 **gameoflove** 2 years, 7 months ago

Selected Answer: A

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

upvoted 1 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.

Correct Answer: AC*Community vote distribution*

AC (82%) Other

 **Untamables**  2 years, 12 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 30 times

 **ixdb** 2 years ago

CD is right.

While this option A works for private access, it does not support public access as DynamoDB tables are not publicly accessible by default.

upvoted 2 times

 **Impromptu** 2 years ago

Option A has the ability to specify an execution role. This IAM role should have the GetItem/PutItem permissions for the given DynamoDB table. That way you can have access to your private table via the DynamoDB API while your API Gateway is publicly available.

So I agree with A and C

upvoted 3 times

 **jpa8300** 1 year, 12 months ago

You cannot choose A and C, you choose A OR C, one excludes the other. When a question says to choose two answers, one shall complement the other.

I agree that the API can integrate directly with DynamoDB, but if I have to choose two answers that complement each other, the A option cannot go with any of the others.

Saying that, the only possible choices should be C and D, you create the Lambda functions to integrate with Dynamodb and then deploy them at Edge, as extra to improve performance and latency you use Global Accelerator. Yes, it is true that this is not a requirement, but it is good to have.

upvoted 4 times

 **cegama543** 1 year, 2 months ago

A and C are compatibles. A for DynamoDB integration and C for escalation

upvoted 3 times

 **Chris_W_1234** 2 months, 3 weeks ago

If you look at other multiple-answer questions, they will state "which combination of..." if the multiple answers are required in combination. This question only asked, which solutions fulfill the requirements. No "combination".

upvoted 1 times

 **atirado**  2 years ago

Selected Answer: AC

Option A - This option might work: REST APIs can run over HTTPS and the integration type DynamoDB is possible

Option B - This option will not work: HTTP APIs do not support integration types for DynamoDB

Option C - This option will work: HTTP APIs support integration with Lambda functions

Option D - This option will not work: Lambda@Edge is a function of CloudFront

Option E - This option will not work: NLB Target groups can target Lambda functions however NLBs are not a Serverless solution (They are deployed on VPCs).

upvoted 15 times

 **CharChe** Most Recent 6 months, 2 weeks ago

Selected Answer: CD

A should be ruled out because although REST API in API GW can be used to access DynamoDB directly, accessing multiple DynamoDB tables by one single API needs a Lambda function to be created.

upvoted 1 times

 **TariqKipkemei** 8 months, 2 weeks ago

Selected Answer: AC

REST API in API Gateway supports AWS service integrations such HTTP endpoints, Lambda functions, or other AWS services including direct calls to DynamoDB without Lambda.

HTTP APIs in API Gateway only support integrations to Lambda functions.

Both options are fully serverless, support HTTPS, and scale automatically.

upvoted 1 times

 **Sin_Dan** 1 year, 2 months ago

A. Amazon API Gateway can be configured as a REST API with direct integration to DynamoDB. This is done using API Gateway's AWS integration type, allowing direct interaction with DynamoDB without needing a Lambda function in between.

C. API Gateway HTTP API can be used to route requests to AWS Lambda functions. The Lambda functions can then interact with DynamoDB to retrieve or modify data and return it to the client through the API.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. Create an Amazon API Gateway REST 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.

upvoted 1 times

 **jyrajan69** 1 year, 4 months ago

On the fact of simplicity it looks like BC, but with C there is an issue of Lambda fetching data, question does not indicate fetching, only put. So it looks like AB

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: AC

A and C

upvoted 1 times

 **Russ99** 1 year, 9 months ago

Selected Answer: CD

The solutions that meet the requirements of using a serverless architecture to make the data accessible publicly through a simple API over HTTPS and scaling automatically in response to demand are: C AND D

upvoted 1 times

 **Russ99** 1 year, 9 months ago

Actually, Option D is out, reason: you cannot use AWS Lambda@Edge with Global accelerator

upvoted 1 times

 **JOKERO** 1 year, 9 months ago

a, c

<https://medium.com/brlink/rest-api-just-with-apigateway-and-dynamodb-8a9b0cd76b7a>

upvoted 1 times

 **anubha.agrahari** 1 year, 9 months ago

Selected Answer: A

API Gateway REST API can invoke DynamoDB directly.

upvoted 1 times

 **DmitriKonnovNN** 1 year, 10 months ago

Sometimes when multiple answers are required, they're supposed to complement each other, but sometimes these have to be just 2 valid but independent solutions... Well API GW with Rest endpoint is a valid solution, since it's had DynamoDB proxy integration lately. We use it in production, and it's a good fit, if you want to have a lot of control and features in your API GW and no lambda functions in between, reason being VTL supports a big set of mutations which is enough to us.

On the flip side, since we're forced to use a combination, then CD is the right answer.

In terms of simplicity, it is the question, what you consider simple. API GW REST endpoint is considered simple, because it provides caching, api keys, usage plans, rate limiting, authorization, deployment stages etc. out of the box. So the plethora of out-of-the-box features is rather simple than implementing them oneself.

upvoted 1 times

✉ ninomfr64 2 years ago

Selected Answer: BC

Not E as I think NLB listener rules don't provide the required capability to forward requests to the appropriate Lambda (you need to have an ALB)
Not D as Lambda@Edge is a CloudFront feature

A, B and C they all work here however the question requires "a simple API over HTTPS". Both REST APIs and HTTP APIs are RESTful API products. REST APIs support more features than HTTP APIs, while HTTP APIs are designed with minimal features so that they can be offered at a lower price. Thus I would go for B and C

upvoted 1 times

✉ ninomfr64 2 years ago

My answer is wrong, double check that DynamoDB is not supported as first-class integration with API Gateway as per doc <https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-develop-integrations-aws-services-reference.html>

Thus the correct answer is A and C

upvoted 2 times

✉ subbupro 2 years ago

C and D is the correct option

1) C- Need server less architecture so need to use lambda function instead of REST API
2) D - Global accelerator works with lambda edge would be best the option compare to NLB for auto scale up and down. It has static address and fixed entry point if we deploy multiple regions.

upvoted 2 times

✉ Hit1979 2 years ago

Selected Answer: CE
REST API - is not simple and limitation around scalability. NLB with listener rules can be used to forward request based on specified conditions to appropriate AWS lambda function

upvoted 1 times

✉ severlight 2 years, 1 month ago

Selected Answer: AC
lambda can have https endpoints available
upvoted 1 times

✉ rodrod 2 years, 3 months ago

Selected Answer: BC
I've read similar questions previously, keyword is "simple API".
REST API adds more features than HTTP API and is considered "more" complex.
So it has to be HTTP just for that reason.

You can use API Gateway (HTTP)->dynamodb:
<https://aws.amazon.com/fr/blogs/compute/using-amazon-api-gateway-as-a-proxy-for-dynamodb/>

so B and C

upvoted 3 times

✉ sonyaws 2 years, 1 month ago

BC
HTTP API supports AWS Integrations + Simple
<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>
upvoted 2 times

Question #28

A company has registered 10 new domain names. The company uses the domains for online marketing. The company needs a solution that will redirect online visitors to a specific URL for each domain. All domains and target URLs are defined in a JSON document. All DNS records are managed by Amazon Route 53.

A solutions architect must implement a redirect service that accepts HTTP and HTTPS requests.

Which combination of steps should the solutions architect take to meet these requirements with the LEAST amount of operational effort? (Choose three.)

- A. Create a dynamic webpage that runs on an Amazon EC2 instance. Configure the webpage to use the JSON document in combination with the event message to look up and respond with a redirect URL.
- B. Create an Application Load Balancer that includes HTTP and HTTPS listeners.
- C. Create an AWS Lambda function that uses the JSON document in combination with the event message to look up and respond with a redirect URL.
- D. Use an Amazon API Gateway API with a custom domain to publish an AWS Lambda function.
- E. Create an Amazon CloudFront distribution. Deploy a Lambda@Edge function.
- F. Create an SSL certificate by using AWS Certificate Manager (ACM). Include the domains as Subject Alternative Names.

Correct Answer: CEF*Community vote distribution*

CEF (39%)	BCF (38%)	11%	10%
-----------	-----------	-----	-----

 **masetromain** Highly Voted  2 years, 11 months ago

Selected Answer: CEF

C: By creating an AWS Lambda function, the solution architect can use the JSON document to look up the target URLs for each domain and respond with the appropriate redirect URL. This way, the solution does not need to rely on a web server to handle the redirects, which reduces operational effort.

E: By creating an Amazon CloudFront distribution, the solution architect can deploy a Lambda@Edge function that can look up the target URLs for each domain and respond with the appropriate redirect URL. This way, CloudFront can handle the redirection, which reduces operational effort.

F: By creating an SSL certificate with ACM and including the domains as Subject Alternative Names, the solution architect can ensure that the redirect service can handle both HTTP and HTTPS requests, which is required by the company.

upvoted 41 times

 **Shahul75** 2 years, 10 months ago

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

upvoted 1 times

 **masetromain** 2 years, 11 months ago

A and B are not the right answer because they would require configuring and maintaining a web server to handle the redirects, which would increase operational effort.

D is not the right answer because it would require creating an API Gateway API, which increases operational effort.

upvoted 8 times

 **Arnaud92** 2 years, 9 months ago

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

upvoted 9 times

 **chathur** Highly Voted  2 years, 7 months 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 41 times

 **dubyaf** 2 years ago

This is the only answer that is completed by using all three options selected BCF. F is mandatory to resolve the marketing domains URLs that are HTTPS. So B and C then work together to redirect to those URLs as a full solution like <https://aws.amazon.com/ko/blogs/networking-and-content-delivery/automating-http-s-redirects-and-certificate-management-at-scale/>

E may have partial potential to do something, but you have no origin with it - and what would the origin be?
With BCF you hit the ALB get a redirect as a result of the Marketing URL and your done-- its a complete redirect solution which is what the whole requirement is.

upvoted 6 times

 **satya89** Most Recent ⓘ 2 weeks, 3 days ago

Selected Answer: CEF

Options that are not optimal:

Option A (EC2 instance with a dynamic webpage) would require more operational effort for server maintenance, patching, and scaling.
Option B (Application Load Balancer) would add unnecessary complexity and cost when CloudFront can handle the traffic more efficiently.
Option D (API Gateway with custom domain) would add an additional layer that's not necessary for this use case, increasing complexity and cost.

upvoted 1 times

 **aka1177** 3 weeks, 2 days ago

Selected Answer: BCF

BCF, - CDN for redirection it's overkill + there is no origin. So only BCF

upvoted 1 times

 **Bugis** 3 weeks, 5 days ago

Selected Answer: CDF

C - This allows for serverless processing with minimal operational management. The Lambda function can easily handle HTTP requests and look up the appropriate redirect URLs based on the incoming domain name.

D - API Gateway will expose the Lambda function via HTTP and HTTPS and handle all incoming requests, providing a simple interface to trigger the Lambda function. A custom domain allows you to map the domain names to the API seamlessly.

F - This ensures secure HTTPS connections for each of the domains, which is essential for user trust and SEO purposes. ACM simplifies SSL management.

upvoted 1 times

 **b0969fd** 2 months, 1 week ago

Selected Answer: CEF

- A. EC2 instance for redirect is overkill
- B. ALB means you need a VPC which is overkill.
- C. Lambda function handles the redirect
- D. API gateway only accepts HTTPS 443 traffic. (Try to curl an AWS API gateway)

upvoted 1 times

 **Murtuza** 3 months, 4 weeks ago

Selected Answer: BCF

The Deciding Factor: "Least Amount of Operational Effort"

While both solutions are serverless, the ALB and Lambda approach is simpler to set up, faster to deploy, and easier to troubleshoot for this specific use case. CloudFront is a powerful tool, but it's overkill for a simple redirect service that doesn't need a global content delivery network.

upvoted 2 times

 **Nad1122** 4 months, 2 weeks ago

Selected Answer: CDF

It is CDF.

upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: CDF

Why not B or E?

B (ALB): Yes, ALB can target Lambda now, but it requires managing listener rules and doesn't natively support multiple domains with one certificate unless using wildcards or SANs. Slightly more overhead than API Gateway for this use case.

E (CloudFront + Lambda@Edge): Designed for CDN and global content caching. For simple redirection, it adds unnecessary complexity (e.g., setting up origins, deployment propagation delays) and higher cost.

upvoted 1 times

 **AI8282** 5 months, 4 weeks ago

Selected Answer: BCF

B: Can handle redirects directly without needing to setup cloudfront which increases complexity.

Then as everyone agrees, C and F.

upvoted 1 times

 **ex_example** 6 months, 1 week ago

Selected Answer: CEF

CEF

C: Read json and redirect

- E: Handle HTTP/HTTPS (intercept request)
F: Required for multiple Certificate management (HTTPS)

WRONG

- A: EC2 too much
B: ALB handles HTTP/HTTPS BUT no dynamic lookup using JSON
D: More operation effort compare to CloudFront

upvoted 1 times

✉ **Kaps443** 6 months, 3 weeks ago

Selected Answer: CDF

Simple, low-maintenance, HTTPS support, no compute needed

upvoted 1 times

✉ **CAIYasia** 8 months ago

Selected Answer: CDF

Request → Route 53 (DNS resolve) → API Gateway (Domain name + ACM cert.) → Lambda (redirect)

upvoted 2 times

✉ **ed605fe** 8 months, 1 week ago

Selected Answer: BCF

Best match

upvoted 1 times

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

Selected Answer: BCF

BCF. You already have a lambda function that does the processing. You don't need Lambda@Edge anymore

upvoted 1 times

✉ **3a05e15** 10 months, 2 weeks ago

Selected Answer: CDF

Option E involves CloudFront with Lambda@Edge, which is more complex to manage than API Gateway for this use case.

upvoted 2 times

✉ **altonh** 11 months, 3 weeks ago

Selected Answer: BCF

CEF - an overkill

CDF - D says that you should create a custom domain. You need to perform several steps just for this custom domain so it is a more complicated setup.

upvoted 1 times

✉ **altonh** 11 months, 3 weeks ago

Also, API Gateway only exposes HTTPS endpoints.

upvoted 1 times

Question #29

A company that has multiple AWS accounts is using AWS Organizations. The company's AWS accounts host VPCs, Amazon EC2 instances, and containers.

The company's compliance team has deployed a security tool in each VPC where the company has deployments. The security tools run on EC2 instances and send information to the AWS account that is dedicated for the compliance team. The company has tagged all the compliance-related resources with a key of "costCenter" and a value or "compliance".

The company wants to identify the cost of the security tools that are running on the EC2 instances so that the company can charge the compliance team's AWS account. The cost calculation must be as accurate as possible.

What should a solutions architect do to meet these requirements?

- A. In the management account of the organization, activate the costCenter user-defined tag. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account. Use the tag breakdown in the report to obtain the total cost for the costCenter tagged resources.
- B. In the member accounts of the organization, activate the costCenter user-defined tag. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account. Schedule a monthly AWS Lambda function to retrieve the reports and calculate the total cost for the costCenter tagged resources.
- C. In the member accounts of the organization activate the costCenter user-defined tag. From the management account, schedule a monthly AWS Cost and Usage Report. Use the tag breakdown in the report to calculate the total cost for the costCenter tagged resources.
- D. Create a custom report in the organization view in AWS Trusted Advisor. Configure the report to generate a monthly billing summary for the costCenter tagged resources in the compliance team's AWS account.

Correct Answer: A*Community vote distribution*

A (96%)	4%
---------	----

 **masetromain**  2 years, 11 months ago

Selected Answer: A

Answer A : because we do not depend on the users, I prefer management account

Option C or A would be the correct answer. In option C, the solution architect would activate the costCenter user-defined tag in the member accounts of the organization, and then schedule a monthly AWS Cost and Usage Report from the management account to retrieve the reports and calculate the total cost for the costCenter tagged resources. In option A, the management account of the organization would activate the costCenter user-defined tag and configure monthly AWS Cost and Usage Reports to be saved to an Amazon S3 bucket in the management account. Then, use the tag breakdown in the report to obtain the total cost for the costCenter tagged resources. Both options would allow the company to accurately identify the cost of the security tools running on the EC2 instances and charge the compliance team's AWS account.

upvoted 21 times

 **dkx** 2 years, 6 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 14 times

 **chathur** 2 years, 7 months ago

User-defined tags can not be allowed from management accounts in AWS Organization. It must done from the management Account.
upvoted 2 times

 **Reval** 1 year, 5 months ago

Did you mean from member account? in this sentence "User-defined tags can not be allowed from management accounts in AWS Organization."

upvoted 1 times

 **Untamables**  2 years, 12 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

 **princajen**  5 months, 3 weeks ago

Selected Answer: A

Only a management account in an organization has access to the cost allocation tags manager in the Billing and Cost Management console.

upvoted 1 times

 **jimee11** 7 months, 3 weeks ago

Selected Answer: A

Cost tags are activated in the Management console.

upvoted 1 times

 **Tiger4Code** 1 year ago

Selected Answer: A

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.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **Jason666888** 1 year, 4 months ago

Selected Answer: A

The most ideal way to get this job done is to use: AWS Cost Explorer

But among all the given options, we should go with option A, as the user defined tag can only be managed in management account

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A is correct

upvoted 1 times

 **subupro** 2 years ago

A is correct, we need to login to management account to create

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: A

yes, you need to activate cost allocation tags before using, you can do this in the same place where you would like to see your reports - management account

upvoted 2 times

 **whenthan** 2 years, 2 months ago

Selected Answer: C

lines up correctly

activate tag in member accounts and generating AWS CUR from management account (has ability to see costs across all member accounts) and Tag breakdown in report

upvoted 1 times

 **imvb88** 2 years, 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/activating-tags.html>

"For tags to appear on your billing reports, you must activate them."

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

"Only a management account in an organization and single accounts that aren't members of an organization have access to the cost allocation tags manager in the Billing and Cost Management console."

-> eliminate B,C. D is not relevant

upvoted 2 times

 **whenthan** 2 years, 3 months ago

Selected Answer: A

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

upvoted 1 times

 **bur4an** 2 years, 3 months ago

Selected Answer: A

Only a management account in an organization and single accounts that aren't members of an organization have access to the cost allocation tags manager in the Billing and Cost Management console.

upvoted 3 times

 **NikkyDicky** 2 years, 6 months ago

it's an A

upvoted 1 times

 **rtguru** 2 years, 7 months ago

I go with D

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: A

Cost center tag int he management account.

upvoted 1 times

Question #30

A company has 50 AWS accounts that are members of an organization in AWS Organizations. Each account contains multiple VPCs. The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account. Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment.

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

- A. From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager.
- B. From the management account, share the transit gateway with member accounts by using an AWS Organizations SCP.
- C. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a VPC transit gateway attachment in a member account. Associate the attachment with the transit gateway in the management account by using the transit gateway ID.
- D. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a peering transit gateway attachment in a member account. Share the attachment with the transit gateway in the management account by using a transit gateway service-linked role.
- E. From the management account, share the transit gateway with member accounts by using AWS Service Catalog.

Correct Answer: AC*Community vote distribution*

AC (95%)	5%
----------	----

 **masetromain** Highly Voted  2 years, 11 months ago

Selected Answer: AC

Option A is sharing the transit gateway with member accounts by using AWS Resource Access Manager, which allows the management account to share resources with member accounts. Option C is launching an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a VPC transit gateway attachment in a member account, and associates the attachment with the transit gateway in the management account by using the transit gateway ID. This automation of creating a new VPC and transit gateway attachment in new member accounts can help to streamline the process and reduce operational effort.

upvoted 26 times

 **jainparag1** 2 years, 1 month ago

Precisely!

upvoted 1 times

 **princaben** Most Recent  5 months, 3 weeks ago

Selected Answer: A

A (Use RAM to share the TGW)
 C (Use StackSets to deploy VPCs + TGW attachments)

upvoted 2 times

 **ausl** 7 months, 3 weeks ago

Selected Answer: AC

From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager

upvoted 1 times

 **Tiger4Code** 1 year ago

Selected Answer: AC

A. From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager. Most Voted
 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.

You want to associate the gateway attachment with the transit gateway that you already shared using RAM

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager.
 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.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: AC

AC are correct

upvoted 1 times

 **rif** 2 years, 2 months ago

AC.

<https://aws.amazon.com/ko/blogs/networking-and-content-delivery/automating-aws-transit-gateway-attachments-to-a-transit-gateway-in-a-central-account/>

<https://cloudjourney.medium.com/aws-ram-and-transit-gateway-8ac230f298e8>

upvoted 1 times

 **Simon523** 2 years, 3 months 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 years, 6 months ago

AC of course

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: AC

AC are my choice.

upvoted 2 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: AC

A and C are the answer for me

upvoted 2 times

 **Untamables** 2 years, 12 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** 3 years 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

An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit (OU) that will be used by procurement managers. The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement. The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers. Other IAM users, groups, roles, and account administrators in the company should be denied Private Marketplace administrative access.

What is the MOST efficient way to design an architecture to meet these requirements?

- A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the PowerUserAccess managed policy to the role. Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.
- B. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the AdministratorAccess managed policy to the role. Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.
- C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.
- D. Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developers. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Apply the SCP to all the shared services accounts in the organization.

Correct Answer: C*Community vote distribution*

C (92%)	8%
---------	----

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: C

The most efficient way to design an architecture to meet these requirements is option C. By creating an IAM role named procurement-manager-role in all the shared services accounts in the organization and adding the AWSPrivateMarketplaceAdminFullAccess managed policy to the role, the procurement managers will have the necessary permissions to administer Private Marketplace. Then, by creating an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role and another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization, the company can restrict access to Private Marketplace administrative access to only the procurement managers.

upvoted 16 times

 **SK_Tyagi** 2 years, 4 months ago

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

upvoted 3 times

 **amministrazione** Most Recent 1 year, 3 months ago

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.

upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

Selected Answer: C

Not D, why? : D. Placing the procurement-manager-role in developer accounts with full Private Marketplace admin access increases the risk of mismanagement. Additionally, applying an SCP only to shared services accounts does not adequately restrict access across the entire organization.

upvoted 1 times

 **cnethe** 1 year, 6 months ago

Why C is right and D is wrong....

Focus on the end of the question :

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?

Who should be excluded? Other IAM users, groups, roles, and account administrators in the company

What is the MOST efficient way? Apply SCP at the root level

D is more work than C, this is a good reason to choose C over D

upvoted 1 times

 **Chakanetsa** 1 year, 7 months ago

Selected Answer: C

C. Most efficient and secure:

Creating the procurement-manager-role in shared services accounts limits its scope to specific OUs, aligning with the organizational structure.

Granting AWSPrivateMarketplaceAdminFullAccess to this role provides the necessary permissions for managing Private Marketplace within the OU.

An organization root-level SCP denying Private Marketplace administration to everyone except the procurement-manager-role ensures centralized control and restricts unauthorized access.

Another SCP preventing the creation of the procurement-manager-role outside of shared services accounts adds an extra layer of security.

upvoted 1 times

 **anubha.agrahari** 1 year, 9 months ago

Selected Answer: C

C, D doesn't make sense.

upvoted 1 times

 **ninomfr64** 2 years ago

Selected Answer: C

Not A as it does not implement the requirement to enforce procurement managers to use the shared services account in each organizational unit

Not B as this would allow developers to administer private market place

not D as this would allow developers to administer private market place

C is correct as it configures the required role (with required permission) only in the shared service account, uses an SCP to deny private market place management to everyone except the role named procurement-manager-role and another SCP to prevent creating a role named procurement-manager-role

upvoted 2 times

 **ninomfr64** 2 years ago

Actually D would do the job, but creating a role in every account is not strictly necessary and would cause more work

upvoted 1 times

 **subupro** 2 years ago

C is the better one than D because we need to apply SCP to the root level with deny policy is the best practices. Create the role and apply to each account is not a correct way and it is overhead to the administrator.

upvoted 2 times

 **severlight** 2 years, 1 month ago

Selected Answer: C

Look on whenthan's answer

upvoted 1 times

 **whenthan** 2 years, 2 months ago

Selected Answer: C

creation of role in all shared services

adding required policy to the role

creation of org root-level to guardrail who can have those privileges

creation of SCP to close out workaround of creation of another role with same access

upvoted 3 times

 **Tarun4b7** 2 years, 3 months ago

Selected Answer: D

C and D options are most relevant. Once you create a role, you cannot create another role with same name. So option C doesn't make sense. So my answer Option D

upvoted 2 times

 **StarBoy01** 1 month, 1 week ago

I think you missed the context of the latter part "Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization."

It is not creating another role with the same name. It is creating a SCP that will deny other accounts within the Organization to create that role.

Therefore, C is the best option here.

upvoted 1 times

 **_Jassybanga_** 1 year, 10 months ago

i am on same page

upvoted 1 times

✉ **_Jassybang_** 1 year, 10 months ago

its C - the role should be in shared service accounts and not all accounts

upvoted 1 times

✉ **qxy** 2 years, 3 months ago

Selected Answer: C

Clearly, it's C.

upvoted 1 times

✉ **Karamen** 2 years, 4 months ago

Selected answer: C

option D: "Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developers", the procurement-manager-role is used by manager not used by developers

upvoted 2 times

✉ **alicewsm** 2 years, 2 months ago

the first sentence "An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace."

upvoted 1 times

✉ **jainparag1** 2 years, 1 month ago

Developers has to ask procurement manager and not purchase by themselves.

upvoted 2 times

✉ **SorenBendixen** 2 years, 4 months ago

Selected Answer: D

Its D - According to this : <https://aws.amazon.com/blogs/awsmarketplace/controlling-access-to-a-well-architected-private-marketplace-using-iam-and-aws-organizations/>

upvoted 2 times

✉ **SorenBendixen** 2 years, 4 months ago

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

upvoted 2 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

Its a C

upvoted 1 times

✉ **gd1** 2 years, 6 months ago

Selected Answer: C

C is correct-

upvoted 1 times

✉ **Maria2023** 2 years, 6 months ago

Selected Answer: C

D is a distractor since the developers do not need to administer the private marketplace. Plus that the procurement team acts only in the shared accounts. That leaves C as the only option

upvoted 4 times

Question #32

Topic 1

A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2, Amazon S3, and Amazon DynamoDB. The developers account resides in a dedicated organizational unit (OU). The solutions architect has implemented the following SCP on the developers account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEC2",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowDynamoDB",
      "Effect": "Allow",
      "Action": "dynamodb:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowS3",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

When this policy is deployed, IAM users in the developers account are still able to use AWS services that are not listed in the policy. What should the solutions architect do to eliminate the developers' ability to use services outside the scope of this policy?

- A. Create an explicit deny statement for each AWS service that should be constrained.
- B. Remove the FullAWSAccess SCP from the developers account's OU.
- C. Modify the FullAWSAccess SCP to explicitly deny all services.
- D. Add an explicit deny statement using a wildcard to the end of the SCP.

Correct Answer: B

Community vote distribution

B (67%)

D (27%)

6%

 **zhangyu20000** Highly Voted 3 years ago

B is correct because default FullAWSAccess SCP is applied
upvoted 19 times

 **Six_Fingered_Jose** Highly Voted 2 years, 3 months 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 12 times

 **jainparag1** 2 years, 1 month ago

That's correct. You can disable AWSFullAccess SCP from member accounts as long as you are replacing it with another policy with specific permissions required.
upvoted 4 times

 **ciscochamps** Most Recent 3 months, 3 weeks ago

Selected Answer: D

Definitely D, removing FullAWSAccess SCP will block everything
upvoted 1 times

 **princajen** 5 months, 3 weeks ago

Selected Answer: B

Best Practice:
Replace FullAWSAccess with a tightly-scoped "Allow-only" SCP, and keep the policy clean and minimal. That ensures least privilege and scalability.
upvoted 2 times

 **jimee11** 7 months, 3 weeks ago

Selected Answer: B

AWS advises you to replace the full access assigned by default in the SCP with your controlled SCP. Enabling SCPs gives you FullAWSAccess of the bat.
upvoted 2 times

 **diazed** 8 months, 2 weeks ago

Selected Answer: B

B is correct. AWS Organizations attaches an AWS managed SCP named FullAWSAccess to every root, OU and account when it's created. This policy allows all services and actions. You can replace FullAWSAccess with a policy allowing only a set of services so that new AWS services are not allowed unless they are explicitly allowed by updating SCPs. For example, if your organization wants to only allow the use of a subset of services in your environment, you can use an Allow statement to only allow specific services. A policy combining the two statements might look like the following example, which prevents member accounts from leaving the organization and allows use of desired AWS services. The organization administrator can detach the FullAWSAccess policy and attach this one instead.

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

upvoted 3 times

 **GabrielShiao** 9 months, 1 week ago

Selected Answer: A

I have to choose A although A is impractical. While most vote B, it is actually impossible since removing FullAWSAccess SCP from OU will deny all the services on the OUs and accounts under the OU. The correct action is to remove FullAWSAccess SCP from the developer account.

upvoted 1 times

 **GabrielShiao** 9 months, 1 week ago

Selected Answer: A

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_evaluation.html
If you removed the default SCP from the OU, you will be denied for these permissions even if allowed in SCP on the account in OU.
upvoted 1 times

 **GabrielShiao** 9 months, 1 week ago

Selected Answer: A

If you removed FullAWSAccess from developer accounts, I vote B, however, B is removing it from OU. Keep in mind every level of organization hierarchy must reside at least one SCP.

upvoted 1 times

 **koneczny69** 1 year, 2 months ago

It can be as well handled with a or d, like

```
{
  "Effect": "Deny",
  "NotAction": [
    "ec2:*",
    "s3:*",
    "dynamodb:*"
  ],
  "Resource": "*"
}
```

upvoted 2 times

 **amministrazione** 1 year, 3 months ago

B. Remove the FullAWSAccess SCP from the developer's account's OU.

upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

Selected Answer: B

B. Remove the FullAWSAccess SCP from the developer's account's OU.

Explanation:

FullAWSAccess SCP: By default, AWS Organizations attaches a FullAWSAccess SCP to all OUs and accounts, allowing access to all AWS services unless restricted by another SCP. If this SCP is still attached to the developer's OU, it will allow access to all services, regardless of the more restrictive SCP you have applied.

SCP Behavior: SCPs are evaluated in an "implicit deny" model. If an action is not explicitly allowed by the SCPs, it is implicitly denied. However, if multiple SCPs are attached and one allows an action (like FullAWSAccess), that action is permitted unless explicitly denied in another SCP.

upvoted 2 times

 **felon124** 1 year, 4 months ago

Selected Answer: B

AWS Organizations attaches an AWS managed SCP named FullAWSAccess to every root, OU and account when it's created. This policy allows all services and actions. You can replace FullAWSAccess with a policy allowing only a set of services so that new AWS services are not allowed unless they are explicitly allowed by updating SCPs.

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

upvoted 1 times

 **8693a49** 1 year, 5 months ago

Selected Answer: D

Best practice would be to create an explicit deny statement. The reason is that other SCPs could be in effect, aside from AWSFullAccess, that could grant access to other services. If the goal is to deny access to any other service, then this must be made explicit.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: B

B is correct

Remove from develop account OU --> implicitly deny all service --> add explicitly 'allow' to restrict only allow related services in SCP.

upvoted 1 times

 **Moghite** 1 year, 5 months ago

Selected Answer: D

```
{  
  "Sid": "ExplicitDeny",  
  "Effect": "Deny",  
  "NotAction": [  
    "ec2:*",  
    "dynamodb:*",  
    "s3:*"  
  ],  
  "Resource": "*"  
}
```

upvoted 2 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: D

FullAWSAccess SCP is inherited from root. Can't be removed from OU.

D is correct answer.

upvoted 2 times

 **sam2ng** 1 year, 4 months ago

It can be, read "How SCPs work with Allow" in here it shows example:

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

upvoted 1 times

Question #33

A company is hosting a monolithic REST-based API for a mobile app on five Amazon EC2 instances in public subnets of a VPC. Mobile clients connect to the API by using a domain name that is hosted on Amazon Route 53. The company has created a Route 53 multivalue answer routing policy with the IP addresses of all the EC2 instances. Recently, the app has been overwhelmed by large and sudden increases to traffic. The app has not been able to keep up with the traffic.

A solutions architect needs to implement a solution so that the app can handle the new and varying load.

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

- A. Separate the API into individual AWS Lambda functions. Configure an Amazon API Gateway REST API with Lambda integration for the backend. Update the Route 53 record to point to the API Gateway API.
- B. Containerize the API logic. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Run the containers in the cluster by using Amazon EC2. Create a Kubernetes ingress. Update the Route 53 record to point to the Kubernetes ingress.
- C. Create an Auto Scaling group. Place all the EC2 instances in the Auto Scaling group. Configure the Auto Scaling group to perform scaling actions that are based on CPU utilization. Create an AWS Lambda function that reacts to Auto Scaling group changes and updates the Route 53 record.
- D. Create an Application Load Balancer (ALB) in front of the API. Move the EC2 instances to private subnets in the VPC. Add the EC2 instances as targets for the ALB. Update the Route 53 record to point to the ALB.**

Correct Answer: A*Community vote distribution*

A (42%)	D (37%)	C (22%)
---------	---------	---------

 **EricZhang** Highly Voted  3 years ago

Selected Answer: A

Serverless requires least operational effort.

upvoted 39 times

 **Jay_2pt0_1** 2 years, 7 months 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

 **Ikyixoayffasdrlaqd** 2 years, 10 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 21 times

 **scuzzy2010** 2 years, 8 months ago

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

upvoted 13 times

 **24Gel** 1 year, 9 months ago

disagree, ASG in Option D, after set up, operational is not overheat as well

upvoted 1 times

 **24Gel** 1 year, 9 months ago

i mean Option C not D

upvoted 1 times

 **24Gel** 1 year, 9 months ago

never mind, A is simpler than C

upvoted 2 times

 **dqwsmtwwvtgxwkvvcv** 2 years, 4 months 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 5 times

 **jooncco** Highly Voted  2 years, 11 months ago

Selected Answer: C

Suppose there are a 100 REST APIs (Since this application is monolithic, it's quite common).

Are you still going to copy and paste all those API codes into lambda?

What if business logic changes?
This is not MINIMAL. I would go with C.
upvoted 34 times

chathur 2 years, 7 months 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 2 years, 4 months ago
Because if you have 4 ec2 in your ASG you need to have 4 records in domain name if ASG scale up to 6 for example you need 2 add 2 records more in domain name
upvoted 4 times

liquen14 1 year, 9 months ago
Too contrived in my opinion, and what about DNS caches in the clients?. You coul get stuck for a while with the previous list of servers. I think it's has to be A (but it would involve a considerable development effort) or D which is extremely easy to implement but and the same time it sounds a little bit fishy because they don't mention anything about ASG or scaling

I hate this kind of questions and I don't understand what kind of useful insight they provide unless they want us to become masters of the art of dealing with ambiguity
upvoted 3 times

cnethers 1 year, 6 months ago
Agree that D does not scale to meet demand, it's just a better way to load balance which was being done at R53 before so the scaling issue has not been resolved.
Also agree A requires more dev effort and less ops effort, so I would have to lean to A...
Answer selection is poor IMO
upvoted 1 times

scuzzy2010 2 years, 10 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 8 times

aviathor 2 years, 5 months 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 2 years, 8 months ago
A monolithic REST api likely has a gazillion individual APIs. This refactor would not be a small one.
upvoted 5 times

jainparag1 2 years, 1 month ago
Dealing with business logic change is applicable to existing solution or any solution based on the complexity. Rather it's easier to deal when these are microservices. You shouldn't hesitate to refactor your application by putting one time effort (dev overhead) to save significant operational overhead on daily basis. AWS is pushing for serverless only for this.
upvoted 1 times

altonh 11 months, 3 weeks ago
Option C means your R53 is playing catch-up with your ASG. What happens if you scale down? Your clients will still have the terminated EC2 in their cache until the next TTL.
upvoted 1 times

mlantonis2 Most Recent 5 days, 1 hour ago

Selected Answer: A
Setup effort may be higher than C but questions is asking for LEAST operational overhead, so A.
upvoted 1 times

Murtuza 3 weeks, 4 days ago

Selected Answer: A
reasoning for choosing A because the question emphasizes least operational overhead, not development effort.
upvoted 1 times

7358228 1 month, 1 week ago

Selected Answer: D
One problem with answer D is that it should include adding the EC2 instances to an ASG, which it does not say. So that would lend credence to A. However, I chose D because A seems like a real pain in the ass and they said LEAST amount of effort. Poorly written...
upvoted 1 times

ysyau 1 month, 2 weeks ago

Selected Answer: D
D instead of A, A will require huge refactoring work to rewrite the application logic from EC2 to Lambda serverless technology

upvoted 2 times

 **hexie** 2 months, 2 weeks ago

Selected Answer: D

D is the least operational overhead way to handle sudden and variable load without rewriting the monolith. It gives managed L7 loadbalancing, TLS offload and a single DNS target for R53.

D also ensure that no app rewrite. Its almost impossible to estimate the overhead of rewriting the API into Lambdas.

A would be good if the question had said "the team is fine with re-architecting and wants the minimum day-2 ops for spiky load" (or something like this), then API Gateway + Lambda would win. But given a monolith and the need to handle bursts quickly with minimal change, D is the pragmatic, lowest-overhead move.

upvoted 1 times

 **Blair77** 2 months, 3 weeks ago

Selected Answer: D

The question asks for the solution with the LEAST operational overhead to handle the varying load.

Option D addresses the problem directly and efficiently by leveraging a managed service (ALB) to handle traffic distribution and scaling. It requires minimal changes to the existing application and infrastructure.

Option A is a major architectural shift. While it solves the scalability problem, the amount of effort and management required makes it a solution with high operational overhead.

upvoted 1 times

 **generic_aws_dude** 3 months, 3 weeks ago

Selected Answer: D

If you were to experience this in your work, what would be lowest hanging fruit?

upvoted 1 times

 **ciscochamps** 3 months, 3 weeks ago

Selected Answer: D

D is the easiest option

upvoted 1 times

 **dsatizabal** 3 months, 4 weeks ago

Selected Answer: C

Why on would converting a monolithic app to serverless have less overhead? for me it is pretty clear that the solution for less effort is to add elasticity to the EC2 instances by creating an ASG

upvoted 1 times

 **ce0b8b3** 4 months, 1 week ago

Selected Answer: D

A. Would require complete rewrite of the monolithic API into Lambda functions. so D

upvoted 1 times

 **3967974** 4 months, 3 weeks ago

Selected Answer: D

D needs less changes.

upvoted 3 times

 **speedt115** 5 months ago

Selected Answer: A

the least operational overhead. That's where Option A shines — it moves the monolithic API to AWS Lambda behind API Gateway, eliminating server management entirely. No patching, no scaling logic, no load balancer configuration. Just pure serverless simplicity.

upvoted 2 times

 **AI8282** 5 months ago

Selected Answer: A

I have to go with A, it was between that and D. D doesn't create an ASG which doesn't address the varying load problem but lambda does. D is also more operational overhead with patching and management of the OS and the question specifically asks to reduce ops overhead. It says nothing about doing it fast, or development overhead. Ideally we would do D quickly, then refactor for A depending on the orgs budgets/timeline/focus/strategic goals.

upvoted 2 times

 **strike3test** 5 months, 2 weeks ago

Selected Answer: D

Why not A -> While API Gateway and Lambda provide great scalability and serverless benefits, converting a monolithic API to Lambda functions requires significant refactoring and operational overhead. Also, API Gateway has request rate limits (default 10,000 RPS), and API Gateway is better suited for API-first, microservices architectures rather than monolithic EC2-hosted applications

upvoted 2 times

 **princajen** 5 months, 2 weeks ago

Selected Answer: D

The key phrase is: "LEAST operational overhead" for a REST-based monolithic API.

The most realistic, scalable, and low-effort solution is to introduce an Application Load Balancer (ALB) in front of your EC2 fleet.
upvoted 2 times

Question #34

A company has created an OU in AWS Organizations for each of its engineering teams. Each OU owns multiple AWS accounts. The organization has hundreds of AWS accounts.

A solutions architect must design a solution so that each OU can view a breakdown of usage costs across its AWS accounts.

Which solution meets these requirements?

- A. Create an AWS Cost and Usage Report (CUR) for each OU by using AWS Resource Access Manager. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.**
- C. Create an AWS Cost and Usage Report (CUR) in each AWS Organizations member account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- D. Create an AWS Cost and Usage Report (CUR) by using AWS Systems Manager. Allow each team to visualize the CUR through Systems Manager OpsCenter dashboards.

Correct Answer: B*Community vote distribution*

B (87%)

11%

 **masetromain** [Highly Voted ] 2 years, 11 months ago

Selected Answer: B

B is the correct answer. The solution would be to create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. This would allow the management account to view the usage costs across all the member accounts, and the teams can visualize the CUR through an Amazon QuickSight dashboard. This allows the organization to have a centralized place to view the cost breakdown and the teams to access the cost breakdown in an easy way.

upvoted 21 times

 **princajen** [Most Recent ] 5 months, 2 weeks ago

Selected Answer: B

Use the management account to create the CUR, and use Amazon QuickSight or Athena for visualization.

upvoted 1 times

 **85b5b55** 11 months ago

Selected Answer: B

using OU Management Account, create a CUR using OU Management account and allow each AWS account to view through Amazon QuickSight.

upvoted 2 times

 **AWSum1** 1 year, 3 months ago

Selected Answer: B

Option B: it must be done from the management account

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.

upvoted 1 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: C

Option C: I hate this questions because you have 2 correct answers however only ONE real correct answer. I have to read the question like 20x until I understood it, the questions is asking for " solution so the EACH OU can VIEW a breakdown of usage across ITS account". Its only asking for each OU breakdown for its members can see the usage cost and NOT the organization. Prior to Dec 2020 Option B would be correct however after its Option C:

Read the following AWS Update - <https://aws.amazon.com/about-aws/whats-new/2020/12/cost-and-usage-report-now-available-to-member-linked-accounts/?pg=ln&sec=uc>

upvoted 4 times

 **ParamD** 9 months, 2 weeks ago

No, ask if for OU level report, not member level. Hence B.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: B

B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.

upvoted 1 times

 **Rajarshi** 1 year, 10 months ago

C

As target is to design a solution so that each OU can view a breakdown of usage costs across its AWS accounts

upvoted 1 times

 **acordovam** 1 year, 10 months ago

Selected Answer: A

The question specifies that each OU should only view their own AWS accounts, not all accounts in the organization. While creating the solution in the management account might offer a centralized approach, it violates this crucial requirement.

upvoted 1 times

 **acordovam** 1 year, 10 months ago

Sorry, I'm wrong, RAM can't create a Cost Report.

upvoted 3 times

 **abeb** 2 years, 1 month ago

B From management account of each account

upvoted 1 times

 **daz2023** 2 years, 2 months ago

AWS Resource Access Manager has nothing to do with creating CUR.

Answer B is correct. Use AWS Organization management account

upvoted 1 times

 **duriselvan** 2 years, 4 months 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 years, 6 months ago

Selected Answer: B

B by elimination

upvoted 1 times

 **gameoflove** 2 years, 7 months ago

Selected Answer: B

B As AWS Organizations Management account is only correct option

upvoted 1 times

 **leehjworking** 2 years, 8 months ago

Can anyone explain why A is wrong? Thank you.

upvoted 1 times

 **scuzzy2010** 2 years, 8 months ago

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

upvoted 4 times

 **mfsec** 2 years, 9 months ago

Selected Answer: B

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

upvoted 2 times

 **masetromain** 3 years 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

A company is storing data on premises on a Windows file server. The company produces 5 GB of new data daily.

The company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. The company already has established an AWS Direct Connect connection between the on-premises network and AWS.

Which data migration strategy should the company use?

- A. Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server, and point the existing file share to the new file gateway.
- B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.**
- C. Use AWS Data Pipeline to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).
- D. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).

Correct Answer: B*Community vote distribution*

B (61%)

A (39%)

✉  **masetromain**  2 years, 11 months ago

Selected Answer: B

B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.
 D. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS) are also valid options. They both use DataSync to schedule a daily task to replicate the data between on-premises and cloud, the main difference is the type of file system in the cloud, Amazon FSx or Amazon Elastic File System (Amazon EFS).
 upvoted 18 times

✉  **rbm2023** 2 years, 7 months ago

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

upvoted 28 times

✉  **Karamen** 2 years, 4 months ago

thanks for this explaination.

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

upvoted 1 times

✉  **victorHugo**  2 years, 3 months 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 14 times

✉  **swadeey** 2 years, 1 month ago

Correct point here is migration not daily sync and replication.

upvoted 3 times

✉  **vn_thanh tung** 2 years, 3 months ago

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

upvoted 3 times

✉  **aka1177**  1 month, 1 week ago

Selected Answer: B

"to AWS and needs the data to be available on a file system in the cloud" - meaning you need file system on AWS, meaning only EFS or FSx. EFS doesn't fit since it support only linux. SO only B is correct.

upvoted 1 times

✉  **AI8282** 5 months ago

Selected Answer: B

I had to pick B over A because it didn't specify "Fsx File Gateway" it just said "File Gateway" which is a separate product used to send data to S3 rather than a file system like Fsx File Gateway would do. Tricky one.

upvoted 1 times

 **princajen** 5 months, 2 weeks ago

Selected Answer: B

Amazon FSx for Windows File Server is the best match for Windows-based workloads.

AWS DataSync can efficiently handle scheduled transfers, perfect for 5 GB/day.

Ideal if the goal is daily replication/migration to make data available in AWS without requiring real-time syncing.

Argument: File Gateway offers real-time access to data from both on-premises and cloud via caching. If immediate cloud access to on-premises files is needed, Amazon FSx File Gateway can serve as a bridge.

Valid if the requirement is active hybrid access.

But not a "data migration" strategy, it doesn't move data to the cloud, it fronts S3 of FSx with a cache.

upvoted 1 times

 **0dc6cac** 6 months ago

Selected Answer: A

Has to be A, it's the only option if you want data to be available on the cloud instantly. B does a daily sync, which means the data is outdated throughout the day

upvoted 1 times

 **0dc6cac** 6 months, 1 week ago

Selected Answer: A

Nothing suggests that we want to do a daily sync in the question. A makes more sense because the files will be always available to use from the cloud. In 99% of the cases that's better, and if it's the remaining 1%, they would have surely mentioned it in the question.

upvoted 1 times

 **happieee** 9 months, 1 week ago

Selected Answer: B

DataSync allows migration and continue access to both on-prem file server and FSx in a synchronised manner.

upvoted 1 times

 **0dc6cac** 6 months ago

but the data is synced daily, will be outdated throughout the day

upvoted 1 times

 **ParamD** 9 months, 2 weeks ago

Selected Answer: A

A seem to be a more efficient solution as it eliminates duplicate storage. Storage gateway has to be FSx, which is implicit in this option.

upvoted 1 times

 **fbukevin** 12 months ago

Selected Answer: B

Comparing A and B, finally I choosed B due to the "scheduling". In A, despite file gateway could provide or combine a scheduling function, B explicitly says that operation.

upvoted 1 times

 **Biden** 12 months ago

Selected Answer: A

Workloads are only partially migrated which means data need to be accessed simultaneously by on-prem VMs and the already migrated VMs in cloud

And we should assume that the data should be up to date all the time not just updated periodically

Finally, File Gateway could be Amazon FSX File GW

Hence clearly A.

upvoted 2 times

 **Tiger4Code** 1 year ago

Selected Answer: B

D is wrong cos EFS support only Linux File System

upvoted 2 times

 **toyaji** 1 year, 2 months ago

Selected Answer: A

Using Amazon FSx File Gateway, you can access data with low latency from on-premise and also in-cloud always. Why do you neet to batch datasync as like B?

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.

upvoted 1 times

 **8693a49** 1 year, 5 months ago

Selected Answer: A

Because part of the workloads have already been migrated we need a solution that keeps the data consistent between on-prem and the cloud. With DataSync files stored by systems on-prem would be visible in the cloud only the following day. This could cause data inconsistencies and business disruption. The best solution is to use a file gateway to maintain files synchronised at all times. 5GBs/day is easily transferable over DX

upvoted 2 times

 **gfhbox0083** 1 year, 5 months ago

B, for sure.

Needs the data to be available on a file system in the cloud.

upvoted 1 times

 **mifune** 1 year, 8 months ago

Selected Answer: B

Windows file server -> FSx (cristal clear)

upvoted 1 times

Question #36

A company's solutions architect is reviewing a web application that runs on AWS. The application references static assets in an Amazon S3 bucket in the us-east-1 Region. The company needs resiliency across multiple AWS Regions. The company already has created an S3 bucket in a second Region.

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

- A. Configure the application to write each object to both S3 buckets. Set up an Amazon Route 53 public hosted zone with a record set by using a weighted routing policy for each S3 bucket. Configure the application to reference the objects by using the Route 53 DNS name.
- B. Create an AWS Lambda function to copy objects from the S3 bucket in us-east-1 to the S3 bucket in the second Region. Invoke the Lambda function each time an object is written to the S3 bucket in us-east-1. Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.
- C. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region. Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.**
- D. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region. If failover is required, update the application code to load S3 objects from the S3 bucket in the second Region.

Correct Answer: C*Community vote distribution*

C (96%)	2%
---------	----

 **zhangyu20000** Highly Voted 3 years ago

C is correct.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html
 upvoted 20 times

 **princajen** Most Recent 5 months, 2 weeks ago

Selected Answer: C

Option C provides an automated, resilient, and low-maintenance solution using S3 CRR and CloudFront origin groups to meet the requirement of multi-Region resiliency with the least operational overhead.
 upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.
 upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

Selected Answer: C

Why not D ? 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:

Manual Failover: This option involves manual updates to the application code in the event of a failover, which adds operational overhead and complexity. CloudFront provides automatic failover and load balancing, making it a more streamlined solution.

upvoted 1 times

 **sarlos** 1 year, 8 months ago

C IS THE answer
 upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C

C is correct
 upvoted 1 times

 **VerRi** 1 year, 10 months ago

Selected Answer: C

Straightforward
 upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: C

Option C is the most efficient solution because it leverages S3's built-in replication feature to automatically replicate objects to a second bucket in another Region, ensuring that the data is resiliently stored across multiple Regions. By using Amazon CloudFront with an origin

group containing both S3 buckets, the application benefits from CloudFront's global content delivery network, which improves load times and provides a built-in failover mechanism. This setup minimizes operational overhead while achieving the desired resiliency and performance improvements.

Option C provides a seamless, automated solution for achieving resiliency across multiple AWS Regions with minimal operational effort, leveraging AWS services designed for replication, content delivery, and failover.

upvoted 1 times

Vaibs099 1 year, 11 months ago

C is correct because,

You can serve Dynamic Websites with Static Content with CDN by having origins for both and in your webserver app refer to DNS for s3 origin from CF to deliver static content. For webserver on EC2 (Custom Origins can be used).

So in above scenario, if you would like to have resiliency. Add another S3 Origin with bucket in different region. Create Origin Group with both S3 Origins. Set priority on Origins and select 4XX and 5XX error codes for failover. You can use DNS returned for Origin Group from Cloud front in your web app and that would do automatic failover with least overheads.

D also solves the purpose, but you will need to build failover mechanism in your app. However, with above Cloudfront Origin group is taking care of that for you.

upvoted 1 times

ninomfr64 2 years ago

Selected Answer: C

All options does the job, but:

A would require code maintenance and managing public hosted zone -> No

B would require Lambda and CloudFront operations -> No

C would require only CloudFront operations -> Yes

D requires a lot of work for failover that appears to be manual -> No

upvoted 2 times

subupro 2 years ago

C is mostly correct, A is not correct - B and D required the code changes. C will take care of the cloud front orgin failover.

upvoted 1 times

abeb 2 years, 1 month ago

C is good

upvoted 1 times

severlight 2 years, 1 month ago

Selected Answer: C

obvious

upvoted 1 times

totten 2 years, 2 months ago

Selected Answer: C

Here's why Option C is the most suitable choice:

Replication: Amazon S3 Cross-Region replication is designed to replicate objects from one S3 bucket to another in a different Region. This ensures data resiliency across Regions with minimal operational overhead. Once configured, replication happens automatically.

CloudFront: Setting up an Amazon CloudFront distribution with an origin group containing the two S3 buckets allows you to use a single CloudFront distribution to serve content from both Regions. CloudFront provides low-latency access to your content, and using an origin group allows for failover if one of the S3 buckets becomes unavailable.

upvoted 4 times

totten 2 years, 2 months ago

Option A suggests configuring the application to write each object to both S3 buckets, which can result in higher operational overhead and may not provide immediate failover capabilities.

Option B involves creating a Lambda function to copy objects, which adds complexity and requires code maintenance for each object written to the S3 bucket in us-east-1.

Option D relies on manual updates to the application code for failover, which is less automated and could result in higher operational overhead.

Therefore, Option C is the most efficient and operationally streamlined solution to achieve data resiliency and availability across multiple AWS Regions.

upvoted 1 times

Simon523 2 years, 3 months ago

Selected Answer: C

C, LEAST operational overhead

upvoted 1 times

TWOCATS 2 years, 4 months 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** 2 years, 4 months ago

Selected Answer: C

upvoted 1 times

Question #37

Topic 1

A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database. A solutions architect must design a scalable and highly available solution to meet the demand of 200,000 daily users.

Which steps should the solutions architect take to design an appropriate solution?

- A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance. The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB.
- B. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.
- C. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer (ALB) in each Region. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions.
- D. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

Correct Answer: B*Community vote distribution*

B (86%) 11%

robertohyena 3 years 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 30 times

kz407 1 year, 9 months ago

I don't think ASGs are cross-region either. This answer in SO gives a serious perspective on this regard.

<https://stackoverflow.com/a/12907101/3126973>

upvoted 1 times

masetromain 2 years, 11 months ago

That's correct, option C is not a valid solution because AWS Elastic Beanstalk is a region-specific service, it cannot span multiple regions. Option B is a valid solution that uses CloudFormation to launch a stack with an Application Load Balancer in front of an Auto Scaling group, a Multi-AZ Aurora MySQL cluster and Route 53 to route traffic to the load balancer, it meets the requirements of scalability and high availability with a good performance and with less operational overhead.

upvoted 6 times

Perkuns 2 years, 6 months ago

if I am not mistaken you can deploy the same EB to a different region. why does that eliminate C? it further increases your availability with geolocation weighted routing, as well as you having DR which even further increases availability along with low RPO and RTO

upvoted 7 times

jpa8300 1 year, 12 months ago

I agree with you, that's the best option, two EBs, one in each region to deploy, manage and monitor all the environment.

upvoted 1 times

Chris_W_1234 2 months, 2 weeks ago

I think the knock-out phrase in solution C is the read replica of the Aurora DB in the second region. Since Aurora can have only one master/read-write node, it means that the EB application in the second region has to write to the read-write node in the first region. Technically possible but I don't think desirable. Therefore, solution B.

upvoted 1 times

masetromain 2 years, 11 months ago

Selected Answer: B

B is correct. The solution architect should use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

This solution provides scalability and high availability for the web application by using an Application Load Balancer and an Auto Scaling group in multiple availability zones, which can automatically scale in and out based on traffic demand. The use of a Multi-AZ Amazon Aurora MySQL DB cluster provides high availability for the database layer and the Retain deletion policy ensures the data is retained even if the DB instance is deleted. Additionally, the use of Route 53 with an alias record ensures traffic is routed to the correct location.

upvoted 8 times

 **Chris_W_1234** Most Recent 2 months, 2 weeks ago

Selected Answer: B

C is close but I think the fact that region B only has a read replica of the MySQL DB is undesirable. Therefore, B.

upvoted 1 times

 **Deztroyer88** 9 months, 3 weeks ago

Selected Answer: B

B is the most appropriate solution that's meeting the scalable and highly available requirement. C is good for DR and that is not what is being asked in the question.

upvoted 1 times

 **Archer1974** 9 months, 4 weeks ago

Selected Answer: C

Highly Available is a key requirement and hence the solution has to span multiple regions. The other options do not handle for Region Failure. Elastic Beanstalk can be deployed across multiple regions. Traffic can be distributed to the appropriate region based on geo-proximity. This is the only correct answer.

upvoted 1 times

 **Tiger4Code** 1 year ago

Selected Answer: B

Answer: 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.

NOT C: Cos geoproximity is used only for private hosted zones, not public

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

Selected Answer: B

B, for sure.

Elastic Beanstalk is region specific.

The "Retain" deletion policy in AWS Aurora ensures that when you delete a database cluster, the automated backups and snapshots of the cluster are retained. This means that even though the database cluster itself is deleted, the backups and snapshots remain, allowing you to restore the cluster from those backups at a later time.

upvoted 3 times

 **gfhbox0083** 1 year, 5 months ago

B, for sure.

Elastic Beanstalk environments are typically created within a single AWS region.

upvoted 1 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: C

Option C: The only AWS documentation I found that supports .NET application migration is for Elastic Beanstalk, it said "EB is the fastest and simplest way to deploy .NET applications on AWS". Many suggestions are selection option "B", the question is not asking about cost or least operational overhead, just scalable and highly available for the migration for a .NET application. Also, I can see why so many people are selecting option "B".

<https://docs.aws.amazon.com/whitepapers/latest/develop-deploy-dotnet-apps-on-aws/aws-elastic-beanstalk.html>

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

upvoted 4 times

 **kz407** 1 year, 9 months ago

Selected Answer: B

B however is not a highly available solution IMO because it is restricted to a region. By any chance if the region goes down, the webapp goes down as well.

A is out of the picture because it involves an NLB.

D is out of the picture because it involves spot instances which is not the choice for HA requirements.

C, everything is good except the mention of "Elastic Beanstalk environment that spans across regions". This is wrong. EB environments are a region construct. You can't have them spanning across regions. You can however have EB in multiple regions.

upvoted 3 times

 **bjexamprep** 1 year, 11 months ago

Selected Answer: B

Guessing the question designer prefers B. But it is wrong. When talking about R53 Alias record, it is wrong. Cause Alias record points to IP address while ALB endpoint is not an IP address.

A has flaw. The question says 3-tier web application. AWS question designers often mess up the definition of 3-tier application, which means there isn't a very clear definition of 3 tier: browser/application server/database is one definition, another one is WebServer/Application Server/database. Looks like A means the latter. Then, if the Elastic Beanstalk is hosting a web server, what are the ASG hosting? And why the R53 is pointing to the NLB which is pointing to the ASG?

C is wrong, cause Elastic Beanstalk cannot span regions.

D is wrong because spot instance is not HA.

Weighting the flaws of different answers, B has the least flaw.

upvoted 1 times

 **ninomfr64** 2 years ago

Selected Answer: B

Not C as we do not need to span multiple Region (DR, global reach, ...), also cross-Region read replica does not fail-over automatically (you need to promote it to primary). Finally from the wording it seems that this imply having a single environment that spans two separate Regions which is not supported (you need two separate environments)

Not D as we have a single RDS DB instance, no HA

Both A and B does the job, but B provides better scalability as it make use of Aurora Multi-AZ that allows secondary (reader) instance(s) to be accessed for reads, while RDS Multi-AZ instance does not allow standby instance endpoint to be accessed. This could be circumvented by using Multi-AZ DB cluster deployment that provides 2 readable standby instance

upvoted 1 times

 **ayadmawla** 2 years ago

Selected Answer: C

Answer is C

The best way to migrate a .NET application to AWS is via Beanstalk (see: <https://docs.aws.amazon.com/whitepapers/latest/develop-deploy-dotnet-apps-on-aws/aws-elastic-beanstalk.html>)

I think that the question regarding spanning a deployment across two regions has triggered some to reject based on the multi-region but if you continue you will notice the separate regional deployments based on two ALBs etc. Just my two pennies :)

upvoted 2 times

 **subbupro** 2 years ago

B is the correct,

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: B

Answer B

upvoted 1 times

 **abeb** 2 years, 1 month ago

B is good

upvoted 1 times

Question #38

A company is using AWS Organizations to manage multiple AWS accounts. For security purposes, the company requires the creation of an Amazon Simple Notification Service (Amazon SNS) topic that enables integration with a third-party alerting system in all the Organizations member accounts.

A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to automate the deployment of CloudFormation stacks. Trusted access has been enabled in Organizations.

What should the solutions architect do to deploy the CloudFormation StackSets in all AWS accounts?

- A. Create a stack set in the Organizations member accounts. Use service-managed permissions. Set deployment options to deploy to an organization. Use CloudFormation StackSets drift detection.
- B. Create stacks in the Organizations member accounts. Use self-service permissions. Set deployment options to deploy to an organization. Enable the CloudFormation StackSets automatic deployment.
- C. Create a stack set in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.
- D. Create stacks in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection.

Correct Answer: C

Community vote distribution

C (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: C

The best solution is C, because it involves creating the stack set in the management account of the organization, which is the central point of control for all the member accounts. This allows the solutions architect to manage the deployment of the stack set across all member accounts from a single location. Service-managed permissions are used, which allows the CloudFormation service to deploy the stack set to all member accounts. The deployment options are set to deploy to the organization and automatic deployment is enabled, which ensures that the stack set is automatically deployed to all member accounts as soon as it is created in the management account.

upvoted 22 times

 **masetromain** Highly Voted 3 years ago

Selected Answer: C

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

upvoted 5 times

 **princajen** Most Recent 5 months, 2 weeks ago

Selected Answer: C

Only the management account can deploy across the organization using service-managed permissions.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

C. Create a stack set in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.

upvoted 1 times

 **Vaibs099** 1 year, 11 months ago

C. Create a stack set in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.

C is more suitable as Enable CloudFormation StackSets automatic deployment will take care of any new account in the Org. Set deployment options to deploy to the organization helps deploying Stack Instances to targeted account in Org. Use service-managed permissions is hassle free as it takes care of roles for you.

D. Create stacks in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection.

D is good option too as StackSets drift detection is a good option to have but not a requirement. It only saves from future troubleshooting of drift scenarios.

upvoted 1 times

 **nharaz** 1 year, 11 months ago

Selected Answer: C

D is wrong - Drift Detection identifies unmanaged changes (Outside CloudFormation)

upvoted 3 times

✉ **jainparag1** 2 years, 1 month ago

Selected Answer: C

I'll go with C since it satisfies all the requirements with minimum operational overhead. But wondering if "Stack Sets drift detection" is just a distractor here. Can someone throw some light on this?

upvoted 2 times

✉ **ninomfr64** 2 years ago

I am not an expert, just sharing my thoughts:

"Stack Sets drift detection" is a feature of stack set, however this is not needed according to the scenario.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-drift.html>.

D is a no-go for me because it deploys in each managed account without making use of stack sets, so you cannot then use stack sets drift detection.

upvoted 1 times

✉ **daz2023** 2 years, 2 months ago

Selected Answer: C

C is the right answer

upvoted 1 times

✉ **NikkyDicky** 2 years, 6 months ago

Selected Answer: C

C no brainer

upvoted 1 times

✉ **mfsec** 2 years, 9 months ago

Selected Answer: C

Create a stack set in the Organizations management account.

upvoted 2 times

✉ **spd** 2 years, 10 months ago

Selected Answer: C

Stack Set in Mgmt account

upvoted 2 times

✉ **Atila50** 3 years ago

I THINK I SHOULD BE A

upvoted 1 times

Question #39

A company wants to migrate its workloads from on premises to AWS. The workloads run on Linux and Windows. The company has a large on-premises infrastructure that consists of physical machines and VMs that host numerous applications.

The company must capture details about the system configuration, system performance, running processes, and network connections of its on-premises workloads. The company also must divide the on-premises applications into groups for AWS migrations. The company needs recommendations for Amazon EC2 instance types so that the company can run its workloads on AWS in the most cost-effective manner.

Which combination of steps should a solutions architect take to meet these requirements? (Choose three.)

- A. Assess the existing applications by installing AWS Application Discovery Agent on the physical machines and VMs.
- B. Assess the existing applications by installing AWS Systems Manager Agent on the physical machines and VMs.
- C. Group servers into applications for migration by using AWS Systems Manager Application Manager.
- D. Group servers into applications for migration by using AWS Migration Hub.
- E. Generate recommended instance types and associated costs by using AWS Migration Hub.
- F. Import data about server sizes into AWS Trusted Advisor. Follow the recommendations for cost optimization.

Correct Answer: ADE*Community vote distribution*

ADE (96%) 4%

 **bititan**  2 years, 11 months ago

Selected Answer: ADE

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

upvoted 24 times

 **ninomfr64**  2 years ago

Selected Answer: ADE

A vs B -> A because we need to use AWS Application Discovery and it provides its own agent
<https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-agent.html>

C vs D -> D because AWS Application Discovery is integrated with AWS Migration Hub and it can be used to group servers into applications
<https://aws.amazon.com/migration-hub/faqs/#:~:text=How%20do%20I%20group%20servers%20into%20an%20application%3F>

E vs. F -> E as AWS Migration Hub allows to generate recommendation for instance types
<https://docs.aws.amazon.com/migrationhub/latest/ug/ec2-recommendations.html>

upvoted 7 times

 **princajen**  5 months, 2 weeks ago

Selected Answer: ADE

1. Install the AWS Application Discovery Agent to collect on-prem data (A).
2. Group resources into applications using AWS Migration Hub (D).
3. Use Migration Hub to generate EC2 instance type and cost recommendations (E).

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

- A. Assess the existing applications by installing AWS Application Discovery Agent on the physical machines and VMs.
- 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.

upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

Selected Answer: ADE

Why not B ? B. Assess the existing applications by installing AWS Systems Manager Agent on the physical machines and VMs:

Explanation: AWS Systems Manager Agent is used for managing and automating tasks on EC2 instances, not for capturing detailed application and performance data during an assessment phase. AWS Application Discovery Agent is more appropriate for this purpose.
 upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: ADE

ADE is correct

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: ADE

The correct answers are:

- * A. Assess the existing applications by installing AWS Application Discovery Agent on the physical machines and VMs. The AWS Application Discovery Service helps gather detailed information about on-premises data centers, including servers, network dependencies, and performance metrics.
- * D. Group servers into applications for migration by using AWS Migration Hub. AWS Migration Hub provides a centralized location to track the progress of application migrations across multiple AWS and partner solutions. It allows grouping discovered servers into applications, which simplifies the organization of migration tasks.
- * E. Generate recommended instance types and associated costs by using AWS Migration Hub. After servers are discovered and grouped into applications, AWS Migration Hub can analyze the collected data to recommend suitable Amazon EC2 instance types. This ensures that the migrated applications are hosted on the most cost-effective resources.

upvoted 4 times

 **Simon523** 2 years, 3 months ago

Selected Answer: ADE

<https://aws.amazon.com/tw/blogs/mt/using-aws-migration-hub-network-visualization-to-overcome-application-and-server-dependency-challenges/>

upvoted 2 times

 **NikkyDicky** 2 years, 6 months ago

Selected Answer: ADE

ADE no brainer

upvoted 1 times

 **ZK000001qws** 2 years, 6 months ago

B is incorrect as System Manager doesn't do discovery however, SSM Agent makes it possible for Systems Manager to update, manage, and configure the resources in AWS as well as on-premises. ADE

upvoted 3 times

 **asifjanjua88** 2 years, 8 months ago

ADE is correct answer.

upvoted 1 times

 **Jacky_exam** 2 years, 8 months 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** 2 years, 9 months ago

B is incorrect because the servers are on prem.

upvoted 1 times

 **ninomfr64** 2 years ago

SSM can be installed on on-premise server. This is not the point for not picking B

upvoted 1 times

 **dev112233xx** 2 years, 9 months ago

Selected Answer: ADE

ADE no doubts 

upvoted 1 times

 **God_Is_Love** 2 years, 10 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** 2 years, 10 months ago

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

upvoted 1 times

 **sambb** 2 years, 10 months ago

AWS SSM Application Manager is used for existing resources deployed to AWS
upvoted 1 times

 **moota** 2 years, 10 months 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

Question #40

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 VPC and attach an endpoint policy to the endpoint to allow the required actions on the S3 bucket.
- D. Attach an Amazon Elastic File System (Amazon EFS) volume to the EC2 instances. Host the images on the EFS volume.

Correct Answer: C

Community vote distribution

C (100%)

 **masetromain** Highly Voted 2 years, 5 months ago

Selected Answer: C

C. Setting up an S3 gateway VPC endpoint in the VPC and attaching an endpoint policy to the endpoint will allow the EC2 instances to securely access the S3 bucket for image storage without the need for NAT gateways, reducing costs without compromising security or increasing ongoing operations. This option reduces the costs associated with the NAT gateways and allows for faster data retrieval from the S3 bucket as traffic does not have to go through the internet gateway.

upvoted 15 times

 **God_Is_Love** Highly Voted 2 years, 4 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 7 times

 **anita_student** 2 years, 4 months ago

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

upvoted 1 times

 **princajen** Most Recent 5 months, 2 weeks ago

Selected Answer: C

By using a VPC Gateway Endpoint for Amazon S3, traffic between the EC2 instances and S3: Stays within the AWS network, avoiding NAT and internet traffic.

Does not incur NAT gateway data processing or data transfer charges.

Improves security because S3 access doesn't require internet access.

Operational Simplicity: A Gateway Endpoint is easy to configure and requires minimal ongoing maintenance, aligning with the requirement to avoid increasing operational overhead.

upvoted 1 times

 **8608f25** 1 year, 4 months ago

Selected Answer: C

Option C is the most cost-effective solution that maintains the service's security posture. An S3 gateway VPC endpoint allows private connections between the VPC and S3 without requiring traffic to go through the internet or NAT gateways. This eliminates the need for NAT gateways when accessing S3, which can significantly reduce costs, especially considering the 1 TB of data retrieved daily from S3. Endpoint policies ensure that the security posture is not compromised by allowing only the required actions on the specific S3 bucket.

upvoted 1 times

 **grire974** 1 year, 5 months ago

Any chance someone could fix the typo in the correct answer; "VPC. Attach..." instead of VPAttach; terribly misleading.

upvoted 2 times

✉️  **daz2023** 1 year, 9 months ago

Selected Answer: C

C for using an endpoint.

upvoted 2 times

✉️  **NikkyDicky** 1 year, 12 months ago

C of course

upvoted 1 times

✉️  **gameoflove** 2 years, 1 month ago

Selected Answer: C

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

upvoted 2 times

✉️  **mfsec** 2 years, 3 months ago

Selected Answer: C

Set up an S3 gateway VPC endpoint

upvoted 3 times

✉️  **dev112233xx** 2 years, 3 months ago

Selected Answer: C

C - easy one 

upvoted 3 times

✉️  **zozza2023** 2 years, 5 months ago

Selected Answer: C

C for sure

upvoted 4 times

Question #41

A company recently deployed an application on AWS. The application uses Amazon DynamoDB. The company measured the application load and configured the RCU and WCU on the DynamoDB table to match the expected peak load. The peak load occurs once a week for a 4-hour period and is double the average load. The application load is close to the average load for the rest of the week. The access pattern includes many more writes to the table than reads of the table.

A solutions architect needs to implement a solution to minimize the cost of the table.

Which solution will meet these requirements?

- A. Use AWS Application Auto Scaling to increase capacity during the peak period. Purchase reserved RCUs and WCUs to match the average load.
- B. Configure on-demand capacity mode for the table.
- C. Configure DynamoDB Accelerator (DAX) in front of the table. Reduce the provisioned read capacity to match the new peak load on the table.
- D. Configure DynamoDB Accelerator (DAX) in front of the table. Configure on-demand capacity mode for the table.

Correct Answer: A*Community vote distribution*

A (69%)	B (20%)	11%
---------	---------	-----

 **zhangyu20000** Highly Voted 2 years, 11 months ago

A is correct. On demand mode is for unknown load pattern, auto scaling is for known burst pattern
upvoted 25 times

 **AimarLeo** 1 year, 10 months ago

But the pattern here is known.. 4 hours peak time etc.. not sure if that would be the write answer
upvoted 1 times

 **dqwsmttvtgxwkvgcvc** 2 years, 4 months ago

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

 **tannh** 2 years, 3 months ago

You can scale DynamoDB tables and global secondary indexes using target tracking scaling policies and scheduled scaling.
<https://docs.aws.amazon.com/autoscaling/application/userguide/services-that-can-integrate-dynamodb.html>
upvoted 2 times

 **ccort** Highly Voted 2 years, 11 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 16 times

 **princajen** Most Recent 5 months, 2 weeks ago

Selected Answer: A

Use AWS Application Auto Scaling to scale provisioned capacity and purchase reserved capacity for the average load.

Best for known, bursty pattern

Most cost-efficient in the long term

Slightly more setup effort but pays off

upvoted 1 times

 **zhen234** 11 months, 2 weeks ago

Selected Answer: A

Reserved capacity applies to the baseline level of provisioned throughput. During peak workloads, Auto Scaling dynamically adjusts the provisioned capacity of a DynamoDB table (RCUs and WCUs) based on the actual workload. You are charged on-demand rates for the excess capacity.

upvoted 1 times

 **wem** 1 year ago

Selected Answer: B

B. Configure on-demand capacity mode for the table.

Explanation:

On-Demand Capacity Mode:

DynamoDB's on-demand capacity mode automatically adjusts to accommodate variable workloads.

It eliminates the need to provision RCUs and WCUs, allowing the table to scale up during the 4-hour peak period and scale down during off-peak times, which is cost-effective when usage is highly variable.

Cost Optimization:

With on-demand capacity, you pay only for the read and write requests that are made. This is ideal for workloads with sporadic or unpredictable traffic patterns, such as this scenario with a weekly 4-hour peak.

Minimized Operational Overhead:

On-demand mode requires no manual adjustments or additional services (like Application Auto Scaling), simplifying management and reducing costs related to provisioning errors or overprovisioning.

Access Pattern with More Writes:

On-demand capacity mode is well-suited for write-heavy workloads as it scales automatically to handle higher write throughput during peak times.

upvoted 3 times

 **5e8c031** 6 months ago

Except that this scenario with a known average and a weekly 4-hour peak is neither unpredictable nor sporadic.

upvoted 1 times

 **Sin_Dan** 1 year, 2 months ago

Selected Answer: B

B is the right answer. Reserved RCU/WCU locks you into fixed cost. Even though on demand is more expensive, the additional cost is paid only for 4 hrs a week.

upvoted 2 times

 **DhirajBansal** 1 year, 1 month ago

but Yes, here in option A it is saying for purchasing average load RCUs and WCUs which will cost less and also auto scaling can be used for scheduled scaling WCU and RCUs which will be cost efficient.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. Use AWS Application Auto Scaling to increase capacity during the peak period. Purchase reserved RCUs and WCUs to match the average load.

upvoted 1 times

 **subbupro** 1 year, 4 months ago

I think B is correct. because reserved is not required, ondemand would be better because it requires only 4 hours per week. so B would be better. Autoscaling of the application can not impact dynamo db tables.

upvoted 1 times

 **vn_hunglv** 1 year, 5 months ago

Selected Answer: A

Tôi chọn A

upvoted 1 times

 **zolthar_z** 1 year, 5 months ago

Selected Answer: A

Auto-scaling is for known traffic pattern, On-demand is for unknown traffic pattern and also could be more expensive

upvoted 2 times

 **Malcnorth59** 1 year, 7 months ago

Selected Answer: A

AWS documentation suggests A is correct:

<https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html>

upvoted 4 times

 **mnsait** 1 year, 1 month ago

Nice. Thanks for the link. It explains clearly.

See this: "Scheduled scaling – Scale a resource one time only or on a recurring schedule."

upvoted 1 times

 **Kubernetes** 1 year, 8 months ago

A is correct. The focus is minimizing the cost of tables.

upvoted 2 times

 **mav3r1ck** 1 year, 9 months ago

Selected Answer: B

Considering the application's need to handle a peak load that is double the average and the fact that the workload is write-heavy, option B (Configure on-demand capacity mode for the table) is the most suitable solution. It directly addresses the variability in workload without requiring upfront capacity planning or additional management overhead, thus likely providing the best cost optimization for this scenario.

On-demand capacity mode eliminates the need to scale resources manually or through Auto Scaling and ensures that you only pay for the write and read throughput you consume.

upvoted 2 times

✉  **mav3r1ck** 1 year, 9 months ago

A. AWS Application Auto Scaling with Reserved Capacity

Pros: Auto Scaling allows you to automatically adjust the provisioned throughput to meet demand, and purchasing reserved RCU and WCU can reduce costs for the capacity you know you'll consistently use.

Cons: This option might not be as cost-effective for workloads with significant variability and a high write-to-read ratio, especially if the peak load is much higher than the average load. Reserved capacity benefits consistent usage patterns, but the peak load being double the average may not be fully optimized here.

upvoted 1 times

✉  **mav3r1ck** 1 year, 9 months ago

B. On-demand Capacity Mode

Pros: On-demand capacity mode is ideal for unpredictable workloads because it automatically scales to accommodate the load without provisioning. You pay for what you use without managing capacity planning. This mode is particularly suitable for the described scenario where the load spikes significantly and unpredictably.

Cons: While potentially more expensive per unit than provisioned capacity with auto-scaling, it eliminates the risk of over-provisioning or under-provisioning.

upvoted 1 times

✉  **kz407** 1 year, 9 months ago

Selected Answer: A

A is badly worded however, because it says "application" autoscaling. We are not talking about that here. Either it should be reworded as "DynamoDB autoscaling" for the answer to be correct.

On-demand capacity mode is for unknown read/write patterns. Since the load change patterns are known, anything that involves on-demand capacity modes can be eliminated (hence not B).

DAX is a caching service deployed in front of DynamoDB. It is geared towards "performance at scale". Problem in the use case, is to optimize table costs. Using DAX will incur additional costs. Hence anything that involves DAX (C and D) can also be eliminated.

upvoted 2 times

✉  **Malcnorth59** 1 year, 7 months ago

I initially thought the same but the AWS definition of Application autoscaling listed here includes DynamoDB:

<https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html>

upvoted 1 times

✉  **anubha.agrahari** 1 year, 9 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/#:~:text>You%20can%20approximate%20a%20blend,save%20money%20as%20reserved%20capacity>

upvoted 2 times

✉  **8608f25** 1 year, 10 months ago

Selected Answer: B

Option B is the most cost-effective solution for workloads with significant fluctuations and unpredictable access patterns. The on-demand capacity mode automatically adjusts the table's throughput capacity as needed in response to actual traffic, eliminating the need to manually configure or manage capacity. This mode is ideal for applications with irregular traffic patterns, such as a significant peak once a week, because you only pay for the read and write requests your application performs, without having to provision throughput in advance. Option B directly addresses the requirement to minimize costs associated with fluctuating loads, especially when the load significantly exceeds the average only during a brief period, by leveraging DynamoDB's on-demand capacity mode to automatically scale and pay only for what is used.

upvoted 1 times

✉  **igor12ghsj577** 1 year, 10 months ago

Selected Answer: A

I think there is mistake in answer A, and it should be DynamoDb auto scaling instead of application autos calling. Or application and dynamoDB auto scaling.

upvoted 1 times

✉  **igor12ghsj577** 1 year, 10 months ago

Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read and write capacity to handle sudden increases in traffic, without throttling. When the workload decreases, Application Auto Scaling decreases the throughput so that you don't pay for unused provisioned capacity.

upvoted 2 times

Question #42

A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours.

What is the MOST cost-effective migration recommendation?

- A. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in an Amazon S3 bucket.
- B. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the files. Store the processed files in Amazon EFS. Shut down the EC2 instance after the task is complete.
- C. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in Amazon EFS.
- D. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. Use Amazon EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the files. Scale the EC2 instances based on the SQS queue length. Store the processed files in an Amazon S3 bucket.

Correct Answer: D

Community vote distribution

D (96%)	2%
---------	----

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: D

The correct answer would be option D.

This option suggests creating a queue using Amazon SQS, configuring the existing web server to publish to the new queue, and using EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the files. The EC2 instances can be scaled based on the SQS queue length, which ensures that the resources are available during peak usage times and reduces costs during non-peak times.

Option A is not correct because it suggests using AWS Lambda which has a maximum execution time of 15 minutes.

Option B is not correct because it suggests creating a new EC2 instance for each message in the queue, which is not cost-effective.

Option C is not correct because it suggests using Amazon EFS, which is not a suitable option for long-term storage of large files.

upvoted 24 times

 **ninomfr64** Highly Voted 2 years ago

Selected Answer: D

Not A - Lambda max execution time is 15 minutes, image processing can take up to 1 hour

Not B - Amazon MQ is not needed (more expensive than SQS) and EFS is more expensive than S3

Not C - Amazon MQ is not needed (more expensive than SQS) and Lambda max execution time is 15 minutes, image processing can take up to 1 hour

D does the job with the lower cost thanks to SQS, S3 and EC2 Auto Scaling Group

upvoted 7 times

 **princajen** Most Recent 5 months, 2 weeks ago

Selected Answer: D

A. Lambda functions cannot handle 1-hour processing task (max 15 min timeout)

B. Amazon MQ more complex and expensive than SQS. Single EC2 instance per task is less efficient than scaling based on queue length.

C. Again Lambda cannot handle 1 hour jobs.

upvoted 1 times

 **mohan_cv** 1 year, 1 month ago

Exam AWS Certified Solutions Architect - Professional SAP-C02 topic 1 question 42 discussion

upvoted 1 times

 **Malcnorth59** 1 year, 7 months ago

Selected Answer: D

Lambda will not work, so A is not possible.

D is going to be the most cost-effective as the resources will scale based on queue length.

upvoted 1 times

✉ mav3r1ck 1 year, 9 months ago

Selected Answer: D

Given the need to process files that can take up to 1 hour each and the variability in workload, option D (Amazon SQS, EC2 Auto Scaling, and S3) appears to be the most cost-effective and practical solution. It leverages SQS for queue management, enabling efficient handling of the processing queue's variability. EC2 Auto Scaling allows for flexible and cost-effective scaling of processing capacity, ramping up during high-demand periods and scaling down when demand wanes, thus optimizing costs. Finally, Amazon S3 offers a highly durable and cost-effective solution for storing the processed media files. This option provides the necessary flexibility for long processing tasks while efficiently managing the variable demand and optimizing storage costs.

upvoted 1 times

✉ Simon523 2 years, 3 months ago

Selected Answer: D

Simple Queuing Service

SQS is based on pull model. Here are some of the important features:

Reliable, scalable, fully-managed message queuing service

High availability

Unlimited scaling

Auto scale to process billions of messages per day

Low cost (Pay for use)

upvoted 1 times

✉ aviathor 2 years, 3 months ago

Selected Answer: D

This is quite simple. Any answer (A and C) consisting of using Lambda for processing the files is out because of the 15 minutes limit on Lambda processes.

B is out because using EFS is expensive and it does not specify how to launch and terminate the EC2 instances. Amazon MQ is not required either.

This leaves D which uses SQS, Auto Scaling Groups and publishes the resulting files to S3.

upvoted 2 times

✉ chico2023 2 years, 4 months 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 years, 6 months ago

Selected Answer: D

d for sure

upvoted 1 times

✉ ailves 2 years, 6 months 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 2 years, 7 months ago

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

upvoted 1 times

✉ huanaws088 2 years, 8 months ago

Selected Answer: B

I sure is B , because

1. SQS , SNS are " cloud - native " services : proprietary protocols from AWS

2. Traditional applications running from on - premises may use open protocols such as : MQTT , AMQP ... , so When migrating to the cloud , instead of re-engineering the application to use SQS and SNS will very expensive, we can use Amazon MQ.

3. Amazon MQ doesn't " scale " as much as SQS / SNS Amazon MQ runs on servers but Amazon MQ has both queue feature (~ SQS) and topic features (~ SNS)

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-difference-from-amazon-mq-sns.html>

upvoted 1 times

✉ hexie 2 years, 5 months 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 2 years, 9 months ago

Selected Answer: D

SQS and autoscaling no doubt answer is D
upvoted 2 times

 **mfsec** 2 years, 9 months ago

Selected Answer: D
SQS and Auto Scaling
upvoted 2 times

 **dev112233xx** 2 years, 9 months 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** 2 years, 10 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

Question #43

Topic 1

A company is using Amazon OpenSearch Service to analyze data. The company loads data into an OpenSearch Service cluster with 10 data nodes from an Amazon S3 bucket that uses S3 Standard storage. The data resides in the cluster for 1 month for read-only analysis. After 1 month, the company deletes the index that contains the data from the cluster. For compliance purposes, the company must retain a copy of all input data.

The company is concerned about ongoing costs and asks a solutions architect to recommend a new solution.

Which solution will meet these requirements MOST cost-effectively?

- A. Replace all the data nodes with UltraWarm nodes to handle the expected capacity. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.
- B. Reduce the number of data nodes in the cluster to 2 Add UltraWarm nodes to handle the expected capacity. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data. Transition the input data to S3 Glacier Deep Archive after 1 month by using an S3 Lifecycle policy.
- C. Reduce the number of data nodes in the cluster to 2. Add UltraWarm nodes to handle the expected capacity. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data. Add cold storage nodes to the cluster. Transition the indexes from UltraWarm to cold storage. Delete the input data from the S3 bucket after 1 month by using an S3 Lifecycle policy.
- D. Reduce the number of data nodes in the cluster to 2. Add instance-backed data nodes to handle the expected capacity. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.

Correct Answer: B

Community vote distribution

B (95%)	5%
---------	----

✉  **masetromain**  2 years, 11 months ago

Selected Answer: B

B is the most cost-effective solution as it reduces the number of data nodes in the cluster to 2 and adds UltraWarm nodes to handle the expected capacity. By configuring the indexes to transition to UltraWarm when OpenSearch Service ingests the data, the company can take advantage of the lower storage costs of UltraWarm. Additionally, by transitioning the input data to S3 Glacier Deep Archive after 1 month using an S3 Lifecycle policy, the company can further reduce costs by using the lower storage costs of S3 Glacier Deep Archive for long-term data retention.

upvoted 23 times

✉  **masetromain** 2 years, 11 months ago

Option C can meet the requirements of reducing the number of data nodes in the cluster and using UltraWarm and cold storage nodes to handle the expected capacity and moving the data to lower cost storage after 1 month. However, it may not be the most cost-effective solution as it involves additional complexity in configuring the indexes to transition between different storage tiers, and may also require additional management and maintenance of the cold storage nodes. Option B, where the data is transitioned from S3 Standard to S3 Glacier Deep Archive using an S3 Lifecycle policy is simpler and more cost-effective as it eliminates the need for additional storage tiers and management.

upvoted 3 times

✉  **God_Is_Love** 2 years, 10 months ago

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

upvoted 5 times

✉  **God_Is_Love** 2 years, 10 months ago

* I meant C says..

upvoted 5 times

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

Selected Answer: B

A: Replacing all data nodes with UltraWarm is not supported.

C: Deleting the input data from S3 violates compliance

D: Transitioning data to Glacier Deep Archive when loading contradicts the need to retain it for 1 month for analysis.

upvoted 1 times

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

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.

upvoted 1 times

✉  **Malcnorth59** 1 year, 7 months ago

Why can't I switch all nodes to ultrawarm. I can't find it anywhere in the documentation and it's not listed in the pre-requisites.

Also why can the number of nodes be reduced from 10 to 2? is that because Ultrawarm use S3?

upvoted 1 times

✉  **sarlos** 1 year, 8 months ago

why not D?

upvoted 1 times

✉  **nynomfr64** 2 years ago

I need help here:

To use UltraWarm storage, domains must have dedicated master nodes as per doc <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/ultrawarm.html>

The scenario mentions "an OpenSearch Service cluster with 10 data nodes". Assuming you only have these nodes in the cluster, in all answers you need to add dedicated master node(s). Assuming we also have dedicated master node why not replacing all data nodes with UltraWarm nodes?

upvoted 1 times

✉  **nynomfr64** 2 years ago

I think I got it, UltraWarm is for read-only data. Thus you still need to have at least a data node

upvoted 1 times

✉  **venvig** 2 years, 4 months 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 3 times

✉  **NikkyDicky** 2 years, 6 months ago

Selected Answer: B

B I think :/

upvoted 2 times

✉  **Damijo** 2 years, 9 months ago

Selected Answer: A

If you look at the IAM documentation here, you can see that the ec2:AuthorizeSecurityGroupIngress action doesn't have any conditions that would allow you to specify the ip addresses in the inbound/outbound rules.https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonec2.html

upvoted 2 times

✉  **Jesuisleon** 2 years, 6 months ago

I think you are referring All AWS Certified Solutions Architect - Professional SAP-C02 Questions, question 44. yes, I changed from D to A after reading this link.

upvoted 1 times

✉  **eddylynx** 2 years, 5 months 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

✉  **dev112233xx** 2 years, 9 months ago

Selected Answer: B

B - makes more sense

upvoted 4 times

✉  **Ajani** 2 years, 9 months 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 3 times

✉  **moota** 2 years, 10 months 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** 2 years, 10 months ago

This eliminates option A

upvoted 3 times

 **Musk** 2 years, 11 months ago

Selected Answer: B

Option B is the most cost-effective solution that meets the requirements. Reducing the number of data nodes in the cluster and adding UltraWarm nodes will help to reduce the ongoing costs of running the OpenSearch Service cluster. Configuring the indexes to transition to UltraWarm when OpenSearch Service ingests the data will further reduce costs. Additionally, transitioning the input data to S3 Glacier Deep Archive after 1 month by using an S3 Lifecycle policy will lower the storage costs of retaining the input data for compliance purposes.

upvoted 4 times

Question #44

Topic 1

A company has 10 accounts that are part of an organization in AWS Organizations. AWS Config is configured in each account. All accounts belong to either the Prod OU or the NonProd OU.

The company has set up an Amazon EventBridge rule in each AWS account to notify an Amazon Simple Notification Service (Amazon SNS) topic when an Amazon EC2 security group inbound rule is created with 0.0.0.0/0 as the source. The company's security team is subscribed to the SNS topic.

For all accounts in the NonProd OU, the security team needs to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source.

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

- A. Modify the EventBridge rule to invoke an AWS Lambda function to remove the security group inbound rule and to publish to the SNS topic. Deploy the updated rule to the NonProd OU.
- B. Add the vpc-sg-open-only-to-authorized-ports AWS Config managed rule to the NonProd OU.
- C. Configure an SCP to allow the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:SourceIp 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:SourceIp condition key is 0.0.0.0/0. Apply the SCP to the NonProd OU.

Correct Answer: D*Community vote distribution*

D (59%)

A (38%)

 **masetromain**  2 years, 11 months ago

Selected Answer: D

The solution that meets this requirement with the LEAST operational overhead is D. Configuring an SCP to deny the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:SourceIp 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 55 times

 **masetromain** 2 years, 11 months ago

Option C does not meet the requirement that the security team needs to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source. It only allows the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:SourceIp 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:SourceIp condition key is 0.0.0.0/0. This will prevent the creation of any security group inbound rule that includes 0.0.0.0/0 as the source.

upvoted 6 times

 **MikelH93** 2 years, 7 months ago

the answer can't be C or D because aws:SourceIp condition key don't exist with SCP.

So answer is A

upvoted 4 times

 **b3llman** 2 years, 4 months ago

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

upvoted 4 times

 **mifune** 1 year, 8 months ago

You mean something like this? It's from the AWS portal...

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "0.0.0.0/0"
          ]
        }
      }
    }
  ]
}
```

```

    "192.0.2.0/24",
    "203.0.113.0/24"
]
}
}
}
}

upvoted 4 times

```

✉ **aokaddaoc** 2 years, 1 month ago

I think the reason why C is wrong is not because C does not meet the requirement but simply because it is too strong: All users can do is to set ingress rule in SG and all other actions are all blocked. Both C and D results the same which users can no longer able to open port to 0.0.0.0/0, but D is more precise without blocking other actions.

upvoted 2 times

✉ **Maria2023**  2 years, 6 months 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:SourceIp": [
"0.0.0.0/0"
]
}
}
}
}

upvoted 37 times

```

✉ **b3llman** 2 years, 4 months ago

Tested and confirmed!

upvoted 6 times

✉ **dqwsrnwwvtgxwkvvcvc** 2 years, 4 months 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 SourceIp is not 0.0.0.0/0?

upvoted 1 times

✉ **vn_thanh tung** 2 years, 3 months 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** 2 years, 3 months ago

Sorry typo.

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

upvoted 1 times

✉ **longns** 2 years, 2 months ago

This will deny all action create a inbound rule not only Inbound rule which have source ip "0.0.0.0/0"

upvoted 4 times

✉ **Malcnorth59** 1 year, 7 months ago

I think that is incorrect. the SCP action is ec2:AuthorizeSecurityGroupIngress and specifically applies to ingress

upvoted 1 times

✉ **tgv** 11 months ago

Tested myself, but this blocks any attempt to create an ingress rule - not only ones that have 0.0.0.0/0 as a source.

aws:SourceIp checks for the IP address of the requester

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html#condition-keys-sourceip

With these options, I think the only option that still stands is [A].

I don't like it because it adds management overhead and it's not preventive - it's reactive. But it seems like the only one which actually performs the task it was asked to perform.

upvoted 1 times

✉ 12db8b7 6 months ago

A can't be because u can create the resource and then is deleted, the question ask to "needs to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source", in A scenario u can do it, just deletes the rule afterwards.
upvoted 1 times

✉ proawsk [Most Recent] 8 months ago

Selected Answer: B

B is correct, you cannot deny SG rule creation with SCP
upvoted 1 times

✉ tgv 11 months ago

Selected Answer: A

aws:SourceIp checks for the ip address of the requester - not the CIDR destination in the rule
upvoted 1 times

✉ TorTo 11 months ago

Selected Answer: D

The only correct answer is D.
The questions states "to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source"

A does not remove the ability, it only corrects the action.
D is correct because it actually restricts the ability.
upvoted 2 times

✉ altonh 11 months, 3 weeks ago

Selected Answer: A

Not D. See here: https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonec2.html. Condition key aws:SourceIp is missing for ec2:AuthorizeSecurityGroupIngress
upvoted 1 times

✉ grumpysloth 1 year ago

Selected Answer: A

You cannot use SCP to control SG rules
upvoted 1 times

✉ chipimbiri 1 year, 1 month ago

Selected Answer: D

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_evaluation.html
An Allow statement in an SCP can't have a Condition element at all.
upvoted 1 times

✉ sashenka 1 year, 2 months ago

Selected Answer: A

Given that the aws:SourceIp condition key refers to the IP address of the principal making the request, and not the IP address specified in the security group rule, D is not appropriate for this scenario.
upvoted 3 times

✉ attila9778 1 year ago

But because of this B is the correct option.

upvoted 1 times

✉ amministrazione 1 year, 3 months ago

D. Configure an SCP to deny the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:SourceIp condition key is 0.0.0.0/0.
Apply the SCP to the NonProd OU.
upvoted 1 times

✉ MAZIADI 1 year, 4 months ago

Selected Answer: D

Why Option D is Better than Option C:
Explicit Deny vs. Implicit Allow:

Option C allows the action unless the aws:SourceIp is 0.0.0.0/0. This creates an implicit allow policy, which means that if any condition is not met, the action is allowed.
Option D uses an explicit deny, which is more secure and straightforward. An explicit deny ensures that if the condition is met (aws:SourceIp is 0.0.0.0/0), the action is blocked regardless of other permissions.
upvoted 3 times

✉ asquared16 1 year, 5 months ago

Selected Answer: A

It's A. Definitely A. Don't get confused.
upvoted 1 times

✉ dzidis 1 year, 6 months ago

Voting for A
upvoted 1 times

 **teo2157** 1 year, 7 months ago

Selected Answer: A

It's A, D is incorrect as it shouldn't be source IP but destination address
upvoted 1 times

 **Malcnorth59** 1 year, 7 months ago

Selected Answer: D

Option D
upvoted 1 times

 **sse69** 1 year, 7 months ago

Selected Answer: A

SourceIP is for requester IP address, not the CIDR referenced in the SG rule.
upvoted 3 times

 **Smart** 1 year, 8 months ago

A (Incorrect): SG is created for a briefly. This goes against the question requirement of "remove the ability to create a security group inbound rule..."
B (Incorrect): Regardless of rule, SGs can be created and remain non-compliant.
C (Incorrect): See D
D (Incorrect): SourceIP condition key of IAM policy is the requestor's IP address. This has nothing to do with SG's inbound rule's sourceIP. This won't allow creating any SG inbound rules when the requestor is making AWS API calls from anywhere (0.0.0.0/0).

Just a crap question and choices.

upvoted 3 times

Question #45

Topic 1

A company hosts a Git repository in an on-premises data center. The company uses webhooks to invoke functionality that runs in the AWS Cloud. The company hosts the webhook logic on a set of Amazon EC2 instances in an Auto Scaling group that the company set as a target for an Application Load Balancer (ALB). The Git server calls the ALB for the configured webhooks. The company wants to move the solution to a serverless architecture.

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

- A. For each webhook, create and configure an AWS Lambda function URL. Update the Git servers to call the individual Lambda function URLs.
- B. Create an Amazon API Gateway HTTP API. Implement each webhook logic in a separate AWS Lambda function. Update the Git servers to call the API Gateway endpoint.
- C. Deploy the webhook logic to AWS App Runner. Create an ALB, and set App Runner as the target. Update the Git servers to call the ALB endpoint.
- D. Containerize the webhook logic. Create an Amazon Elastic Container Service (Amazon ECS) cluster, and run the webhook logic in AWS Fargate. Create an Amazon API Gateway REST API, and set Fargate as the target. Update the Git servers to call the API Gateway endpoint.

Correct Answer: B

Community vote distribution

B (73%)	A (17%)	10%
---------	---------	-----

 **masetromain** Highly Voted  2 years, 11 months ago

Selected Answer: B

B. Create an Amazon API Gateway HTTP API. Implement each webhook logic in a separate AWS Lambda function. Update the Git servers to call the API Gateway endpoint. This solution will provide low operational overhead as it utilizes the serverless capabilities of AWS Lambda and API Gateway, which automatically scales and manages the underlying infrastructure and resources. It also allows for the webhook logic to be easily managed and updated through the API Gateway interface.

The answer should be B because it is the best solution in terms of operational overhead.

upvoted 25 times

 **masetromain** 2 years, 11 months ago

Option A would require updating the Git servers to call individual Lambda function URLs for each webhook, which would be more complex and time-consuming than calling a single API Gateway endpoint.

Option C would require deploying the webhook logic to AWS App Runner, which would also be more complex and time-consuming than using an API Gateway.

Option D would also require containerizing the webhook logic and creating an ECS cluster and Fargate, which would also add complexity and operational overhead compared to using an API Gateway.

upvoted 8 times

 **hobokabobo** 2 years, 10 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 2 times

 **hobokabobo** 2 years, 10 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 2 times

 **ninomfr64** Highly Voted  2 years ago

Selected Answer: A

I need help here: what's wrong with Lambda Function URL?

With A I just need to handle my Lambda functions, updates go through updating my aliases pointing to a new version. Here I am just missing all the capabilities provided by API Gateway that seems not to be requested (transformations, throttling, quotas, cache, api keys, auth, OpenAPI, ...). With B I still need to implement each webhook logic in a separate AWS Lambda function and update git server + I need to operate API Gateway.

Any other option requires 2 or more services thus generating more operations, also:
Not C as app runner is not a target for ALB (private IP, ECS, EC2 instance, Lambda)
Not D as you cannot set Fargate as API Gateway target (while you can use ECS as target)

Can you help me understand why B requires less operations overhead?

upvoted 6 times

✉ **Malcnorth59** 1 year, 7 months ago

Option A requires that you update the webhooks for each lambda function. This will create a considerable operational overhead not just for the initial change but going forward as well.

API Gateway (B) decouple the functions from the Webhooks.

upvoted 2 times

✉ **Chris_W_1234** 2 months, 2 weeks ago

I don't buy answer B. Changing the webhooks once is not operational overhead. It is development effort. Once the webhooks have been updated to point to the respective function URLs, they never need to be touched again.

upvoted 1 times

✉ **g1f** [Most Recent] 11 months, 2 weeks ago

Selected Answer: A

B is plain wrong. With an HTTP API Gateway you're publishing your API on the Internet, which could be forbidden by security policy. Even if it is not, you at least need to setup authentication, with OAuth2 or custom Lambda authorizer. And in this case, you lose the advantage in terms of operational overhead.

upvoted 1 times

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

Selected Answer: C

Deploy the web hook logic to the Apprunner which takes a minor effort to build and deploy the container image automatically without underlying infrastructure management.

upvoted 1 times

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

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.

upvoted 1 times

✉ **subupro** 1 year, 4 months ago

C is the best one . Operational over head - existing web logic needs to be change into the lambda. But in C - just we can use the same logic just deployment activities. Please go with C

upvoted 1 times

✉ **Malcnorth59** 1 year, 7 months ago

Selected Answer: B

A: large operational overhead

B: Choice

C: App runner doesn't use ALB

D: Unnecessary complexity with containers

upvoted 3 times

✉ **Fu7ed** 1 year, 7 months ago

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

upvoted 2 times

✉ **Fu7ed** 1 year, 7 months ago

choose B

upvoted 1 times

✉ **kz407** 1 year, 9 months ago

Selected Answer: B

Given the current answers, I think B is the only possible option with least overhead.

C would have been a better candidate over B, if it mentioned to include the App Runner in a Target Group TG and assign TG as the target for the API Gateway. As it stands now, C is not correct because App Runner app can't be directly assigned as a target for API Gateway.

upvoted 1 times

✉ **gofavad926** 1 year, 9 months ago

Selected Answer: A

A, because is the solution with less operational overhead. Also option B also will create new lambda functions per webhook, and you have to define the specific path in the apigateway and integrate it with your specific lambda...

upvoted 5 times

✉ **bjexamprep** 1 year, 9 months ago

Selected Answer: B

Lambda function is the easiest way to implement the webhook logic. App Runner and ECS all requires more ops overhead. So the answer is between A and B. Someone argue that using A introduces ops overhead of mapping every Lambda function to the webhooks, but actually with B, users don't need to map Lambda function in git webhooks, but move the Lambda function mapping ops to API gateway. The mapping need to be done, that's an ops overhead that cannot be ignored. I'm guessing the question designer prefers to use API GW, because the description "Update the Git servers to call the individual Lambda function URLs." doesn't look good. While, in reality, the repo developers create the Lambda function, and they know the URL, it's very easy to launch the Lambda function from the web hook. No additional API GW is required.

upvoted 1 times

 **master9** 1 year, 11 months ago

Selected Answer: C

You can set App Runner as a target for ALB.

AWS App Runner can use your code. You can use AWS App Runner to create and manage services based on two fundamentally different service sources: source code and source image. App Runner starts, runs, scales, and balances your service regardless of the source type. You can use the CI/CD capability of App Runner to track changes to your source image or code. When App Runner discovers a change, it automatically builds (for source code) and deploys the new version to your App Runner service

upvoted 1 times

 **djeong95** 1 year, 10 months ago

Looks like App Runner is built more for deploying web applications rather than hosting webhook logics.

upvoted 1 times

 **uas99** 1 year, 12 months ago

A. is the right answer as no need to introduce gateway here

upvoted 2 times

 **subupro** 2 years ago

Least operations is the key. App runner is a aws managed one and can deploy it easily, A and B we need to create lamda for each web hook it is very complex . So C would be correct

upvoted 1 times

 **jpa8300** 1 year, 12 months ago

ninomfr64 says that App runner cannot be a target for ALB, so that's the reason you cannot select C.

upvoted 2 times

 **severlight** 2 years, 1 month ago

Selected Answer: B

Don't see the exact reasons to not choose A for now, but B will work for sure.

upvoted 1 times

 **severlight** 2 years, 1 month ago

UPD: Don't see the exact reasons why A won't work for now, but B will work for sure.

upvoted 1 times

 **whenthan** 2 years, 2 months ago

Selected Answer: B

reducing operational overhead!

upvoted 1 times

 **Andy97229** 2 years, 2 months ago

Selected Answer: C

B vs C. Looking at App Runner C makes more sense.

upvoted 1 times

Question #46

A company is planning to migrate 1,000 on-premises servers to AWS. The servers run on several VMware clusters in the company's data center. As part of the migration plan, the company wants to gather server metrics such as CPU details, RAM usage, operating system information, and running processes. The company then wants to query and analyze the data.

Which solution will meet these requirements?

- A. Deploy and configure the AWS Agentless Discovery Connector virtual appliance on the on-premises hosts. Configure Data Exploration in AWS Migration Hub. Use AWS Glue to perform an ETL job against the data. Query the data by using Amazon S3 Select.
- B. Export only the VM performance information from the on-premises hosts. Directly import the required data into AWS Migration Hub. Update any missing information in Migration Hub. Query the data by using Amazon QuickSight.
- C. Create a script to automatically gather the server information from the on-premises hosts. Use the AWS CLI to run the put-resource-attributes command to store the detailed server data in AWS Migration Hub. Query the data directly in the Migration Hub console.
- D. Deploy the AWS Application Discovery Agent to each on-premises server. Configure Data Exploration in AWS Migration Hub. Use Amazon Athena to run predefined queries against the data in Amazon S3.

Correct Answer: D*Community vote distribution*

D (91%)	9%
---------	----

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: D

The correct answer is D: Deploy the AWS Application Discovery Agent to each on-premises server. Configure Data Exploration in AWS Migration Hub. Use Amazon Athena to run predefined queries against the data in Amazon S3.

Here is why the other choices are not correct:

A. Deploy and configure the AWS Agentless Discovery Connector virtual appliance on the on-premises hosts. Configure Data Exploration in AWS Migration Hub. Use AWS Glue to perform an ETL job against the data. Query the data by using Amazon S3 Select. - AWS Agentless Discovery Connector will help in discovering and inventory servers but it does not provide the same level of detailed metrics as the AWS Application Discovery Agent, it also does not cover process information.

upvoted 47 times

 **masetromain** 2 years, 11 months ago

B. Export only the VM performance information from the on-premises hosts. Directly import the required data into AWS Migration Hub. Update any missing information in Migration Hub. Query the data by using Amazon QuickSight. - It does not cover process information and it's not the best way to collect the required data, it's not efficient and it might miss some important information.

C. Create a script to automatically gather the server information from the on-premises hosts. Use the AWS CLI to run the put-resource-attributes command to store the detailed server data in AWS Migration Hub. Query the data directly in the Migration Hub console. - this solution might not be very reliable and it does not cover process information, also it does not provide a way to query and analyze the data.

upvoted 6 times

 **masetromain** 2 years, 11 months ago

D. Deploy the AWS Application Discovery Agent to each on-premises server. Configure Data Exploration in AWS Migration Hub. Use Amazon Athena to run predefined queries against the data in Amazon S3. - This is the correct answer as it covers all the requirements mentioned in the question, it will allow collecting the detailed metrics, including process information and it provides a way to query and analyze the data using Amazon Athena.

upvoted 5 times

 **icassp** Highly Voted 2 years, 11 months ago

Selected Answer: D

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

upvoted 6 times

 **oatif** 2 years, 10 months ago

I think A is a better solution because the Agentless discovery connector is custom-made for the VMware environment. It will save us time and collect all the necessary data we need. Installing a Discovery agent in every server would be very time-consuming. S3 select allows simple select operations against your raw data. I don't think we need athena for

upvoted 4 times

 **djeong95** 1 year, 10 months ago

As written by jainparag1, S3 Select is definitely the wrong solution here. As you said, it only allows for very simple select operations. Athena is a better way to go once you have configured the Migration hub settings correctly.

upvoted 1 times

 **jainparag1** 2 years, 1 month ago

A is horrible. You can write only simple SQLs using S3 select. But here you need a sophisticated solution to query these special metrics. D is satisfying all the requirements.

upvoted 3 times

 **Jorkaef** Most Recent 1 year, 1 month ago

A is correct

upvoted 1 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: D

If precise information about each running Process is required, it is necessary to consider using Agent-based Discovery.

upvoted 2 times

 **amministrazione** 1 year, 3 months ago

D. Deploy the AWS Application Discovery Agent to each on-premises server. Configure Data Exploration in AWS Migration Hub. Use Amazon Athena to run predefined queries against the data in Amazon S3.

upvoted 1 times

 **Jason666888** 1 year, 4 months ago

Selected Answer: D

D for sure

upvoted 1 times

 **vip2** 1 year, 7 months ago

Selected Answer: D

see <https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>

for VMs hosted on VMware, you can use both the Agentless Collector and Discovery Agent to perform discovery simultaneously.

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. Therefore, if you need this level of detail and want to take a closer look at some of your existing VMs in order to assist in planning your migration, you can install the Discovery Agent on an as-needed basis.

upvoted 3 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: D

D is correct

upvoted 1 times

 **whichonce** 1 year, 10 months ago

Selected Answer: A

Definitely A

<https://docs.aws.amazon.com/application-discovery/latest/userguide/agentless-collector-data-collected-vmware.html>

Vmware supports agentless connector with AWS, and data can be imported ove Migration Hub

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: D

Option D is the most efficient and streamlined solution for the requirements. Deploying the AWS Application Discovery Agent on each on-premises server allows for detailed collection of server metrics, including CPU usage, RAM usage, operating system details, and running processes. By configuring Data Exploration in AWS Migration Hub, the collected data can be analyzed and queried effectively. Using Amazon Athena for querying enables powerful SQL-based exploration of the data stored in Amazon S3, offering a flexible and scalable way to analyze the migration readiness and planning data.

It is not option C because, Option C involves creating a custom script to gather server information and using the AWS CLI to store data in AWS Migration Hub. While this approach could potentially work, it requires significant manual effort to develop, deploy, and maintain the scripts across 1,000 servers, which is not ideal for minimizing operational overhead.

upvoted 1 times

 **ninomfr64** 2 years ago

Selected Answer: D

Not A - as AWS Agentless Discovery Connector does not provide processes visibility

Not B - as Migration Hub Import functionality does not support process data <https://docs.aws.amazon.com/cli/latest/reference/mgh/put-resource-attributes.html>, also I do not see how to query with QuickSight as there is not direct integration with Migration Hub to my knowledge

Not C - as it seems that put-resource-attributes command does not support process data

<https://docs.aws.amazon.com/cli/latest/reference/mgh/put-resource-attributes.html>

D is correct as Discovery Agent collects the required data including processes, Data Exploration in Migration Hub allows to use Amazon

Athena and comes with pre-defined queries as well. <https://docs.aws.amazon.com/application-discovery/latest/userguide/explore-data.html>

upvoted 1 times

 **edder** 2 years, 1 month ago

Selected Answer: D

<https://docs.aws.amazon.com/application-discovery/latest/userguide/explore-data.html>

upvoted 1 times

 **punkbuster** 2 years, 4 months ago

Selected Answer: D

The agent-based collector can collect data related to running processes which is not available to the Agentless Collector.

Check out for yourself in the FAQs:

<https://aws.amazon.com/application-discovery/faqs/>

upvoted 1 times

 **xplusfb** 2 years, 4 months ago

Selected Answer: A

As far as i learned for VM based envs we can go with agentless. And we can use a OVA image via collect the metrics and so on. im going with A . <https://docs.aws.amazon.com/application-discovery/latest/userguide/agentless-data-collected.html>

upvoted 2 times

 **chico2023** 2 years, 4 months 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** 2 years, 4 months 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** 2 years, 4 months ago

Selected Answer: D

I prefer D

upvoted 1 times

 **ggrodskiy** 2 years, 4 months 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

Question #47

Topic 1

A company is building a serverless application that runs on an AWS Lambda function that is attached to a VPC. The company needs to integrate the application with a new service from an external provider. The external provider supports only requests that come from public IPv4 addresses that are in an allow list.

The company must provide a single public IP address to the external provider before the application can start using the new service.

Which solution will give the application the ability to access the new service?

- A. Deploy a NAT gateway. Associate an Elastic IP address with the NAT gateway. Configure the VPC to use the NAT gateway.
- B. Deploy an egress-only internet gateway. Associate an Elastic IP address with the egress-only internet gateway. Configure the elastic network interface on the Lambda function to use the egress-only internet gateway.
- C. Deploy an internet gateway. Associate an Elastic IP address with the internet gateway. Configure the Lambda function to use the internet gateway.
- D. Deploy an internet gateway. Associate an Elastic IP address with the internet gateway. Configure the default route in the public VPC route table to use the internet gateway.

Correct Answer: A

Community vote distribution

A (93%)	6%
---------	----

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: A

A. Deploy a NAT gateway. Associate an Elastic IP address with the NAT gateway. Configure the VPC to use the NAT gateway.

This solution will give the Lambda function access to the internet by routing its outbound traffic through the NAT gateway, which has a public Elastic IP address. This will allow the external provider to whitelist the single public IP address associated with the NAT gateway, and enable the application to access the new service.

upvoted 32 times

 **Jacky_exam** 2 years, 8 months ago

Options A are not appropriate solutions because they involve deploying a NAT gateway or an egress-only internet gateway, which are used for different purposes, such as allowing resources in a private subnet to access the internet while using a static public IP address. These options will not provide the Lambda function with a single public IP address to be used for external requests.

upvoted 5 times

 **ninomfr64** 1 year, 12 months ago

The question includes "The external provider supports only requests that come from public IPv4 addresses that are in an allow list" this imply the Lambda needs to call the external provider

upvoted 1 times

 **JMAN1** 2 years ago

Big Thank to you. masetromain.

upvoted 2 times

 **vvahe** Highly Voted 2 years, 9 months 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 9 times

 **toyaji** Most Recent 1 year, 2 months ago

Selected Answer: A

There are many misleading explanations here.

You cannot attach ElasticIP to Internet Gateway which uses instance public IP for NAT. -

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-igw-internet-access.html#ip-addresses-and-nat>

But NAT can be used with Elastic IP for fixed outbound IP. That's the difference. -

https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/nat-gateway-scenarios.html#private-nat-allowed-range

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. Deploy a NAT gateway. Associate an Elastic IP address with the NAT gateway. Configure the VPC to use the NAT gateway.
upvoted 1 times

 **subupro** 1 year, 4 months ago

A is correct, NAT not only provides the internet outbound , but also provides single public IP address, So Selected Answer: A
upvoted 1 times

 **Jason666888** 1 year, 4 months ago

THE ANSWER HAS TO BE A!!!!

For B:

Wrong. Egress only internet gateway is for IPV6, not for IPV4

For C&D:

Internet gateway is for both inbound and outbound traffic. In our case we only need outbound traffic, so it has to be NAT Gateway.
upvoted 4 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: D

NAT gateway doesn't allow inbound traffic flow into service behind NAT gateway. ALB or internet gateway can. However internet gateway can't be attached to lambda service directly. I vote D as correct answer.

upvoted 2 times

 **kz407** 1 year, 9 months ago

Selected Answer: A

Option A will be the only solution that matches the given requirements.

The problem with any solution that involves IGw is that IGw DOES NOT perform NAT. In fact, it does not alter the source IP field at all, meaning that we don't really have a mechanism of having a static public IP address set to the outbound traffic, while ensuring security. So, the only practical solution is to go with the NAT option.

upvoted 3 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A, deploy nat gateway and associate an elastic ip

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Can an admin please take a look at _all_ the "correct answers" in this exam? They really cannot be trusted and reduce the usefulness of ExamTopics altogether. As things are, you should always just disregard the correct answer as it so often is insane.

The correct answer is of course A.

upvoted 3 times

 **Vsos_in29** 1 year, 10 months ago

A is correct option, Other approach to enable internet access

<https://www.linkedin.com/pulse/aws-lambda-accessing-private-vpc-resources-internet-without-vokhmin-pyxbe/>

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: A

The solution that enables the Lambda function in a VPC to access an external service that requires requests to come from a specific public IPv4 address, and to provide a single public IP address for allow listing, is:

* Option A is correct because a NAT (Network Address Translation) gateway allows instances or AWS Lambda functions in a private subnet of a VPC to initiate outbound traffic to the internet (or external services) while preventing unsolicited inbound traffic from the internet. By associating an Elastic IP address with the NAT gateway, all outbound traffic from the Lambda function routed through the NAT gateway will appear to come from this single public IP address, which can be provided to the external provider for allow listing.

upvoted 2 times

 **8608f25** 1 year, 10 months ago

It is not option C because, Option C describes deploying an internet gateway and associating an Elastic IP address with it. However, Lambda functions cannot be directly associated with Elastic IP addresses, and internet gateways are used to route traffic between a VPC and the internet, not to provide a static public IP address for outbound traffic.

upvoted 3 times

 **ninomfr64** 1 year, 12 months ago

Selected Answer: A

Not B. egress-only internet gateway is IPv6 only, the question is about IPv6

Not C. you cannot associate Elastic IP to IGW also Lambda deployed in VPC cannot egress to internet via IGW, you need a NAT Gateway / NAT Instance

Not D. same as C.

A is the right solution (even if it is not well explained in my opinion)

upvoted 1 times

 **cgsoft** 2 years ago

Selected Answer: A

As per <https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html>, "To access private resources, connect your function to private subnets. If your function needs internet access, use network address translation (NAT). Connecting a function to a public subnet doesn't give it internet access or a public IP address."

upvoted 1 times

 **enk** 2 years, 1 month ago

Selected Answer: A

Just to clarify...If the Lambda function is already attached to a VPC, it's implied that it's in a private subnet since Lambda functions can't be directly placed in public subnets. So C and D are out.

upvoted 2 times

 **Pupu86** 2 years, 1 month ago

Selected Answer: A

Option B is definitely out as egress-only internet gateway is applicable solely for IPv6 traffic.

upvoted 2 times

 **whenthan** 2 years, 2 months ago

Selected Answer: A

internet gateway - cant assign elastic IP to internet gateway

upvoted 1 times

Question #48

Topic 1

A solutions architect has developed a web application that uses an Amazon API Gateway Regional endpoint and an AWS Lambda function. The consumers of the web application are all close to the AWS Region where the application will be deployed. The Lambda function only queries an Amazon Aurora MySQL database. The solutions architect has configured the database to have three read replicas.

During testing, the application does not meet performance requirements. Under high load, the application opens a large number of database connections. The solutions architect must improve the application's performance.

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

- A. Use the cluster endpoint of the Aurora database.
- B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.
- C. Use the Lambda Provisioned Concurrency feature.
- D. Move the code for opening the database connection in the Lambda function outside of the event handler.
- E. Change the API Gateway endpoint to an edge-optimized endpoint.

Correct Answer: BD

Community vote distribution

BD (99%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: BD

The correct answer is B and D.

B. Using RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database can help improve the performance of the application by reducing the number of connections opened to the database. RDS Proxy manages the connection pool and routes incoming connections to the available read replicas, which can help with connection management and reduce the number of connections that need to be opened and closed.

D. Moving the code for opening the database connection in the Lambda function outside of the event handler can help to improve the performance of the application by allowing the database connection to be reused across multiple requests. This avoids the need to open and close a new connection for each request, which can be time-consuming and resource-intensive.

upvoted 48 times

 **masetromain** 2 years, 11 months ago

A. Using the cluster endpoint of the Aurora database instead of the reader endpoint would not help improve performance in this case, because the solution architect is already using read replicas to offload read traffic from the primary instance.

C. Using the Lambda Provisioned Concurrency feature would not help improve performance in this case, as the problem is related to the number of connections to the database, not the number of instances running the Lambda function.

E. Changing the API Gateway endpoint to an edge-optimized endpoint would not help improve performance in this case, as the problem is related to the number of connections to the database, not the location of the API Gateway endpoint.

upvoted 14 times

 **mnsait** 1 year, 1 month ago

This phrase helped me understand why A is not correct "the solution architect is already using read replicas to offload read traffic from the primary instance". Thank you @masetromain for the explanation.

upvoted 1 times

 **b0969fd** Most Recent 2 months, 1 week ago

Selected Answer: BD

Based on experience, and a very costly one at that. RDS Proxy is built to handle RDS database connections when used by Lambda function.

Lambda Provisioned Concurrency solves a different problem. It keeps your lambda prewarm and reduce cold starts

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.

D. Move the code for opening the database connection in the Lambda function outside of the event handler.

upvoted 1 times

 **Malcnorth59** 1 year, 7 months ago

Selected Answer: BD

The issue is with the number of database connections, there are the only two changes that would impact the number of concurrent DB connections.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: BD

B and D

upvoted 1 times

 **totten** 2 years, 2 months ago

Selected Answer: BD

B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.

RDS Proxy helps manage and efficiently pool database connections, reducing the number of database connections required by the application. It helps improve performance and reduces the load on the database.

D. Move the code for opening the database connection in the Lambda function outside of the event handler.

By reusing database connections, you can reduce the overhead of opening and closing connections for each Lambda invocation. You can use the Lambda execution context to keep the database connection open and reuse it across multiple requests within the same execution context.

upvoted 3 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: BD

BD for sure

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: BD

RDS proxy + Lambda function

upvoted 4 times

 **dev112233xx** 2 years, 9 months ago

Selected Answer: BD

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

upvoted 3 times

 **kiran15789** 2 years, 9 months ago

Selected Answer: BD

the Lambda function only queries an Amazon Aurora MySQL database- so i would reject option C

upvoted 2 times

 **God_Is_Love** 2 years, 10 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 3 times

 **moota** 2 years, 10 months 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** 2 years, 10 months ago

BD

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

upvoted 4 times

 **masssa** 2 years, 11 months ago

B/C

lambda provisioned concurrency and RDS proxy are mentioned in same page.

<https://quintagroup.com/blog/aws-lambda-provisioned-concurrency>

upvoted 1 times

 **Untamables** 2 years, 11 months ago

Selected Answer: BC

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.howitworks.html>

<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html>

upvoted 1 times

 **jhonivy** 2 years, 11 months ago

B/C

Provisioned Concurrency needed: https://www.reddit.com/r/aws/comments/gcwtqt/lambda_provisioned_concurrency_with_aurora/

With connection Pool, no to worry D

upvoted 1 times

Question #49

A company is planning to host a web application on AWS and wants to load balance the traffic across a group of Amazon EC2 instances. One of the security requirements is to enable end-to-end encryption in transit between the client and the web server.

Which solution will meet this requirement?

- A. Place the EC2 instances behind an Application Load Balancer (ALB). Provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB. Export the SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances.
- B. Associate the EC2 instances with a target group. Provision an SSL certificate using AWS Certificate Manager (ACM). Create an Amazon CloudFront distribution and configure it to use the SSL certificate. Set CloudFront to use the target group as the origin server.
- C. Place the EC2 instances behind an Application Load Balancer (ALB). Provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB. Provision a third-party SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances.
- D. Place the EC2 instances behind a Network Load Balancer (NLB). Provision a third-party SSL certificate and install it on the NLB and on each EC2 instance. Configure the NLB to listen on port 443 and to forward traffic to port 443 on the instances.

Correct Answer: C*Community vote distribution*

C (50%)	D (41%)	8%
---------	---------	----

 **pitakk** Highly Voted 2 years, 11 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 51 times

 **_Jassybang_** 1 year, 10 months ago

in C , the encryption will terminate at ALB so its not an end-2-end encryption , for e2e end encryption need NLB
upvoted 3 times

 **hobokabobo** 2 years, 10 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

 **bjexamprep** 1 year, 8 months ago

that means you are decrypting the data on ALB and encrypt it again to send it to EC2. Does that sound E2E?
upvoted 5 times

 **Untamables** Highly Voted 2 years, 11 months ago

Selected Answer: D

Vote D.

If you need to pass encrypted traffic to targets without the load balancer decrypting it, you can create a Network Load Balancer or Classic Load Balancer with a TCP listener on port 443.
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>
upvoted 42 times

 **hobokabobo** 2 years, 10 months ago

coorect. but they want to upload the the certificate to the NLB for unknown reasons.
upvoted 7 times

 **Arnaud92** 2 years, 9 months ago

You can use NLB with ACM cert on it. NLB can do TLS termination (<https://aws.amazon.com/blogs/aws/new-tls-termination-for-network-load-balancers/>) and re-encrypt to target
upvoted 2 times

 **Ikyixoayffasdrlaqd** 2 years, 10 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 12 times

 **eesa** Most Recent 8 months, 1 week ago

Selected Answer: C

Why option C is correct:

End-to-end encryption implies traffic is encrypted both from the client to the load balancer and from the load balancer to the EC2 instances.

Application Load Balancers (ALBs) support HTTPS termination at the ALB level using AWS Certificate Manager (ACM) certificates.

To encrypt traffic between the ALB and EC2 instances, you must install a separate SSL/TLS certificate directly onto each EC2 instance.

AWS Certificate Manager (ACM) certificates cannot be exported or installed directly on EC2 instances; thus, a third-party SSL certificate (such as from Let's Encrypt or a commercial provider) must be used on the EC2 instances themselves.

upvoted 3 times

 **Trap_D0_r** 10 months ago

Selected Answer: C

Please read the question carefully: "end-to-end encryption IN TRANSIT"--There is no requirement for TLS termination at the NLB, and uploading the certificate to the NLB would effectively negate this anyway (I think it's thrown in there specifically to show this is the wrong answer). While it's worded poorly, the only good answer is C, which will decrypt and reencrypt traffic at the ALB only, but all traffic traversing the network will be encrypted while IN TRANSIT.

upvoted 1 times

 **uffd** 10 months, 1 week ago

Selected Answer: D

A is not correct because as pitakk mentioned, Amazon-issued public certificates from AWS Certificate Manager (ACM) cannot be directly installed on an EC2 instance. It requires 3rd party certificates.

B doesn't make any sense.

C is not correct because ALB decrypts the traffic before sending it to the target EC2 instances.

D is correct because NLB has TCP pass through. With this, NLB doesn't have to decrypt the traffic before forwarding it to the target instances.

Courtesy to Perplexity & DeepSeek.

upvoted 1 times

 **attila9778** 1 year ago

Selected Answer: C

<https://docs.aws.amazon.com/acm/latest/userguide/acm-services.html>

AWS Certificate Manager (ACM) certificates cannot be directly installed on Amazon EC2 instances, except for those connected to a Nitro Enclave. Therefore my choice is also C.

upvoted 1 times

 **Heman31in** 1 year ago

from your link : You cannot associate ACM certificates with an EC2 instance that is not connected to a Nitro Enclave. this is for Nitro case . Also : ACM is integrated with Elastic Load Balancing to deploy ACM certificates on the load balancer. For more information, so Answer is A .

upvoted 1 times

 **sergza** 1 year ago

Selected Answer: D

According to: <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html> 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. With a TCP listener, the load balancer passes encrypted traffic through to the targets without decrypting it.

upvoted 3 times

 **henrikhmkhitaryan59** 1 year, 1 month ago

Selected Answer: D

end-to-end encryption

upvoted 3 times

 **AWSum1** 1 year, 3 months ago

Selected Answer: D

I'm leaning closer to D because, NLB supports e2e. I feel that if the question asked about offloading then the ALB options may have been better. But here it's asking for e2e and can only be done with an NLB

upvoted 3 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **toma** 1 year, 5 months ago

it is D, C is more complex.

upvoted 1 times

 **higashikumi** 1 year, 7 months ago

Selected Answer: C

To achieve end-to-end encryption for a web application using AWS, place the EC2 instances behind an Application Load Balancer (ALB). Provision an SSL certificate using AWS Certificate Manager (ACM) and associate it with the ALB to handle HTTPS traffic from clients to the ALB. Additionally, install a third-party SSL certificate on each EC2 instance to ensure that traffic between the ALB and the instances is also encrypted. Configure the ALB to listen on port 443 and forward traffic to port 443 on the instances. This setup ensures that all data in transit is encrypted from the client through the ALB to the backend EC2 instances, meeting security requirements for end-to-end encryption while leveraging ACM for simplified certificate management [OBJ] [OBJ] [OBJ].

upvoted 1 times

 **Malcnorth59** 1 year, 7 months ago

Selected Answer: D

The key here is end-to-end, so that rules out ALB. Instead Use NLB with TLS termination which will pass the traffic on encrypted.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html#:~:text=The%20load%20balancer%20passes%20the,combination%20of%20protocols%20and%20ciphers>.

upvoted 2 times

 **titi_r** 1 year, 7 months ago

Selected Answer: D

"To enable END-TO-END encryption, you must procure an SSL certificate from a third-party vendor. You can then install the certificate on the EC2 instance and also associate the SAME certificate with the (network) Load Balancer by importing it into Amazon Certificate Manager."

<https://www.youtube.com/watch?v=6Nz0RFfBqVE&t=44s>

TLS listeners for your Network Load Balancer

"... if you need to pass encrypted traffic to the targets without the (network) load balancer decrypting it, create a TCP listener on port 443 instead of creating a TLS listener."

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

P.S. The answer is misleading because it says to install the certificate on the NLB; read it as "import it to ACM and associate it with the NLB.

upvoted 3 times

 **vip2** 1 year, 7 months ago

Selected Answer: C

C is correct because

ALB+Self-signed Certification

NLB+Public Certification

upvoted 1 times

 **EmmanuelPR** 1 year, 9 months ago

Selected Answer: A. Public Certificates: You can request Amazon-issued public certificates from ACM. ACM manages the renewal and deployment of public certificates that are used with ACM-integrated services, including Amazon CloudFront, Elastic Load Balancing, and Amazon API Gateway. <https://aws.amazon.com/es/certificate-manager/faqs/>

upvoted 2 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C

C: use ACM in the ALB and third-party SSL certificate in the EC2 instances

upvoted 2 times

Question #50

Topic 1

A company wants to migrate its data analytics environment from on premises to AWS. The environment consists of two simple Node.js applications. One of the applications collects sensor data and loads it into a MySQL database. The other application aggregates the data into reports. When the aggregation jobs run, some of the load jobs fail to run correctly.

The company must resolve the data loading issue. The company also needs the migration to occur without interruptions or changes for the company's customers.

What should a solutions architect do to meet these requirements?

- A. Set up an Amazon Aurora MySQL database as a replication target for the on-premises database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind a Network Load Balancer (NLB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the NLB.
- B. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Move the aggregation jobs to run against the Aurora MySQL database. Set up collection endpoints behind an Application Load Balancer (ALB) as Amazon EC2 instances in an Auto Scaling group. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- C. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer (ALB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- D. Set up an Amazon Aurora MySQL database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as an Amazon Kinesis data stream. Use Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the Kinesis data stream.

Correct Answer: C

Community vote distribution

C (96%)	4%
---------	----

 **OCHT**  2 years, 8 months 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 20 times

 **amministrazione**  1 year, 3 months ago

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.

upvoted 1 times

 **ninomfr64** 1 year, 12 months ago

Selected Answer: C

Not A. not clear how the on-premises database is replicated on the Aurora MySQL, also you cannot place Lambda behind NLB as NLB only supports private IPs, instances and ALB <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html>

Not B. this will keep executing the aggregation job and the load on the same database instance and this will not resolve loading issues

Not D. using Kinesis Data Firehose to replicate the database is not recommended, the solution should involve DMS. also moving to Kinesis

Data Stream for data load requires some changes on the customer side which is not part of the request.

C is the right solution: use DMS to migrate on-premise database, move the aggregation job to the read replica, using Lambda (that supports node.js) behind ALB will not impact client side

upvoted 3 times

shaaam80 2 years ago

Selected Answer: C

Answer C

upvoted 1 times

NikkyDicky 2 years, 5 months ago

Selected Answer: C

It's a c

upvoted 1 times

SkyZeroZx 2 years, 6 months ago

Selected Answer: C

Keywords = DMS & RDS Proxy

Then C

upvoted 2 times

leehjworking 2 years, 7 months ago

Selected Answer: C

AD: restart = interruption?

B: ASG...Why?

upvoted 3 times

chikorita 2 years, 7 months ago

why ...oh...why?

upvoted 1 times

mfsec 2 years, 9 months ago

Selected Answer: C

ill go with C

upvoted 1 times

dev112233xx 2 years, 9 months ago

Selected Answer: C

C.. even though question didn't mention the total time of each job. If the job takes more than 15m then Lambda can't be used. Probably the solution with ASG and EC2 is better .. not sure!

upvoted 3 times

zejou1 2 years, 9 months 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 2 years, 9 months ago

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

upvoted 1 times

zejou1 2 years, 9 months 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 2 years, 10 months ago

Selected Answer: C

I would say C.

upvoted 1 times

hobokabobo 2 years, 10 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 if the approaches addresses that aggregation tasks fail because of inconsistency of the data base.

upvoted 1 times

✉ hobokabobo 2 years, 10 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 2 years, 10 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 onpremises.Writing app to DB and Reading app from DB for reports.
Writing app needs RDSProxy and saves data.Reading app reads from replica.
B is wrong because, Reading job (aggregation) needs to use replica which is mentioned in C. C is correct.

upvoted 2 times

✉ Fatoch 2 years, 10 months ago

is it C or B?

Same person answers two times two different answers

upvoted 1 times

✉ zozza2023 2 years, 11 months ago

Selected Answer: C

C is corect

upvoted 3 times

✉ masetromain 2 years, 11 months ago

Selected Answer: C

C.

This option would meet the requirements of resolving the data loading issue and migrating without interruption or changes for the company's customers. By using AWS DMS for continuous data replication, the company can ensure that the data being migrated is up to date. By setting up an Aurora Replica and moving the aggregation jobs to run against it, the company can offload some of the read workload from the primary database and reduce the risk of issues with the load jobs. By using AWS Lambda functions behind an ALB and Amazon RDS Proxy to write to the Aurora MySQL database, the company can add an extra layer of security and scalability to the data collection process. Finally, by pointing the collector DNS record to the ALB after the databases are synced and disabling the AWS DMS sync task, the company can ensure a smooth cutover to the new environment.

upvoted 4 times

✉ masetromain 2 years, 11 months ago

A.

This option would not work as it would require to change the primary database and also it may cause interruption for the company's customers during the cutover process.

B.

This option would not work as it would not include Aurora Replica to offload the read workload, this would result in aggregation jobs running on the primary database which can cause the load jobs to fail during heavy loads.

D.

This option would not work as it would require to use kinesis data stream which may cause performance issues and also it may not be the best fit for this use case. Additionally, using Kinesis Data Firehose would add complexity to the data replication process, and may result in increased latency or data loss.

upvoted 2 times

Question #51

A health insurance company stores personally identifiable information (PII) in an Amazon S3 bucket. The company uses server-side encryption with S3 managed encryption keys (SSE-S3) to encrypt the objects. According to a new requirement, all current and future objects in the S3 bucket must be encrypted by keys that the company's security team manages. The S3 bucket does not have versioning enabled.

Which solution will meet these requirements?

- A. In the S3 bucket properties, change the default encryption to SSE-S3 with a customer managed key. Use the AWS CLI to re-upload all objects in the S3 bucket. Set an S3 bucket policy to deny unencrypted PutObject requests.
- B. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to deny unencrypted PutObject requests. Use the AWS CLI to re-upload all objects in the S3 bucket.**
- C. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to automatically encrypt objects on GetObject and PutObject requests.
- D. In the S3 bucket properties, change the default encryption to AES-256 with a customer managed key. Attach a policy to deny unencrypted PutObject requests to any entities that access the S3 bucket. Use the AWS CLI to re-upload all objects in the S3 bucket.

Correct Answer: B*Community vote distribution*

B (62%)

D (36%)

 **masetromain** Highly Voted  2 years, 11 months ago

Selected Answer: B

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

So the correct answer is B. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to deny unencrypted PutObject requests. Use the AWS CLI to re-upload all objects in the S3 bucket.

upvoted 44 times

 **hamimelon** 2 years, 3 months 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 5 times

 **hogtrough** 1 year, 10 months ago

This is why they would use Customer-managed keys in AWS KMS. It is absolutely B

upvoted 5 times

 **jpa8300** 1 year, 12 months ago

Hamimmelon, the Company's security Team can manage the AWS KMS service, so B is the right answer. All the others are not valid.

upvoted 3 times

 **hobokabobo** 2 years, 10 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** 2 years, 9 months 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** 2 years, 8 months ago

Task is to replace any AWS Managed keys to ones "that the company's security team manages"

So they tell us to find a solution that does not use AWS Managed Keys.

upvoted 4 times

 **hogtrough** 1 year, 10 months ago

No, the task was to replace SSE-SE keys which have no relation to AWS KMS.

"Amazon S3 automatically enables server-side encryption with Amazon S3 managed keys (SSE-S3) for new object uploads.

Unless you specify otherwise, buckets use SSE-S3 by default to encrypt objects. However, you can choose to configure buckets to use server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS) instead. "

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

upvoted 1 times

 **Musk** 2 years, 11 months ago

What about the requirement of customer managed keys?

upvoted 10 times

 **masetromain** 2 years, 11 months ago

Option A is not correct because it uses SSE-S3 with a customer-managed key, but it does not specify how the security team will manage the encryption keys. Additionally, it only denies unencrypted PutObject requests but does not specify how the objects will be encrypted.

Option C is not correct because it does not specify how the security team will manage the encryption keys and it does not specify how the objects will be encrypted.

Option D is not correct because it uses AES-256 with a customer-managed key, but it does not specify how the security team will manage the encryption keys. Additionally, it simply denies unencrypted PutObject requests, but it doesn't specify how the objects will be encrypted.

upvoted 8 times

 **jpa8300** 1 year, 12 months ago

And adding to this in option D they specify uses default AES-256, but KMS also uses the same, so this option just don't make sense.

upvoted 1 times

 **Untamables** Highly Voted  2 years, 11 months ago

Selected Answer: D

I think D is correct.

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

upvoted 21 times

 **djeong95** 1 year, 10 months ago

The issue with D is that it doesn't make it clear where the encryption is happening like all the other options do. Is it server-side (we assume that it is, but it is not what is written)? Or is it client-side?

upvoted 1 times

 **evargasbrz** Most Recent  3 weeks ago

Selected Answer: B

You can enforce encryption on PutObject but not on GetObject. Objects are automatically decrypted on retrieval if you have KMS permissions.

upvoted 1 times

 **vcc300625** 5 months, 4 weeks ago

Selected Answer: B

Answer A uses SSE-S3 (still an AWS managed key, which does not meet the requirements).

Answer C is incorrect because there is no bucket policy that automatically encrypts when GetObject is used.

Answer D is confused about terminology (AES-256 is the algorithm, not the customer managed key).

upvoted 1 times

 **Curious76** 7 months, 1 week ago

Selected Answer: A

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.

Here's why:

Requirements Recap:

All current and future objects must be encrypted using customer-managed keys.

The current encryption is SSE-S3, which uses S3-managed keys, not customer-managed keys.

The bucket does not have versioning enabled, so overwriting (re-uploading) is necessary to change encryption on existing objects.

upvoted 1 times

 **amministrazione** 1 year, 3 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.

upvoted 1 times

 **Jason666888** 1 year, 4 months ago

Selected Answer: B

AWS KMS (Key Management Service) allows for customer-managed keys (CMKs), which can indeed be considered as "keys that the company's security team manages"

upvoted 1 times

 **Helpnose** 1 year, 6 months ago

Selected Answer: B

In S3 option there is no option to select AES256 custom key.

upvoted 1 times

 **higashikumi** 1 year, 7 months ago

Selected Answer: B

To meet the requirement for encrypting all current and future objects in an Amazon S3 bucket with keys managed by the company's security team, change the S3 bucket's default encryption to server-side encryption with AWS KMS managed keys (SSE-KMS). Implement an S3 bucket policy to deny unencrypted PutObject requests, ensuring all new uploads are encrypted with the specified KMS key. Then, use the AWS CLI to re-upload all existing objects to the S3 bucket, enforcing the new encryption policy on current data. This approach ensures compliance by applying KMS encryption to both new and existing objects without causing disruptions   .

upvoted 1 times

 **Malcnorth59** 1 year, 7 months ago

Selected Answer: B

The solutions need to use SSE-KMS so that the security team can manage the keys, but they also need to ensure that current and future objects are encrypted using customer-managed keys.

upvoted 1 times

 **TonytheTiger** 1 year, 7 months ago

Selected Answer: D

Not Option D: "Amazon S3 server-side encryption uses 256-bit Advanced Encryption Standard Galois/Counter Mode (AES-GCM) to encrypt all uploaded objects." AES-256 is already the default, so you can't change it.

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

upvoted 1 times

 **mav3r1ck** 1 year, 9 months ago

Selected Answer: B

Correct Approach: This option is accurate and meets all the specified requirements. By changing the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS), the company can use customer managed keys (CMKs) for encryption. This allows the security team to manage the keys, addressing the core requirement.

Setting an S3 bucket policy to deny unencrypted PutObject requests ensures future compliance with the encryption policy.

Re-uploading all objects using the AWS CLI ensures that existing objects are encrypted under the new policy, making sure that both current and future objects are encrypted with the keys managed by the company's security team.

upvoted 2 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: B

B, option D confuses encryption options. AES-256 is part of the SSE-S3 encryption method and doesn't directly involve customer-managed keys

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: B

The solution that meets the requirements for encrypting all current and future objects in the Amazon S3 bucket with keys that the company's security team manages, while ensuring server-side encryption, is:

Option B is correct because it directly addresses the new requirement by changing the default encryption method to SSE-KMS, which allows the use of AWS Key Management Service (KMS) keys managed by the company's security team. This option ensures that all future uploads are encrypted with the specified KMS key. It also includes re-uploading existing objects to ensure they are encrypted under the new scheme. Setting an S3 bucket policy to deny unencrypted PutObject requests enforces the encryption requirement for all new uploads.

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Option D is incorrect because it refers to "AES-256 with a customer managed key" in a way that mixes concepts. AES-256 is the encryption standard used by SSE-S3 and does not directly apply to the use of customer managed keys. For managing keys, the correct approach is through SSE-KMS, which allows specifying a customer managed AWS KMS key.

upvoted 1 times

 **ninomfr64** 1 year, 12 months ago

Selected Answer: B

Not A. SSE-S3 with a customer managed key is not an actual option as SSE-S3 uses S3 managed keys

Not C. S3 bucket policy cannot automatically encrypt objects on GetObject and PutObject requests. With policies you can only allow/deny actions from specific principals

Not D. AES-256 with a customer managed key is not an actual option as AES-256 is used as value for the header x-amz-server-side-encryption to set SSE-S3 on putObject and SSE-S3 uses S3 managed keys

B is correct as server-side encryption with AWS KMS managed encryption keys (SSE-KMS) is an actual default encryption settings for S3 bucket and you can use S3 bucket policy to deny unencrypted PutObject. These ensure all new objects will be encrypted with customer managed keys. Then using aws cli to re-upload all object will overwrite existing objects (versioning is not enabled)

upvoted 2 times

 **ismeagain** 2 years ago

Selected Answer: D

i think D is correct as B is mentioned KMS managed key..

upvoted 1 times

 **Impromtu** 2 years ago

Selected Answer: B

A - You cannot define your own key

B - Correct. Using SSE-KMS and your own KMS customer managed key, you adhere to the requirements

C - Does not encrypt existing objects, and you cannot "change" the request to "automatically" encrypt

D - You can only choose between SSE-S3 and SSE-KMS (or now DSSE-KMS as well) for default encryption. Underlying the SSE-S3 refers to AES-256 (cfr. "s3:x-amz-server-side-encryption": "AES256") but you cannot specify your customer managed key in that case.

upvoted 1 times

Question #52

A company is running a web application in the AWS Cloud. The application consists of dynamic content that is created on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group that is configured as a target group for an Application Load Balancer (ALB).

The company is using an Amazon CloudFront distribution to distribute the application globally. The CloudFront distribution uses the ALB as an origin. The company uses Amazon Route 53 for DNS and has created an A record of www.example.com for the CloudFront distribution.

A solutions architect must configure the application so that it is highly available and fault tolerant.

Which solution meets these requirements?

- A. Provision a full, secondary application deployment in a different AWS Region. Update the Route 53 A record to be a failover record. Add both of the CloudFront distributions as values. Create Route 53 health checks.
- B. Provision an ALB, an Auto Scaling group, and EC2 instances in a different AWS Region. Update the CloudFront distribution, and create a second origin for the new ALB. Create an origin group for the two origins. Configure one origin as primary and one origin as secondary.
- C. Provision an Auto Scaling group and EC2 instances in a different AWS Region. Create a second target for the new Auto Scaling group in the ALB. Set up the failover routing algorithm on the ALB.
- D. Provision a full, secondary application deployment in a different AWS Region. Create a second CloudFront distribution, and add the new application setup as an origin. Create an AWS Global Accelerator accelerator. Add both of the CloudFront distributions as endpoints.

Correct Answer: B

Community vote distribution

B (98%)

 **masetromain**  2 years, 11 months ago

Selected Answer: B

The correct answer is B. Provisioning an ALB, an Auto Scaling group, and EC2 instances in a different AWS region provides redundancy and failover capability for the application. By creating a second origin for the new ALB in the second region, the CloudFront distribution can automatically route traffic to the healthy origin in case of an issue with the primary origin. This ensures that the application remains highly available and fault-tolerant.

Option A is not correct because it uses Route 53 failover records, which can result in increased latency and DNS resolution time for clients. Option C is not correct because it doesn't provide redundancy for the load balancer, which is a critical component of the application. Option D is not correct because it does not provide redundancy for the application in case of an issue with the primary origin in the first region.

upvoted 28 times

 **God_Is_Love**  2 years, 10 months ago

For HA, always use second region but it's 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 region 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 11 times

 **amministrazione**  1 year, 3 months ago

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.

upvoted 1 times

 **8693a49** 1 year, 5 months ago

Selected Answer: A

This architecture is an active-active DR strategy. You would do it with R53 failover because R53 has healthchecks, and once the primary is down all requests go to the failover. With CloudFront failover, all requests would continue to hit the failed primary before being routed to the failover distribution, which increases latency and possibly compounds problems in the failed stack. Interestingly, the best solution would actually be a combination between A and B, as this blog post shows:

<https://aws.amazon.com/blogs/networking-and-content-delivery/improve-web-application-availability-with-cloudfront-and-route53-hybrid-origin-failover/>

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: B

- A is wrong because CloudFront distros can't be added to Route 53.
B is correct
C is wrong because ALBs are single region and don't do failover.
D would work, but is overengineered in this context.

upvoted 2 times

 **8693a49** 1 year, 5 months ago

You can add CloudFront distros to R53 using alias records: <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html>

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: B

Option B is correct because it involves creating a redundant setup in another AWS Region with its own ALB, Auto Scaling group, and EC2 instances. By updating the CloudFront distribution to include a second origin for the new ALB and creating an origin group with primary and secondary origins, CloudFront can automatically route traffic to the secondary origin if the primary is unhealthy. This setup leverages CloudFront's global reach to improve availability and fault tolerance without the need for DNS-level changes.

Option A is not correct because it suggests creating a secondary deployment and updating the Route 53 A record to be a failover record with both CloudFront distributions as values. While Route 53 health checks and failover records can improve availability, CloudFront distributions themselves cannot be directly specified as values in A records for failover purposes. This option might lead to confusion in its implementation details.

upvoted 2 times

 **bjexamprep** 1 year, 11 months ago

Selected Answer: B

Who the hell cooked this terrible question design.

Usually, HA means single region, DR means cross region. The question is asking HA while all the answer are using cross region solutions. When Dynamic content is involved, the dynamic content has to be stored in a persistent storage, while question says the dynamic content is stored on the EC2 instances in an ASG, which means the EC2 instances are ephemeral.

And when Dynamic content is involved, no matter HA or DR, a replication component must be built so that the Dynamic content will be replicated to the other side so that it can be available when the event happens. While, none of the answers mention replication at all.

upvoted 2 times

 **ninomfr64** 1 year, 12 months ago

Selected Answer: B

Not A. CloudFront is a global service, having two distributions will not increase fault-tolerance

Not C. Single ALB is a single-point-of-failure and also you cannot have Target Group in a different region

Not D. CloudFront is a global service, having two distributions will not increase fault-tolerance and combining CloudFront with AWS Global Accelerator makes no sense

B is correct as provisioning an ALB, an Auto Scaling group, and EC2 instances in a different AWS region provides redundancy and failover capability for the application. The origin group is the right way to enable failover for CloudFront distributions origin

upvoted 3 times

 **holymancolin** 2 years, 1 month ago

Selected Answer: B

Not Create a second CloudFront Distribution, it's update the distribution with multi origins.

Ref:

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

"Make sure the distribution has more than one origin. If it doesn't, add a second origin."

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

it's a B

upvoted 1 times

 **[Removed]** 2 years, 6 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 2 times

 **mfsec** 2 years, 9 months ago

Selected Answer: B

Provision an ALB, an Auto Scaling group, and EC2 instances in a different AWS Region.

upvoted 1 times

 **dev112233xx** 2 years, 9 months ago

Selected Answer: B

B is the best solution with very high availability (compared to the R53 failover solution)

upvoted 1 times

 **Ajani** 2 years, 9 months ago

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html
upvoted 1 times

 **Sarutobi** 2 years, 10 months ago

Selected Answer: B

B looks good.

upvoted 1 times

 **masssa** 2 years, 11 months ago

Selected Answer: B

B is correct.

C is not correct, because ALB is regional service, so ALB have to be added too.

upvoted 2 times

Question #53

A company has an organization in AWS Organizations that has a large number of AWS accounts. One of the AWS accounts is designated as a transit account and has a transit gateway that is shared with all of the other AWS accounts. AWS Site-to-Site VPN connections are configured between all of the company's global offices and the transit account. The company has AWS Config enabled on all of its accounts.

The company's networking team needs to centrally manage a list of internal IP address ranges that belong to the global offices. Developers will reference this list to gain access to their applications securely.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Create a JSON file that is hosted in Amazon S3 and that lists all of the internal IP address ranges. Configure an Amazon Simple Notification Service (Amazon SNS) topic in each of the accounts that can be invoked when the JSON file is updated. Subscribe an AWS Lambda function to the SNS topic to update all relevant security group rules with the updated IP address ranges.
- B. Create a new AWS Config managed rule that contains all of the internal IP address ranges. Use the rule to check the security groups in each of the accounts to ensure compliance with the list of IP address ranges. Configure the rule to automatically remediate any noncompliant security group that is detected.
- C.** In the transit account, create a VPC prefix list with all of the internal IP address ranges. Use AWS Resource Access Manager to share the prefix list with all of the other accounts. Use the shared prefix list to configure security group rules in the other accounts.
- D. In the transit account, create a security group with all of the internal IP address ranges. Configure the security groups in the other accounts to reference the transit account's security group by using a nested security group reference of "/sg-1a2b3c4d".

Correct Answer: C

Community vote distribution

C (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: C

The correct answer is option C. In this solution, a VPC prefix list is created in the transit account with all of the internal IP address ranges, and then shared to all of the other accounts using AWS Resource Access Manager. This allows for central management of the IP address ranges, and eliminates the need for manual updates to security group rules in each account. This solution also allows for compliance checks to be run using AWS Config and for any non-compliant security groups to be automatically remediated.

Option A is not correct because it would require manual updates to the JSON file and would also require developers to manually update their security group rules, which would lead to operational overhead.

Option B is not correct because it would require the creation of a new AWS Config managed rule and it would also require manual updates to the security group rules in each account.

Option D is not correct because it would require manual updates to the security group in the transit account and it would also lead to operational overhead.

upvoted 24 times

 **jpa8300** 1 year, 12 months ago

I agree that option C is probably the best one, but B is also correct, there is no manual updates to the SG, the remediation is automated in AWS Config. In option C you also need to manually update the prefix list, no? Imagine a new CIDR appears in the offices.

upvoted 1 times

 **chicagobeef** 1 year, 11 months ago

I doubt all the security groups in the accounts will use the same CIDR ranges. They just need a way to centrally manage the CIDR prefixes. The question did not say that everyone has to comply and any non-compliant resources need to be remediated.

upvoted 2 times

 **Aritra88** Most Recent 1 year ago

Selected Answer: C

A VPC Prefix List is a reusable, user-defined resource in Amazon Virtual Private Cloud (VPC) that contains a collection of IP address ranges. These ranges can represent destinations or sources for traffic, and the prefix list can be referenced in various configurations like security groups, route tables, or network ACLs.

upvoted 1 times

 **Tiger4Code** 1 year ago

Selected Answer: C

C: in the shared account create a VPC Prefix list, share it using RAM, then SGs can reference it

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **nynomfr64** 1 year, 11 months ago

Selected Answer: C

Not A. This requires to maintain the JSON file, SNS topic in each account, Lambda to update SG. This is a lot of work, also not clear what accounts holds the S3 with the JSON

Not B. I was not able to spot a managed AWS Config rule that could help in this case

<https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html> (but I do not recall managed rule by hart and this doesn't sound like a remote use case, so in the exam this could trick me)

upvoted 2 times

 **nynomfr64** 1 year, 11 months ago

Not D. You can reference a VPC SG in other account VPCs when you have VPC peering in place, this is not mentioned in the scenario <https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html>. Since there is a Transit Gateway involved it is unlikely to have VPC peering and the resources in a VPC attached to a transit gateway cannot access the security groups of a different VPC that is also attached to the same transit gateway <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-vpc-attachments.html> (this option initially was not bad for me)

C works well as prefix lists are created exactly for this purpose <https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html>

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C for sure

upvoted 1 times

 **Asds** 2 years, 6 months ago

Selected Answer: C

Definitely prefix

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

prefix list and RAM

upvoted 2 times

 **dev112233xx** 2 years, 9 months ago

Selected Answer: C

C makes sense 

upvoted 2 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/82131-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

 **AjayD123** 2 years, 11 months ago

Selected Answer: C

[https://aws.amazon.com/blogs/networking-and-content-delivery/simplify-network-routing-and-security-administration-with-vpc-prefix-lists/#:~:text=A%20Prefix%20List%20is%20a,Resource%20Access%20Manager%20\(RAM\).](https://aws.amazon.com/blogs/networking-and-content-delivery/simplify-network-routing-and-security-administration-with-vpc-prefix-lists/#:~:text=A%20Prefix%20List%20is%20a,Resource%20Access%20Manager%20(RAM).)

upvoted 4 times

Question #54

A company runs a new application as a static website in Amazon S3. The company has deployed the application to a production AWS account and uses Amazon CloudFront to deliver the website. The website calls an Amazon API Gateway REST API. An AWS Lambda function backs each API method.

The company wants to create a CSV report every 2 weeks to show each API Lambda function's recommended configured memory, recommended cost, and the price difference between current configurations and the recommendations. The company will store the reports in an S3 bucket.

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

- A. Create a Lambda function that extracts metrics data for each API Lambda function from Amazon CloudWatch Logs for the 2-week period. Collate the data into tabular format. Store the data as a .csv file in an S3 bucket. Create an Amazon EventBridge rule to schedule the Lambda function to run every 2 weeks.
- B. Opt in to AWS Compute Optimizer. Create a Lambda function that calls the ExportLambdaFunctionRecommendations operation. Export the .csv file to an S3 bucket. Create an Amazon EventBridge rule to schedule the Lambda function to run every 2 weeks.
- C. Opt in to AWS Compute Optimizer. Set up enhanced infrastructure metrics. Within the Compute Optimizer console, schedule a job to export the Lambda recommendations to a .csv file. Store the file in an S3 bucket every 2 weeks.
- D. Purchase the AWS Business Support plan for the production account. Opt in to AWS Compute Optimizer for AWS Trusted Advisor checks. In the Trusted Advisor console, schedule a job to export the cost optimization checks to a .csv file. Store the file in an S3 bucket every 2 weeks.

Correct Answer: B*Community vote distribution*

B (79%)	12%	9%
---------	-----	----

 **masetromain** Highly Voted  2 years, 11 months ago

Selected Answer: B

The correct answer is B. Opting in to AWS Compute Optimizer and creating a Lambda function that calls the ExportLambdaFunctionRecommendations operation is the least development time solution. This option allows you to use the built-in AWS Compute Optimizer service to extract metrics data and export it as a CSV file, which can then be stored in an S3 bucket.

Option A is not correct because it requires the development of a Lambda function that extracts metrics data and collates it into tabular format, which adds development time. Option C is not correct because it requires the setup of enhanced infrastructure metrics, which adds development time. Option D is not correct because it requires purchasing the AWS Business Support plan and using the Trusted Advisor console, which adds development time.

upvoted 23 times

 **zozza2023** Highly Voted  2 years, 11 months ago

Selected Answer: B

AWS compute optimizer+ lambda

upvoted 9 times

 **evargasbrz** Most Recent  3 weeks ago

Selected Answer: B

C is not possible because the console only supports daily, weekly, or monthly schedules. For biweekly, you have to use another approach.

upvoted 1 times

 **Aritra88** 1 year ago

Selected Answer: B

Answer B

Solution Steps

1. Use AWS Compute Optimizer for Lambda Recommendations

AWS Compute Optimizer provides recommendations for Lambda functions, including:

- * Recommended memory size to improve performance or reduce cost.
- * Current and recommended cost comparisons.

You can query AWS Compute Optimizer using the AWS Management Console, AWS CLI, or SDKs to retrieve the necessary data for your report.

2. Automate Data Retrieval

Set up an AWS Lambda function to automate the process:

1. Query Compute Optimizer:

- * Use the GetLambdaFunctionRecommendations API to retrieve:

- * Current memory size

- * Recommended memory size
 - * Current and recommended cost
- upvoted 1 times

amministrazione 1 year, 3 months ago

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.

upvoted 1 times

8693a49 1 year, 5 months ago

Why would anyone need to memorize whether Compute Optimizer reports can be scheduled from the UI or must be done through API calls? This is so unnecessary *rolls eyes

upvoted 3 times

khchan123 1 year, 9 months ago

Selected Answer: C

The correct answer is C.

Option A involves creating a custom Lambda function to extract metrics data from CloudWatch Logs and generate the CSV report, which would require more development time compared to using the Compute Optimizer service.

Option B is partially correct, as it involves using Compute Optimizer and a Lambda function, but it misses the ability to schedule recurring exports directly within the Compute Optimizer console.

Option D suggests using AWS Trusted Advisor, which is a service for monitoring best practices and resources, but it does not provide the specific Lambda function memory and cost recommendations required in this scenario.

upvoted 3 times

helloworldabc 1 year, 3 months ago

just B

upvoted 2 times

8608f25 1 year, 10 months ago

Selected Answer: B

Option B is the most efficient and straightforward solution. By opting into AWS Compute Optimizer, the company can leverage AWS's service for recommendations on optimal AWS resource configurations based on utilization metrics. Using the ExportLambdaFunctionRecommendations operation allows for automating the retrieval of the desired optimization data with minimal code. Scheduling this operation with an Amazon EventBridge rule to run every 2 weeks and exporting the results directly to a CSV file in an S3 bucket meets all the stated requirements with minimal development effort.

upvoted 1 times

ninomfr64 1 year, 11 months ago

Selected Answer: C

Not A. This requires some serious development, also not 100% sure CW Logs alone provides all the required info.

Not B. This requires some coding to call the ExportLambdaFunctionRecommendations API

Not D. To create CSV reports (organizational view reports) in Trusted Advisor you need to enable Trusted Advisor in your organization, and AWS Organization is not mentioned in the scenario <https://docs.aws.amazon.com/awssupport/latest/user/organizational-view.html>

C is the right solution as it allows to schedule report with the required info with no development <https://docs.aws.amazon.com/compute-optimizer/latest/ug/exporting-recommendations.html>. This was misleading for me as it mentions to set up enhanced infrastructure metrics that is only available for EC2, but you can do it without development (you can do it from console), this adds cost but the ask focuses on development effort.

upvoted 2 times

8608f25 1 year, 10 months ago

It is not C. Option C describes using AWS Compute Optimizer and setting up a job within the Compute Optimizer console. However, as of the last update, Compute Optimizer does not provide a direct scheduling feature within the console for exporting recommendations to a CSV file. This option suggests functionality that is not directly available in Compute Optimizer.

upvoted 5 times

AWSCertification2024 1 year, 12 months ago

Selected Answer: B

B is correct

Not C because Enhanced infrastructure metrics is a paid feature of Compute Optimizer that applies to Amazon EC2 instances and instances that are part of Auto Scaling groups.

upvoted 3 times

enk 2 years, 1 month ago

Selected Answer: D

Lambda = development. Option D has no development. If you are not familiar with dev'ing - publishing a simple Lambda function can require you to wrap all the Node.js or Python or whatever programming language libraries with it in order to execute correctly within AWS Lambda. Configuring Trusted Advisor (GUI) or scheduling a job is NOT considered Development.

upvoted 3 times

KCjoe 2 years, 2 months ago

Selected Answer: D

Basic plan of Trusted Advisor only has 7 core checks. Business plan has all these, so with LEAST development, it must be business plan.
Check categories
Cost optimization
Performance
Security
Fault tolerance
Service limits
upvoted 5 times

 **rif** 2 years, 2 months ago

B.
Option C is not correct because "Enhanced infrastructure metrics is a paid feature of Compute Optimizer that applies to Amazon EC2 instances."
<https://docs.aws.amazon.com/compute-optimizer/latest/ug/enhanced-infrastructure-metrics.html>
upvoted 1 times

 **awsent** 2 years, 3 months 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 4 times

 **awsent** 2 years, 3 months ago

Answer: B
<https://aws.amazon.com/blogs/compute/optimizing-aws-lambda-cost-and-performance-using-aws-compute-optimizer/>
upvoted 1 times

 **Simon523** 2 years, 3 months ago

Selected Answer: B
AWS Compute Optimizer helps avoid overprovisioning and underprovisioning four types of AWS resources—Amazon Elastic Compute Cloud (EC2) instance types, Amazon Elastic Block Store (EBS) volumes, Amazon Elastic Container Service (ECS) services on AWS Fargate, and AWS Lambda functions—based on your utilization data.
upvoted 4 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B
its a B
upvoted 1 times

Question #55

A company's factory and automation applications are running in a single VPC. More than 20 applications run on a combination of Amazon EC2, Amazon Elastic Container Service (Amazon ECS), and Amazon RDS.

The company has software engineers spread across three teams. One of the three teams owns each application, and each team is responsible for the cost and performance of all of its applications. Team resources have tags that represent their application and team. The teams use IAM access for daily activities.

The company needs to determine which costs on the monthly AWS bill are attributable to each application or team. The company also must be able to create reports to compare costs from the last 12 months and to help forecast costs for the next 12 months. A solutions architect must recommend an AWS Billing and Cost Management solution that provides these cost reports.

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

- A. Activate the user-defined cost allocation tags that represent the application and the team.
- B. Activate the AWS generated cost allocation tags that represent the application and the team.
- C. Create a cost category for each application in Billing and Cost Management.
- D. Activate IAM access to Billing and Cost Management.
- E. Create a cost budget.
- F. Enable Cost Explorer.

Correct Answer: ACF*Community vote distribution*

ACF (57%)

ADF (43%)

 **masetromain**  2 years, 11 months ago

Selected Answer: ACF

A, C and F are the correct answers because they provide the required cost reports and analysis for the company's applications and teams.

A. Activating user-defined cost allocation tags that represent the application and the team allows the company to assign costs to specific applications and teams. This allows the company to see how much each application and team is costing them, which is important for cost forecasting and budgeting.

C. Creating a cost category for each application in Billing and Cost Management allows the company to group costs by application. This makes it easier to understand the costs associated with each application and to compare the costs of different applications over time.

F. Enabling Cost Explorer allows the company to analyze costs and usage over time, and to create custom reports and forecasts. This is important for understanding the costs associated with each application and team, and for forecasting future costs.

upvoted 43 times

 **masetromain** 2 years, 11 months ago

B is not correct because AWS generated cost allocation tags are automatically created for some AWS resources, but it does not provide the required cost reports and analysis for the company's applications and teams.

Option D is not correct because IAM access controls are used to limit access to the billing and cost management features, but it is not necessary to configure it to meet the requirements.

E is not correct because Creating a cost budget allows the company to set a budget for their costs and to receive alerts when costs exceed the budget, but it does not provide the required cost reports and analysis for the company's applications and teams.

upvoted 7 times

 **a_c_** 2 years, 7 months ago

With out granting IAM Access, IAM users cannot access Billing console, so s cannot see the Cost explorer
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/control-access-billing.html>.

Question says teams are responsible for cost

I

upvoted 10 times

 **djeong95** 1 year, 10 months ago

In addition to the IAM access problem answer ACF will face, the problem statement already presents us with the information that resources are already tagged by team/application. Creating cost category seems redundant and even if you did create this redundancy, you are faced with the IAM access problem.

If each team is responsible for the cost and the performance, they would need access to the billing console for their team.
upvoted 2 times

 **e4bc18e** 1 year, 8 months ago

So you are wrong, tags can be applied to applications so you can easily find them but unless they are actually activated as user defined billing tags then you will not be able to use those tags in cost analysis. Also you have to enable cost explorer it is not enabled by default and cost explorer lets you see the previous 12 months and creates projections for the next 12, so without that option you will not meet the objective.

upvoted 3 times

 **spd**  2 years, 10 months ago

Selected Answer: ADF

Correct ADF - Since resources are tagged, C may not require ?

upvoted 18 times

 **eesa**  8 months, 1 week ago

Selected Answer: ACF

A. Activate the user-defined cost allocation tags

User-defined tags must be explicitly activated in AWS Billing and Cost Management for cost allocation.

Since the teams already have tags on their resources representing their applications and teams, activating these user-defined tags allows AWS to organize the costs accordingly.

C. Create a cost category for each application

Cost categories simplify grouping related costs.

You can group resources by application or team, making it easier to manage and report on costs for comparison and forecasting.

F. Enable Cost Explorer

Cost Explorer provides historical cost reports and visualizes trends over the past 12 months.

It also allows cost forecasting for the next 12 months, directly fulfilling the requirement to compare and forecast costs.

upvoted 1 times

 **bhanus** 1 year ago

Selected Answer: ACF

ACF

User defined tags to separate out billing.

Grouping the costs.

Cost Explorer to analyze the costs.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. Activate the user-defined cost allocation tags that represent the application and the team.

C. Create a cost category for each application in Billing and Cost Management.

E. Create a cost budget

upvoted 3 times

 **neta1o** 1 year, 5 months ago

Selected Answer: ACF

The company needs to determine which costs on the monthly AWS bill are attributable to each application or team. - Tagging and Cost Categories

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. -Cost Explorer

upvoted 3 times

 **alex_heavy** 1 year, 5 months ago

Selected Answer: ADF

A. User defined cost allocation tags: application, team

D. Activate IAM access to Billing and Cost Management:

"The teams use IAM access for daily activities."

<https://docs.aws.amazon.com/cost-management/latest/userguide/control-access-billing.html>

F. Enable Cost Explorer: <https://docs.aws.amazon.com/cost-management/latest/userguide/ce-enable.html>

C is NOT needed, because A already will give a usage view by "tags that represent their application and team" "The company needs to determine which costs on the monthly AWS bill are attributable to each application or team"

upvoted 4 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: ACF

Option ACF and NOT ADF - Cost allocation helps you identify who is spending what, within your organization. Cost categories is a cost allocation service to help you map your AWS costs, to your unique internal business structures.

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html>

upvoted 3 times

✉ **mav3r1ck** 1 year, 9 months ago

Selected Answer: ACF

Focusing on enabling the company to attribute AWS costs to each application or team, create cost comparison reports for the last 12 months, and forecast costs for the next 12 months,..Answer: A, C, F.

upvoted 2 times

✉ **mav3r1ck** 1 year, 9 months ago

here's the detailed recommendation:

upvoted 1 times

✉ **mav3r1ck** 1 year, 9 months ago

F. Enable Cost Explorer: Cost Explorer is essential for analyzing past spending and forecasting future costs. It allows for detailed reports that can compare costs from the last 12 months and helps in forecasting for the next 12 months. With the data segmented by user-defined cost allocation tags, Cost Explorer can provide the insights needed to meet the company's reporting and forecasting requirements.

C. Create a cost category for each application in Billing and Cost Management: Cost categories allow for the organization of cost and usage data into logical groups that reflect the company's internal structure, such as by application or team. By leveraging the user-defined tags activated in step A, cost categories can automate the process of cost attribution to these entities, simplifying the creation of targeted reports and forecasts.

upvoted 1 times

✉ **mav3r1ck** 1 year, 9 months ago

A. Activate user-defined cost allocation tags: User-defined tags need to be activated for cost allocation purposes. These tags, representing applications and teams, are crucial for attributing costs accurately to the responsible entities within the company. Once activated, these tags will appear in the AWS Billing and Cost Management dashboard, enabling detailed tracking and reporting based on the specified tags.

upvoted 1 times

✉ **mav3r1ck** 1 year, 9 months ago

Explanation of Exclusions: B, D, F

upvoted 1 times

✉ **mav3r1ck** 1 year, 9 months ago

B. Activate AWS generated cost allocation tags: While AWS-generated tags provide useful information, they might not directly align with the specific needs for application or team-based reporting. For the purpose of attributing costs to custom-defined entities like specific applications or teams, user-defined tags are more directly applicable.

upvoted 1 times

✉ **mav3r1ck** 1 year, 9 months ago

[correction for typo error above] Explanation of Exclusions: B, D, E

upvoted 1 times

✉ **mav3r1ck** 1 year, 9 months ago

D. Activate IAM access to Billing and Cost Management: While important for ensuring that team members can access billing information, this action itself doesn't contribute directly to organizing or reporting on costs by application or team, nor does it facilitate forecasting.

upvoted 1 times

✉ **gofavad926** 1 year, 9 months ago

Selected Answer: ACF

Agree with ACF

upvoted 3 times

✉ **Dgix** 1 year, 9 months ago

Selected Answer: ACF

For the full granularity, C is needed rather than D.

upvoted 3 times

✉ **a54b16f** 1 year, 9 months ago

Selected Answer: ADF

C is not needed. Option A activated the tag, so we could use tags to generate reports. There is no need to create cost category for individual applications, which could be a huge effort and not practical, what if you have hundreds of applications...

upvoted 3 times

✉ **a54b16f** 1 year, 10 months ago

Selected Answer: ADF

Correct ADF - Since resources are tagged

upvoted 2 times

 **8608f25** 1 year, 10 months ago

Selected Answer: ACF

Correct answers are:

- A. Activate the user-defined cost allocation tags that represent the application and the team. User-defined cost allocation tags allow you to organize your AWS bill by categorizing costs according to your business's organizational structures (e.g., by application or team).
- C. Create a cost category for each application in Billing and Cost Management. Cost categories enable you to create custom groupings of your AWS costs. By creating a cost category for each application, you can group costs more granularly, which is helpful for detailed reporting and cost attribution to specific teams or applications.
- F. Enable Cost Explorer. Cost Explorer is a tool that allows you to visualize, understand, and manage your AWS costs and usage over time. By enabling Cost Explorer, you can create detailed reports to compare costs from the last 12 months and forecast costs for the next 12 months, meeting the company's requirements for cost management and planning.

upvoted 2 times

 **8608f25** 1 year, 10 months ago

Option B is not correct. It refers to activating AWS generated cost allocation tags. While AWS-generated tags can provide useful information, they do not typically represent specific applications or teams unless those entities are directly associated with AWS-defined resources or actions. For custom application and team tracking, user-defined tags (Option A) are more appropriate.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: ADF

Not B. AWS generated tags do not allow you to identify app. You need user-defined tags for this

Not C. Cost Categories allows to define rule to group costs into categories using different dimensions such as: account, tag, service, charge type, and other cost categories. In this scenario User-defined tags are enough to identify applications and teams.

Not E. Budget doesn't help you in creating reports to compare costs from the last 12 months and to help forecast costs for the next 12 months. Use Cost Explorer instead-

upvoted 5 times

 **jpa8300** 1 year, 12 months ago

Selected Answer: ADF

See below severlight explanation. I agree with it.

upvoted 3 times

 **Dips3009** 2 years ago

can someone help me with this solutions, as I am confused between ACF and ADF

upvoted 1 times

Question #56

An AWS customer has a web application that runs on premises. The web application fetches data from a third-party API that is behind a firewall. The third party accepts only one public CIDR block in each client's allow list.

The customer wants to migrate their web application to the AWS Cloud. The application will be hosted on a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in a VPC. The ALB is located in public subnets. The EC2 instances are located in private subnets. NAT gateways provide internet access to the private subnets.

How should a solutions architect ensure that the web application can continue to call the third-party API after the migration?

- A. Associate a block of customer-owned public IP addresses to the VPC. Enable public IP addressing for public subnets in the VPC.
- B. Register a block of customer-owned public IP addresses in the AWS account. Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC.
- C. Create Elastic IP addresses from the block of customer-owned IP addresses. Assign the static Elastic IP addresses to the ALB.
- D. Register a block of customer-owned public IP addresses in the AWS account. Set up AWS Global Accelerator to use Elastic IP addresses from the address block. Set the ALB as the accelerator endpoint.

Correct Answer: B*Community vote distribution*

B (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: B

The correct solution is B. Register a block of customer-owned public IP addresses in the AWS account. Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC. This will ensure that the web application can continue to call the third-party API after the migration by using the customer-owned public IP addresses that were assigned to the NAT gateways. This ensures that the third-party API will only see traffic coming from the customer-owned IP addresses that are on the allow list. Option A,C and D doesn't make sense in this context.

upvoted 21 times

 **amministrazione** Most Recent 1 year, 3 months ago

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.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: B

In this scenario EC2 instances access the 3P APIs via NAT Gateway. 3P API FW see IP of the NAT Gateway. You can assign Elastic IP to NAT Gateway and you can allocate an IP address from a pool that you have brought to your AWS account to the Elastic IP. Thus B is correct.
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

its a B

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: B

KEYWORD = NAT gateways in the VPC

upvoted 2 times

 **AWS_Sam** 2 years, 7 months ago

B is the only option that makes sense.

upvoted 1 times

 **SkyZeroZx** 2 years, 7 months ago

Selected Answer: B

B make sense

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: B

Register a block of customer owned public IP's
upvoted 2 times

 **dev112233xx** 2 years, 9 months ago

Selected Answer: B
B is the only solution
upvoted 2 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: B
The correct solution is B
upvoted 4 times

A company with several AWS accounts is using AWS Organizations and service control policies (SCPs). An administrator created the following SCP and has attached it to an organizational unit (OU) that contains AWS account 1111-1111-1111:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsAllActions",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Sid": "DenyCloudTrail",
      "Effect": "Deny",
      "Action": "cloudtrail:*",
      "Resource": "*"
    }
  ]
}
```

Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets. How should the administrator address this problem?

- A. Add s3:CreateBucket with "Allow" effect to the SCP.
- B. Remove the account from the OU, and attach the SCP directly to account 1111-1111-1111.
- C. Instruct the developers to add Amazon S3 permissions to their IAM entities.
- D. Remove the SCP from account 1111-1111-1111.

Correct Answer: C

Community vote distribution

C (87%)

13%

✉  **Atila50**  2 years, 11 months ago

Selected Answer: C

SCP doesn't grant permission
upvoted 24 times

✉  **c73bf38** 2 years, 10 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 7 times

✉  **c73bf38** 2 years, 10 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 12 times

✉  **zhangyu20000**  2 years, 11 months 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 13 times

✉  **29fb203**  9 months, 3 weeks ago

Selected Answer: A

IAM permissions do not override SCPs. Even if developers have IAM policies allowing s3:CreateBucket, an SCP restriction will still block it unless explicitly allowed.

upvoted 1 times

 **vmia159** 9 months, 3 weeks ago

Your statement is correct but the policy does not deny action on S3. So the SCP is not causing any problems. So it is C.
upvoted 1 times

 **longlehoang** 10 months, 2 weeks ago

Selected Answer: A

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "*",  
      "Resource": "*"  
    },  
    {  
      "Sid": "DenyCloudTrail",  
      "Effect": "Deny",  
      "Action": "cloudtrail:*",  
      "Resource": "*"  
    },  
    {  
      "Sid": "AllowS3CreateBucket",  
      "Effect": "Allow",  
      "Action": "s3:CreateBucket",  
      "Resource": "*"  
    }  
  ]  
}
```

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **helloworldabc** 1 year, 3 months ago

just C

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C

C, SCP is just a distractor, the users need direct permissions

upvoted 3 times

 **8608f25** 1 year, 10 months ago

Selected Answer: C

The problem described does not originate from the Service Control Policy (SCP) itself based on the SCP content provided. The SCP allows all actions ("Action": "") except for actions related to AWS CloudTrail ("Action": "CloudTrail:"), which are explicitly denied. Therefore, the inability for developers to create Amazon S3 buckets is not due to this SCP, as the SCP does not restrict S3 actions.

Given the situation, the correct way to address the developers' inability to create Amazon S3 buckets would be:

* C. Instruct the developers to add Amazon S3 permissions to their IAM entities.

Option C is the correct action because the issue likely stems from the IAM permissions (or lack thereof) assigned to the developers' IAM entities (users, groups, or roles). IAM permissions are required to perform actions within AWS accounts, such as creating S3 buckets. If developers lack the necessary IAM permissions, they would not be able to create S3 buckets regardless of the SCP settings.

upvoted 2 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: C

The SCP in the scenario is allowing any actions with the exception of clouptrail. Thus, the SCP is not preventing user to create S3 bucket. If the user cannot create a bucket, then the user IAM user/role is missing permissions to create S3 bucket.

upvoted 3 times

 **shaam80** 2 years ago

Selected Answer: C

Answer C.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

it's a C

upvoted 1 times

 **javitech83** 2 years, 6 months ago

Selected Answer: C

C is correct
upvoted 1 times

 **SkyZeroZx** 2 years, 6 months 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** 2 years, 6 months ago

C is the answer. SCP DONT grant permissions. They just set boundaries on what account is capable of giving access to all users. For example, we applied a SCP on an OU that has account A. This SCP has S3fullAWSaccess. This does NOT mean that any IAM user can perform any S3 action. You still need to explicitly define IAM permissions for user to perform action on S3. This is called whitelisting. Another example, You wrote an SCP that DENIES S3 access and applied it to an OU that has account B. Now Lets say ROOT user of Account B (who got admin privileges) tries to create S3 bucket, they get DENIED error as SCP has already set a bounday saying NOONE in this OU can access S3

upvoted 2 times

 **Asds** 2 years, 6 months ago

Selected Answer: C

Need to deal with iam policy auth now
upvoted 1 times

 **Asds** 2 years, 6 months ago

C is right
upvoted 1 times

 **leehjworking** 2 years, 7 months ago

I am not sure the given situation is possible.
When I tested, member (1111-1111-1111) could create bucket without any policy which can be attached or detached by the oneself.
upvoted 2 times

 **leehjworking** 2 years, 7 months ago

Are developers allowed to modify their IAM entities in the situation of option C? If so, I am not sure this is the best practice.
upvoted 2 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

C is correct
upvoted 2 times

Question #58

A company has a monolithic application that is critical to the company's business. The company hosts the application on an Amazon EC2 instance that runs Amazon Linux 2. The company's application team receives a directive from the legal department to back up the data from the instance's encrypted Amazon Elastic Block Store (Amazon EBS) volume to an Amazon S3 bucket. The application team does not have the administrative SSH key pair for the instance. The application must continue to serve the users.

Which solution will meet these requirements?

- A. Attach a role to the instance with permission to write to Amazon S3. Use the AWS Systems Manager Session Manager option to gain access to the instance and run commands to copy data into Amazon S3.
- B. Create an image of the instance with the reboot option turned on. Launch a new EC2 instance from the image. Attach a role to the new instance with permission to write to Amazon S3. Run a command to copy data into Amazon S3.
- C. Take a snapshot of the EBS volume by using Amazon Data Lifecycle Manager (Amazon DLM). Copy the data to Amazon S3.
- D. Create an image of the instance. Launch a new EC2 instance from the image. Attach a role to the new instance with permission to write to Amazon S3. Run a command to copy data into Amazon S3.

Correct Answer: A*Community vote distribution*

A (59%) C (40%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: C

The correct answer is C. Taking a snapshot of the EBS volume using Amazon Data Lifecycle Manager (DLM) will meet the requirements because it allows you to create a backup of the volume without the need to access the instance or its SSH key pair. Additionally, DLM allows you to schedule the backups to occur at specific intervals and also enables you to copy the snapshots to an S3 bucket. This approach will not impact the running application as the backup is performed on the EBS volume level.

Option A is not correct because the instance would need an IAM role with permission to write to S3 and access to the instance via Systems Manager Session Manager.

Option B is not correct because it would require stopping the instance, which would impact the running application.

Option D is not correct because it would require stopping the instance and creating a new EC2 instance, which would impact the running application.

upvoted 40 times

 **Sab** 2 years, 1 month ago

Your reasoning is wrong . Option A has mentioned that instance profile role is attached to EC2 instance.

upvoted 2 times

 **Atila50** 2 years, 11 months ago

thank you for correcting some of these answers and for the explanations to them

upvoted 3 times

 **mmendoza** 2 years, 11 months ago

Assuming that EBS is encrypted, I think that is much easier to run the copy command from AW system manager

upvoted 10 times

 **aviathor** 2 years, 5 months ago

The question does not state that the SSM Daemon is running on the instance...

upvoted 3 times

 **g0h4n** 2 years, 2 months ago

Linux amazon 2 has SSM agent installed by default

upvoted 9 times

 **bititan** Highly Voted 2 years, 11 months ago

Selected Answer: A

taking a backup of the data to s3. aws doesn't allow up to view snapshots in s3

upvoted 13 times

 **tmlong18** 1 year, 11 months ago

The requirement is only 'back up'

upvoted 1 times

 **evargasbrz** Most Recent 3 weeks ago

Selected Answer: A

C is not possible. Amazon DLM can create snapshots of encrypted EBS volumes, but you cannot directly copy EBS snapshots to S3.
upvoted 1 times

 **aka1177** 3 weeks, 2 days ago

Selected Answer: C

In reality it will be C; If the legal department is requesting the data, then a full disk copy is required — you're not going to manually copy all the files after logging in.

upvoted 1 times

 **b0969fd** 2 months, 1 week ago

Selected Answer: A

The easiest way to do what is asked.

For option C, it is a bit possible but you have to spin a new EC2 instance using the new snapshot. Make sure all configuration is set so that the data from the encrypted snapshot is useable in that EC2 instance. And you have to do that activity every x amount of times in case you have to back up new data. While operational efficiency isn't required, I am not going to those steps as it's too tedious

upvoted 1 times

 **strike3test** 5 months, 2 weeks ago

Selected Answer: A

Why not D -> snapshots are stored in EBS, not in S3 directly accessible.

upvoted 2 times

 **strike3test** 6 months, 1 week ago

Selected Answer: C

This requires that the instance has the SSM agent installed and configured, and the instance profile has the right permissions. However, the question does not confirm that SSM is enabled on the instance.

upvoted 1 times

 **0dc6cac** 6 months, 2 weeks ago

Selected Answer: C

They don't mention whether the instance has SSM permissions, adding that would require a restart of the EC2 instance, causing an interruption. Hence I think C is more appropriate, we can back-up the EBS and there are tools to access data, or we can start up a new instance and get the data when needed.

upvoted 1 times

 **Kaps443** 6 months, 3 weeks ago

Selected Answer: A

A is the most elegant and operationally safe solution.

It allows you to access the instance securely, without SSH, and back up the data live to S3 — with no service interruption.

upvoted 3 times

 **eesa** 8 months, 1 week ago

Selected Answer: A

Why Option A is correct:

The AWS Systems Manager (SSM) Session Manager allows secure, shell-level access to EC2 instances without the need for an SSH key pair.

Attaching an IAM role with appropriate permissions to the EC2 instance allows it to securely interact with Amazon S3 without manual credential management.

Session Manager does not require a restart of the instance or impact the application availability, ensuring no downtime and continuous service to users.

This solution directly fulfills the requirement: securely copying data from the encrypted EBS volume to S3 without administrative SSH access and without disruption.

upvoted 4 times

 **grumpysloth** 1 year ago

Selected Answer: D

This is a badly designed question IMO. (D) could be correct but creating an AMI by default will reboot the instance, and no mention of SSM role permissions. (A) could also work but no mention of SSM permissions in the role. Amazon Linux 2 have pre-installed the SSM agent. (B) is wrong since it interrupts the app. (C) won't work.

upvoted 1 times

 **Heman31in** 1 year ago

Selected Answer: A

not C because of How EBS Snapshot Export Works

When you export an EBS snapshot to S3, the export creates an Amazon Machine Image (AMI)-compatible format of the snapshot. This export process results in a snapshot stored as disk image files (e.g., .vmdk, .vhdx, .raw, etc.), depending on the format chosen. The data is not immediately readable or usable as a plain text or object file in S3.

When is the Data Readable?

To make the exported data readable:

Reimport the Snapshot: You would need to reimport the disk image into AWS as a new EBS volume using the VM Import/Export service.

Custom Processing: If the snapshot contains a file system, you could manually process the exported image to extract the data using tools compatible with the format (e.g., mounting a .raw image locally).

upvoted 2 times

Heman31in 1 year ago

Selected Answer: A

C. Take a snapshot of the EBS volume by using Amazon Data Lifecycle Manager (Amazon DLM). Copy the data to Amazon S3.

Challenges:

While creating an EBS snapshot is feasible without requiring instance access, transferring the data from the snapshot to S3 still requires additional steps.

Snapshot-based backup does not provide direct file-level access for selective backups to S3.

Conclusion: Partially valid, but it does not meet the requirement to back up the data directly to S3. Since it is a legal department ..why to have another copy before transferring to final S3 destination.

upvoted 2 times

Aritra88 1 year ago

Selected Answer: A

Leverages AWS Systems Manager Session Manager:

Session Manager allows secure shell-less access to the instance without requiring an SSH key.

It provides a way to run commands directly on the instance, even if SSH access is unavailable.

No Disruption to the Application:

The instance remains operational, and the application continues to serve users while the commands are executed.

S3 IAM Role for Access:

By attaching an IAM role to the instance with permissions to write to S3, you can securely transfer data without needing to configure additional credentials.

Efficient and Direct Backup:

Data is copied directly from the running instance to the S3 bucket, eliminating the need for intermediate snapshots, new instances, or additional resources.

Minimal Development Time:

This approach avoids creating images, launching new instances, or performing additional resource management steps.

upvoted 2 times

DhirajBansal 1 year ago

Selected Answer: A

A is Correct Answer.

IAM Role will provide EC2 instance to write data to S3 bucket.

Systems Manager Session Manager will access system and initiate back writing in S3. This will satisfy the condition of not having SSH Keys.

upvoted 3 times

amministrazione 1 year, 3 months ago

C. Take a snapshot of the EBS volume by using Amazon Data Lifecycle Manager (Amazon DLM). Copy the data to Amazon S3.

upvoted 1 times

Jason666888 1 year, 4 months ago

Selected Answer: C

Key point: The application must continue to serve the users.

If we choose A, then it may impact the application.

C wouldn't have that problem

upvoted 2 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.

Correct Answer: BDF*Community vote distribution*

BDF (95%)	3%
-----------	----

 **icassp** Highly Voted 2 years, 11 months ago

Selected Answer: BDF

"The above command should be executed with destination AWS IAM user account credentials only otherwise the copied objects in destination S3 bucket will still have the source account permissions and won't be accessible by destination account users." According to <https://medium.com/tensult/copy-s3-bucket-objects-across-aws-accounts-e46c15c4b9e1>.

upvoted 27 times

 **masetromain** 2 years, 11 months ago

You are correct, step E should be executed using the IAM user credentials from the destination account. This is because when objects are copied from one bucket to another, the object's permissions (ACLs) are also copied. Therefore, if the objects are copied using the IAM user credentials from the source account, the objects will have the same permissions as they did in the source bucket, which may not include permissions for the user in the destination account. By using the IAM user credentials from the destination account, the objects will have the appropriate permissions for the user in the destination account once they are copied.

upvoted 5 times

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: BDF

I switch to BDF;
Step B is necessary so that the user in the destination account has the necessary permissions to access the source bucket and list its contents, read its objects.

Step D is needed so that the user in the destination account has the necessary permissions to access the destination bucket and list contents, put objects, and set object ACLs

Step F is necessary because the aws s3 sync command needs to be run using the IAM user credentials from the destination account, so that the objects will have the appropriate permissions for the user in the destination account once they are copied.

The other choices are not correct because :

A. and C. are about creating policies in the source account but the user who wants to access the data is in the destination account
E. is about running the command with the source account, which is not suitable because it will lead to copied objects in destination S3 bucket still have the source account permissions and won't be accessible by destination account users.

upvoted 16 times

 **jAtlas7** Most Recent 1 year, 1 month ago

BDF is the answer - see: <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

 **amministrazione** 1 year, 3 months ago

- 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.
- 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. F. Run the aws s3 sync command as a user in the destination account. Specify the source and destination buckets to copy the data.

upvoted 1 times

8608f25 1 year, 10 months ago

Selected Answer: BDF

B. Create a bucket policy to allow a user in the destination account to list the source bucket's contents and read the source bucket's objects. Attach the bucket policy to the source bucket. This step ensures that the destination account has the necessary permissions to access the data in the source bucket.

D. Create an IAM policy in the destination account. Configure the policy to allow a user in the destination account to list contents and get objects in the source bucket, and to list contents, put objects, and set object ACLs in the destination bucket. Attach the policy to the user. This step provides the necessary permissions for a user in the destination account to both access the source bucket's contents and write to the destination bucket.

upvoted 1 times

8608f25 1 year, 10 months ago

F. Run the aws s3 sync command as a user in the destination account. Specify the source and destination buckets to copy the data. Performing the sync operation as a user in the destination account, who has been granted the appropriate permissions, ensures that the data can be copied from the source bucket to the destination bucket successfully.

upvoted 1 times

ninomfr64 1 year, 11 months ago

Selected Answer: BDF

Not A. A bucket policy attached to destination bucket cannot allow the source bucket to execute actions

Not C. Because we are picking option B which relies on a policy allowing a user in the destination account.

Not E. Because we are picking options B and D which rely on a user in the destination account

upvoted 1 times

jpa8300 1 year, 12 months ago

Selected Answer: BDF

No need for more explanations, the ones below are enough.

upvoted 1 times

edder 2 years, 1 month ago

Selected Answer: BDF

BD:

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

F:

<https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-commands.html>

upvoted 1 times

aviathor 2 years, 3 months ago

Selected Answer: BDF

A is incorrect since a bucket policy cannot allow another bucket to do anything. B. Is however an option since you can indeed create a bucket policy to allow a user in another account to perform operations on the bucket.

Once you have chosen B, then D and F are the only possible choices.

upvoted 2 times

H4des 2 years, 4 months 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 2 years, 4 months ago

Selected Answer: BDF

I prefer BDF, I do not know why the correct answer is ADF

upvoted 1 times

Christina666 2 years, 5 months 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 2 times

NikkyDicky 2 years, 5 months ago

Selected Answer: BDF

it's BDF for sure

upvoted 1 times

Maria2023 2 years, 6 months ago

Selected Answer: BDF

The entire idea of A is wrong (you achieve nothing by giving rights from one bucket to another) so we start from B and the rest are a common sense

upvoted 2 times

 **huanaws088** 2 years, 8 months ago

Selected Answer: BDF

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/copy-data-from-an-s3-bucket-to-another-account-and-region-by-using-the-aws-cli.html>

upvoted 3 times

 **God_Is_Love** 2 years, 10 months ago

Logical answer : Who ever uploads to a bucket becomes its owner. So A should ring a flaw in it. Similar issue in C. So straight away, A, C are wrong. that points to B,D to be correct. Refer <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/copy-data-from-an-s3-bucket-in-one-account-and-region-to-another-account-and-region.html>

Now E or F ? the hint is in D. Destination account user has the necessary privileges to get/put objects permission. So choose destination account or run sync/copy commands. So the answer should be B, D , F

upvoted 6 times

 **hobokabobo** 2 years, 10 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(pushng from source to destination) as only read access is granted to the foreign account but no write access - especially regarding human error: one cannot accidentally tamper with the source, so the worst thing that could happen is that one needs to sync again. The other options don't fit together with other parts.

upvoted 1 times

Question #60

Topic 1

A company built an application based on AWS Lambda deployed in an AWS CloudFormation stack. The last production release of the web application introduced an issue that resulted in an outage lasting several minutes. A solutions architect must adjust the deployment process to support a canary release.

Which solution will meet these requirements?

- A. Create an alias for every new deployed version of the Lambda function. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load.
- B. Deploy the application into a new CloudFormation stack. Use an Amazon Route 53 weighted routing policy to distribute the load.
- C. Create a version for every new deployed Lambda function. Use the AWS CLI update-function-configuration command with the routing-config parameter to distribute the load.
- D. Configure AWS CodeDeploy and use CodeDeployDefault.OneAtATime in the Deployment configuration to distribute the load.

Correct Answer: A

Community vote distribution

A (97%)

✉  **masetromain**  2 years, 11 months ago

Selected Answer: A

A. Create an alias for every new deployed version of the Lambda function. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load is the correct answer as it meets the requirement of supporting a canary release.

Option B is not correct because while it would allow for a canary release, it would involve deploying the new version of the application into a separate CloudFormation stack, which would be a more complex and time-consuming process compared to creating an alias for a new version of the Lambda function.

Option C is not correct because while it would allow for a canary release, it would involve creating a version for every new deployed Lambda function, which would be more complex and time-consuming process compared to creating an alias for a new version of the Lambda function.

upvoted 21 times

✉  **masetromain** 2 years, 11 months ago

Option D is not correct because AWS CodeDeploy is a deployment service that allows you to automate code deployments to a variety of compute services like EC2 and on-premises servers, but it does not support routing configuration for a canary release on AWS Lambda.

upvoted 6 times

✉  **karma4moksha** 2 years, 7 months ago

Thank you masetromain, you have been really helpful for taking the time and providing explanation.

upvoted 1 times

✉  **Jesuisleon** 2 years, 7 months ago

He copied from chatgpt, you didn't find it ?

upvoted 10 times

✉  **ninomfr64** 1 year, 11 months ago

This is not 100% correct. Actually CodeDeploy support deploy to an AWS Lambda compute platform, the deployment configuration specifies the way traffic is shifted to the new Lambda function versions in your application. You can shift traffic using a canary, linear, or all-at-once deployment configuration. The following lists the predefined configurations available for AWS Lambda canary deployments:

- CodeDeployDefault.LambdaCanary10Percent5Minutes
- CodeDeployDefault.LambdaCanary10Percent10Minutes
- CodeDeployDefault.LambdaCanary10Percent15Minutes
- CodeDeployDefault.LambdaCanary10Percent30Minutes

upvoted 3 times

✉  **Jason666888** 1 year, 4 months ago

Yeah the reason D is wrong is not because CodeDeploy doesn't support lambda canary deployment, it's because 'OneAtATime' deployment strategy is only for EC2 instances but not for lambdas

upvoted 3 times

✉  **Atila50**  2 years, 11 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/28312-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 10 times

 **29fb203** Most Recent 9 months, 3 weeks ago

Selected Answer: D

AWS CodeDeploy supports canary releases for Lambda functions, which is what the requirement is aiming for.
upvoted 1 times

 **d401c0d** 11 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
upvoted 1 times

 **Heman31in** 1 year ago

Selected Answer: A

Not D because, the CodeDeployDefault.OneAtATime deployment configuration is primarily designed for EC2 and on-premises instances. For AWS Lambda functions, AWS CodeDeploy provides deployment strategies specific to Lambda, such as Canary, Linear, and All-at-Once.
upvoted 1 times

 **Aritra88** 1 year ago

Selected Answer: A

Using Lambda Aliases for Canary Releases:

- * Lambda aliases are pointers to specific versions of a Lambda function.
- * You can use the update-alias command with the routing-config parameter to configure traffic shifting between the current version and the newly deployed version.
- * This allows a gradual shift of traffic to the new version while maintaining traffic to the current version.

AWS CLI Example:

- * Create a new alias or update an existing alias to shift a portion of the traffic

Testing and Monitoring:

Gradually increase the percentage of traffic to the new version.

Use Amazon CloudWatch metrics to monitor errors, latency, or other performance issues.

Roll back traffic to the previous version if any issues are detected.

```
aws lambda update-alias \
--function-name MyFunction \
--name MyAlias \
--routing-config '{"AdditionalVersionWeights": {"2": 0.10}}'
```

upvoted 2 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **Chakanetsa** 1 year, 5 months ago

Selected Answer: A

A. Create an alias for every new deployed version of the Lambda function. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load.

Explanation:

This option provides a granular level of control for canary deployments:

Versioning: Creating a new version for each deployment ensures that you have a clear record of changes.

Alias: An alias acts as a stable endpoint, allowing you to gradually shift traffic to the new version.

Routing configuration: The routing-config parameter provides fine-grained control over traffic distribution between versions.

By using this approach, you can gradually increase the percentage of traffic to the new version, monitor its performance, and roll back if necessary, minimizing the impact of potential issues.

upvoted 2 times

 **Chakanetsa** 1 year, 5 months ago

Breakdown of other options:

B: While Route 53 weighted routing can distribute traffic, it's less granular than using Lambda aliases and doesn't provide the same level of control.

C: Using the update-function-configuration command doesn't provide the flexibility to gradually shift traffic.

D: CodeDeploy is primarily for deploying code to EC2 instances, not for managing Lambda function traffic.

By using Lambda aliases and the routing-config parameter, you can effectively implement a canary release strategy for your Lambda functions.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: A

Not B. This introduces R53 in the scenario, but we are not sure if R53 fits in the scenario. To combine R53 and Lambda we should use function URL that is not mentioned and we don't know if the app is public. A lot of uncertainty here

Not C. routing-config is an Alias specific configuration aka Weighted Alias and it is not available for the update-function-configuration command <https://docs.aws.amazon.com/cli/latest/reference/lambda/update-function-configuration.html>

Not D. CodeDeployDefault.OneAtATime is a CodeDeploy option for EC2/on-premise, while in this scenario we need a canary option for Lambda such as CodeDeployDefault.LambdaCanary10Percent5Minutes

A does the job <https://docs.aws.amazon.com/cli/latest/reference/lambda/update-alias.html> and <https://docs.aws.amazon.com/lambda/latest/dg/configuration-aliases.html#configuring-alias-routing>
upvoted 1 times

JMAN1 2 years ago

100% A is correct. :) I was confused between D and A. But, this url says Codedeploye.AllatOnce deploy option is not for 'canary release'.
https://docs.aws.amazon.com/ko_kr/codedeploy/latest/userguide/deployment-configurations.html
upvoted 2 times

totten 2 years, 2 months ago

Selected Answer: A

Here's why Option A is suitable:

Create an alias: For every new version of your Lambda function, create an alias. Aliases allow you to associate a user-friendly name with a specific version of the function.

Routing configuration: AWS Lambda supports routing configurations that allow you to gradually shift traffic from one alias to another. Using the "routing-config" parameter with the AWS CLI "update-alias" command, you can specify how much traffic each alias should receive.

Gradual release: By configuring the routing, you can control the percentage of traffic directed to the new version (canary). You can gradually increase the traffic percentage as you gain confidence in the new release. If issues arise, you can quickly roll back by adjusting the routing configuration.

upvoted 3 times

Christina666 2 years, 5 months 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 years, 5 months ago

Selected Answer: A

D would be an optionn if used Lambda-specific config

upvoted 2 times

SkyZeroZx 2 years, 6 months 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 3 times

AMEJack 2 years, 7 months ago

Sorry OneAtTime

upvoted 1 times

AMEJack 2 years, 7 months ago

Selected Answer: A

CodeDeploy: Although CodeDeploy can help but AllAtOnce is not used for canary traffic shifting.
upvoted 1 times

God_Is_Love 2 years, 10 months 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 5 times

Question #61

Topic 1

A finance company hosts a data lake in Amazon S3. The company receives financial data records over SFTP each night from several third parties. The company runs its own SFTP server on an Amazon EC2 instance in a public subnet of a VPC. After the files are uploaded, they are moved to the data lake by a cron job that runs on the same instance. The SFTP server is reachable on DNS sftp.example.com through the use of Amazon Route 53.

What should a solutions architect do to improve the reliability and scalability of the SFTP solution?

- A. Move the EC2 instance into an Auto Scaling group. Place the EC2 instance behind an Application Load Balancer (ALB). Update the DNS record sftp.example.com in Route 53 to point to the ALB.
- B. Migrate the SFTP server to AWS Transfer for SFTP. Update the DNS record sftp.example.com in Route 53 to point to the server endpoint hostname.
- C. Migrate the SFTP server to a file gateway in AWS Storage Gateway. Update the DNS record sftp.example.com in Route 53 to point to the file gateway endpoint.
- D. Place the EC2 instance behind a Network Load Balancer (NLB). Update the DNS record sftp.example.com in Route 53 to point to the NLB.

Correct Answer: B

Community vote distribution

B (100%)

 **tinyflame** Highly Voted 2 years, 10 months ago

Selected Answer: B

A=ALB cannot be used with SFTP
B = Correct
C=Storage Gateway is not an SFTP Server
D=NLB can be used with SFTP, but EC2 is single
upvoted 31 times

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: B

Option B is the correct answer. Migrating the SFTP server to AWS Transfer for SFTP will improve the reliability and scalability of the SFTP solution. AWS Transfer for SFTP is a fully managed SFTP service that enables the company to transfer files directly into and out of Amazon S3 using the SFTP protocol. By using this service, the company can offload the management of the SFTP server to AWS, which will provide high availability, scalability, and security. The company can then update the DNS record sftp.example.com in Route 53 to point to the server endpoint hostname, which will ensure that the SFTP server is reachable on the DNS.

upvoted 14 times

 **masetromain** 2 years, 11 months ago

Option A, C and D do not provide the same level of scalability and reliability as AWS Transfer for SFTP. While placing the EC2 instance behind a load balancer can help improve availability, it will not necessarily improve scalability, and it would still require the company to manage the SFTP server. Option C , migrating the SFTP server to a file gateway in AWS Storage Gateway, would not necessarily improve the scalability and reliability of the SFTP solution, as it would still require the company to manage the SFTP server.

upvoted 4 times

 **rioisverycute** 2 years ago

How about the cron job?
upvoted 1 times

 **amministrazione** Most Recent 1 year, 3 months ago

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.
upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B of course
upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: B

keyword = AWS Transfer for SFTP
then B
upvoted 2 times

 **mfsec** 2 years, 9 months ago

Selected Answer: B

B is the way to go..

upvoted 3 times

Question #62

A company wants to migrate an application to Amazon EC2 from VMware Infrastructure that runs in an on-premises data center. A solutions architect must preserve the software and configuration settings during the migration.

What should the solutions architect do to meet these requirements?

- A. Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows File Server. Use the SMB share to host the VMware data store. Use VM Import/Export to move the VMs to Amazon EC2.
- B. Use the VMware vSphere client to export the application as an image in Open Virtualization Format (OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command.
- C. Configure AWS Storage Gateway for files service to export a Common Internet File System (CIFS) share. Create a backup copy to the shared folder. Sign in to the AWS Management Console and create an AMI from the backup copy. Launch an EC2 instance that is based on the AMI.
- D. Create a managed-instance activation for a hybrid environment in AWS Systems Manager. Download and install Systems Manager Agent on the on-premises VM. Register the VM with Systems Manager to be a managed instance. Use AWS Backup to create a snapshot of the VM and create an AMI. Launch an EC2 instance that is based on the AMI.

Correct Answer: B

Community vote distribution

B (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: B

The correct answer is B. Use the VMware vSphere client to export the application as an image in Open Virtualization Format (OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command. This approach allows the solutions architect to export the application as an image in OVF format, which preserves the software and configuration settings, and then import it into Amazon EC2 using the EC2 import command.

upvoted 15 times

 **sammyhaj** 1 year, 11 months ago

<https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

upvoted 3 times

 **masetromain** 2 years, 11 months ago

Option A is incorrect because it uses AWS DataSync and FSx for Windows File Server to replicate the data store, but it doesn't preserve the software and configuration settings of the application.

Option C is incorrect because it uses AWS Storage Gateway to export a CIFS share, but it doesn't preserve the software and configuration settings of the application.

Option D is incorrect because it uses AWS Systems Manager and AWS Backup to create a snapshot of the VM, but it doesn't preserve the software and configuration settings of the application.

upvoted 9 times

 **amministrazione** Most Recent 1 year, 3 months ago

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.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: B

A = SMB share cannot host VMware datastore. Also, installing agent modify configuration settings

B = correct

C = not clear how the backup copy is created and what format is used to allow then creating an AMI from it

D = hybrid activation allows SSM to manage on-premise / other cloud VM but doesn't enable AWS Backup. This instead requires a backup gateway to backup VMware environment <https://aws.amazon.com/blogs/storage/backup-and-restore-on-premises-vmware-virtual-machines-using-aws-backup/>

upvoted 2 times

 **SorenBendixen** 2 years, 4 months 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 3 times

 **Brightalw** 2 years, 4 months ago

what the B is wrong is that the VM format, should be OVA or VMDK or VHD, not OVF

upvoted 2 times

 **CuteRunRun** 2 years, 4 months ago

Selected Answer: B

I prefer B I do not know why the correct is D.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

it's a B

upvoted 1 times

 **rbm2023** 2 years, 7 months ago

Selected Answer: B

<https://www.learnitguide.net/2023/01/how-to-migrate-vmware-vm-to-aws-ec2.html>

upvoted 3 times

 **Brightalw** 2 years, 4 months ago

It said the VM fomat is OVA or VMDK, not OVF

upvoted 1 times

 **asifjanjua88** 2 years, 8 months ago

I vote to B. Why the admin has selected D as Answer.

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: B

B is the answer - OVF.

upvoted 2 times

 **God_Is_Love** 2 years, 10 months ago

Selected Answer: B

Use VM Import/Export. B is correct . <https://aws.amazon.com/ec2/vm-import/>

upvoted 4 times

 **God_Is_Love** 2 years, 10 months 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** 2 years, 11 months ago

Selected Answer: B

I vote B

<https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

upvoted 1 times

Question #63

Topic 1

A video processing company has an application that downloads images from an Amazon S3 bucket, processes the images, stores a transformed image in a second S3 bucket, and updates metadata about the image in an Amazon DynamoDB table. The application is written in Node.js and runs by using an AWS Lambda function. The Lambda function is invoked when a new image is uploaded to Amazon S3.

The application ran without incident for a while. However, the size of the images has grown significantly. The Lambda function is now failing frequently with timeout errors. The function timeout is set to its maximum value. A solutions architect needs to refactor the application's architecture to prevent invocation failures. The company does not want to manage the underlying infrastructure.

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

- A. Modify the application deployment by building a Docker image that contains the application code. Publish the image to Amazon Elastic Container Registry (Amazon ECR).
- B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargate. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- C. Create an AWS Step Functions state machine with a Parallel state to invoke the Lambda function. Increase the provisioned concurrency of the Lambda function.
- D. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of Amazon EC2. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- E. Modify the application to store images on Amazon Elastic File System (Amazon EFS) and to store metadata on an Amazon RDS DB instance. Adjust the Lambda function to mount the EFS file share.

Correct Answer: AB

Community vote distribution

AB (87%) 8%

 **zhangyu20000**  2 years, 11 months ago

A: create Docker image and save it to ECR
B: run this image on Fargate

No answer should have Lambda the will be time out
upvoted 27 times

 **masetromain** 2 years, 11 months ago

You are correct, both options A and B involve creating a Docker image of the application code and running it on Amazon Elastic Container Service (ECS) using either Fargate or EC2 as the launch type. These options would allow for more control over the resources allocated to the application and potentially prevent timeout errors. Option A is necessary to create the image and store it in a registry, and option B is necessary to run the image on Fargate which is a managed container orchestration service that eliminates the need for provisioning and scaling of the underlying infrastructure.

upvoted 9 times

 **GabrielShiao** 11 months, 1 week ago

While voting A and B, B doesn't really work because Lambda has reached the 15-minute timeout limitation.
upvoted 1 times

 **masetromain**  2 years, 11 months ago

Selected Answer: AB

The correct answer is A and B.

A. Modify the application deployment by building a Docker image that contains the application code. Publish the image to Amazon Elastic Container Registry (Amazon ECR).

- This step is necessary to package the application code in a container and make it available for running on ECS.

B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargate. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.

- This step is necessary to run the containerized application on Fargate, which is a fully managed container orchestration service that eliminates the need to provision and scale the underlying infrastructure.

upvoted 14 times

✉ **masetromain** 2 years, 11 months ago

Option C and E are not correct because they don't address the problem of timeout errors. AWS Step Functions and Amazon Elastic File System (EFS) are services that can be used to coordinate and manage workflows and file storage respectively, but they don't help with the specific problem of the Lambda function timing out.

Option D is not correct because AWS Fargate is a serverless compute engine for containers that eliminates the need for provisioning and scaling the underlying infrastructure.

It means that the company does not have to manage the underlying infrastructure, which is what the company wants.

upvoted 6 times

✉ **amministrazione** Most Recent 1 year, 3 months ago

- 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.

upvoted 1 times

✉ **MAZIADI** 1 year, 4 months ago

Selected Answer: AB

To be honest, I don't trust the examtopic answers anymore, we should only rely on most voted ones

upvoted 1 times

✉ **gofavad926** 1 year, 9 months ago

Selected Answer: AB

AB, ECR + ECS Margate

upvoted 1 times

✉ **Ak47g** 1 year, 12 months ago

Selected Answer: AB

A: create Docker image and save it to ECR

B: run this image on Fargate

upvoted 1 times

✉ **Nicoben** 2 years ago

Selected Answer: AB

A: create docker image and store in on ECR

B: run it on a AWS-managed infrastructure (as required)

upvoted 1 times

✉ **blackgamer** 2 years, 2 months ago

The correct answer is A and B. But Lambda function should be replaced with EventBridge.

upvoted 1 times

✉ **ggrodsckiy** 2 years, 2 months ago

Selected Answer: BC

B - 100%

C OR E ??

upvoted 1 times

✉ **CuteRunRun** 2 years, 4 months ago

Selected Answer: AB

I think is AB

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: AB

it's AB

upvoted 1 times

✉ **Jonalb** 2 years, 6 months ago

Selected Answer: AB

AB

its correct!

upvoted 1 times

✉ **SkyZeroZx** 2 years, 6 months 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** 2 years, 9 months ago

Selected Answer: B

A + B.

upvoted 2 times

 **dev112233xx** 2 years, 9 months ago

Selected Answer: AB

A+B makes sense to me

upvoted 2 times

 **God_Is_Love** 2 years, 10 months ago

Selected Answer: AB

Based on Serverless solutions used, need to go with Fargate in combination with either ECS/EC2. As company does not want to manage infra, we go for because Fargate-ECS combo as Fargate-EC2 needs more maintenance. That means D is out. E is obviously out. EFS does not contribute to Lambda invocation timeouts.

C is wrong because, increased concurrency (more Lambda versions) won't solve timeouts.

That leaves A and B as right answers.

upvoted 4 times

 **klog** 2 years, 10 months 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

Question #64

A company has an organization in AWS Organizations. The company is using AWS Control Tower to deploy a landing zone for the organization. The company wants to implement governance and policy enforcement. The company must implement a policy that will detect Amazon RDS DB instances that are not encrypted at rest in the company's production OU.

Which solution will meet this requirement?

- A. Turn on mandatory guardrails in AWS Control Tower. Apply the mandatory guardrails to the production OU.
- B. Enable the appropriate guardrail from the list of strongly recommended guardrails in AWS Control Tower. Apply the guardrail to the production OU.
- C. Use AWS Config to create a new mandatory guardrail. Apply the rule to all accounts in the production OU.
- D. Create a custom SCP in AWS Control Tower. Apply the SCP to the production OU.

Correct Answer: B*Community vote distribution*

B (94%)

6%

✉  **masetromain**  2 years, 11 months ago

Selected Answer: B

The correct answer is B. AWS Control Tower provides a set of "strongly recommended guardrails" that can be enabled to implement governance and policy enforcement. One of these guardrails is "Encrypt Amazon RDS instances" which will detect RDS DB instances that are not encrypted at rest. By enabling this guardrail and applying it to the production OU, the company will be able to enforce encryption for RDS instances in the production environment.

Option A is incorrect because mandatory guardrails are pre-defined by AWS and cannot be customized.

Option C is incorrect because AWS Config does not provide mandatory guardrails for RDS instances.

Option D is incorrect because AWS Control Tower does not provide a feature called custom SCP (Service Control Policy), it uses guardrails instead.

upvoted 20 times

✉  **pitakk**  2 years, 11 months ago

Selected Answer: B

<https://docs.aws.amazon.com/controlltower/latest/userguide/strongly-recommended-controls.html#disallow-rds-storage-unencrypted>

upvoted 5 times

✉  **Musk** 2 years, 11 months ago

The only thing is that this option talks about guardrails, while the article talks about controls, not mandatory.

upvoted 1 times

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

Selected Answer: B

This approach leverages Control Tower's detective guardrails, which use AWS Config behind the scenes, and is designed specifically to detect resource misconfigurations like unencrypted RDS, making it the best solution.

upvoted 1 times

✉  **pk0619** 1 year ago

Selected Answer: B

Guardrails are now called Controls in Control Tower.

upvoted 1 times

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

B. Enable the appropriate guardrail from the list of strongly recommended guardrails in AWS Control Tower. Apply the guardrail to the production OU.

upvoted 1 times

✉  **AloraCloud** 1 year, 5 months ago

The keyword in the question is detect which indicates Config.

"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."

upvoted 1 times

✉  **8608f25** 1 year, 10 months ago

Selected Answer: B

Option B is correct because AWS Control Tower's strongly recommended guardrails include checks for best practices and additional security measures that are not enforced by default but are highly recommended. Among these, there is likely a guardrail that can detect unencrypted RDS DB instances, aligning with the company's requirement. Applying this guardrail to the production OU will ensure that all RDS DB instances in that OU are checked for encryption at rest.

upvoted 1 times

 ninomfr64 1 year, 11 months ago

Selected Answer: B

A = Mandatory controls are owned by AWS Control Tower, and they apply by default to every OU on your landing zone and they can't be deactivated

B = correct <https://docs.aws.amazon.com/controlltower/latest/userguide/strongly-recommended-controls.html#disallow-rds-storage-unencrypted>

C = You cannot create new mandatory controls as they are owned by AWS Control Tower

D = You can create custom SCP in AWS Control Tower as part of the Customizations for AWS Control Tower

<https://docs.aws.amazon.com/controlltower/latest/userguide/cfcn-set-up-custom-scps.html> However this requires a lot of work

upvoted 3 times

 ninomfr64 1 year, 11 months ago

Note on D, the question is asking to detect and not to mandate, thus D would not meet requirement

upvoted 3 times

 severlight 2 years, 1 month ago

Selected Answer: B

check masetromain's comment

upvoted 1 times

 dkx 2 years, 5 months 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 4 times

 NikkyDicky 2 years, 5 months ago

Selected Answer: B

It's. B

upvoted 1 times

 SkyZeroZx 2 years, 6 months ago

Selected Answer: B

A seems but previous exist rule

then B is more appropriate in this case

<https://docs.aws.amazon.com/controlltower/latest/userguide/strongly-recommended-controls.html#disallow-rds-storage-unencrypted>

upvoted 1 times

 EricZhang 2 years, 7 months ago

C - using AWS Config for detective action

upvoted 2 times

 OCHT 2 years, 8 months 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 3 times

 passthatexam1 2 years, 8 months ago

It's incorrect ideally you only apply to the OU and not to an individual account, therefore this needs to be discounted.

upvoted 1 times

 mfsec 2 years, 9 months ago

Selected Answer: B

Enable the appropriate guardrail

upvoted 2 times

 **Ajani** 2 years, 9 months 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/controlltower/latest/userguide/rds-rules.html#ct-rds-pr-16-description>

Optional controls are OU specific.

upvoted 4 times

 **God_Is_Love** 2 years, 10 months 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

Question #65

Topic 1

A startup company hosts a fleet of Amazon EC2 instances in private subnets using the latest Amazon Linux 2 AMI. The company's engineers rely heavily on SSH access to the instances for troubleshooting.

The company's existing architecture includes the following:

- A VPC with private and public subnets, and a NAT gateway.
- Site-to-Site VPN for connectivity with the on-premises environment.
- EC2 security groups with direct SSH access from the on-premises environment.

The company needs to increase security controls around SSH access and provide auditing of commands run by the engineers.

Which strategy should a solutions architect use?

- A. Install and configure EC2 Instance Connect on the fleet of EC2 instances. Remove all security group rules attached to EC2 instances that allow inbound TCP on port 22. Advise the engineers to remotely access the instances by using the EC2 Instance Connect CLI.
- B. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs.
- C. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Enable AWS Config for EC2 security group resource changes. Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules.
- D. Create an IAM role with the AmazonSSMManagedInstanceCore managed policy attached. Attach the IAM role to all the EC2 instances. Remove all security group rules attached to the EC2 instances that allow inbound TCP on port 22. Have the engineers install the AWS Systems Manager Session Manager plugin for their devices and remotely access the instances by using the start-session API call from Systems Manager.

Correct Answer: D*Community vote distribution*

D (91%) 9%

 **masetromain**  2 years, 11 months ago

Selected Answer: D

The correct answer is D. This strategy uses IAM roles and AWS Systems Manager to provide secure and auditable SSH access to the instances. The IAM role is attached to all the EC2 instances and has the AmazonSSMManagedInstanceCore managed policy attached, which allows the instances to be managed by Systems Manager. The engineers then install the AWS Systems Manager Session Manager plugin for their devices and remotely access the instances by using the start-session API call from Systems Manager. This approach provides secure and auditable access to the instances without the need for IP-based security group rules or additional infrastructure.

upvoted 20 times

 **masetromain** 2 years, 11 months ago

Option A uses EC2 Instance Connect to provide secure and auditable SSH access to the instances, but it requires additional infrastructure and configuration.

Option B provides auditing of commands run by the engineers, but it relies on IP-based security group rules, which can be difficult to manage and may not be as secure as using IAM roles.

Option C uses AWS Config and Firewall Manager to automatically remediate changes to security group rules, but it still relies on IP-based security group rules and does not provide an auditable method of access to the instances.

upvoted 4 times

 **masetromain** 2 years, 11 months ago

For option A to work, the following additional infrastructure and configuration would be required:

The EC2 Instance Connect service needs to be enabled in the AWS account and the appropriate IAM permissions would need to be granted to the engineers.

The EC2 instances would need to have the EC2 Instance Connect agent installed and configured.

The engineers would need to install the EC2 Instance Connect CLI on their devices and have the necessary credentials to authenticate with AWS.

In addition, the company would need to update their processes and procedures to ensure that engineers are only using EC2 Instance Connect to access the instances and that all access is being logged and audited.

upvoted 4 times

✉  **adrian202** 2 years ago

The key factor is that Option A explains to remove the port 22 inbound SSH access security group, they would need to keep that present: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-prerequisites.html>

upvoted 3 times

✉  **God_Is_Love**  2 years, 10 months 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 11 times

✉  **kgpoj** 1 year, 3 months ago

The explanation for A is wrong.

AWS EC2 Instance Connect does support auditing.

upvoted 1 times

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

Selected Answer: D

Use AWS Systems Manager Session Manager to securely access EC2 instances without SSH.

This enhances security by eliminating port 22 access and enables auditing of all commands run when logs are configured to go to CloudWatch Logs or S3.

This approach satisfies both security and compliance needs in a fully managed, serverless manner.

upvoted 1 times

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

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.

upvoted 1 times

✉  **gofavad926** 1 year, 9 months ago

Selected Answer: D

D, use SSM

upvoted 1 times

✉  **8608f25** 1 year, 10 months ago

Selected Answer: D

Option D is the best strategy because it leverages AWS Systems Manager Session Manager, which allows for secure instance management without the need for SSH access. By attaching an IAM role with the AmazonSSMManagedInstanceCore policy to EC2 instances, engineers can use Session Manager for shell access to instances without needing to open port 22, significantly enhancing security. Session Manager also automatically logs session activity to S3 or CloudWatch Logs, providing the required command auditing capability. This eliminates the need for direct SSH access and offers a centralized, secure, and audited method for engineers to access and run commands on instances.

upvoted 2 times

✉  **rioisverycute** 2 years ago

Selected Answer: B

It required to increase security around ssh access, why so many people voted on D?

upvoted 1 times

✉  **djeong95** 1 year, 10 months ago

Cloudwatch agent does not provide auditable logs for SSH sessions; it only provides metrics about CPU/Memory/Network Packets/etc; nothing about what user started session at what time and ran certain trackable API calls while in that session.

upvoted 1 times

✉  **Chung234** 2 years, 2 months ago

The answer is D. Option A is wrong because EC2 Instance Connect requires the host security group to permit SSH traffic inbound. <https://repost.aws/questions/QUnV4R9EoeSdW0GT3cKBUR7w/what-is-the-difference-between-ec2-instance-connect-and-session-manager-ssh-connections>

upvoted 2 times

✉  **NikkyDicky** 2 years, 5 months ago

Selected Answer: D

It's D

upvoted 1 times

✉️ **SkyZeroZx** 2 years, 6 months ago

Selected Answer: D

keyword = AWS Systems Manager Session Manager
then D

upvoted 1 times

✉️ **mfsec** 2 years, 9 months ago

Selected Answer: D

D for sure.

upvoted 2 times

✉️ **Ajani** 2 years, 9 months ago

Why its NOT A

To connect using the Amazon EC2 console, the instance must have a public IPv4 address.

If the instance does not have a public IP address, you can connect to the instance over a private network using an SSH client or the EC2 Instance Connect CLI. For example, you can connect from within the same VPC or through a VPN connection, transit gateway, or AWS Direct Connect.

EC2 Instance Connect does not support connecting using an IPv6 address.

going with D:

upvoted 2 times

✉️ **lygf** 2 years, 10 months ago

Selected Answer: D

Need to be able to audit the commands ran on the machine.

upvoted 2 times

✉️ **DWsk** 2 years, 10 months ago

I don't understand why it can't be A for this one. Why is AWS Systems Manager Session better than EC2 Instance Connect? They both require installing something on the instances.

upvoted 1 times

✉️ **lygf** 2 years, 10 months ago

Could option A audit the commands ran on the server, as required by the question? I knew D certainly can.

upvoted 1 times

✉️ **anita_student** 2 years, 9 months ago

For EC2 instance connect there are a few requirements:

- instance has public IP (the instances in question are private)
- you have port 22 open (A says remove port 22 inbound)

upvoted 4 times

✉️ **moota** 2 years, 10 months 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** 2 years, 10 months ago

Selected Answer: B

provide auditing of commands run by the engineers = B Only

upvoted 3 times

✉️ **joefrommc** 2 years, 4 months ago

Read docs you can audit command using SSM <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging.html>

upvoted 1 times

✉️ **rif** 2 years, 2 months ago

"In addition to providing information about current and completed sessions in the Systems Manager console, Session Manager provides you with the ability to audit session activity in your AWS account using AWS CloudTrail"

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

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

upvoted 1 times

Question #66

A company that uses AWS Organizations allows developers to experiment on AWS. As part of the landing zone that the company has deployed, developers use their company email address to request an account. The company wants to ensure that developers are not launching costly services or running services unnecessarily. The company must give developers a fixed monthly budget to limit their AWS costs.

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

- A. Create an SCP to set a fixed monthly account usage limit. Apply the SCP to the developer accounts.
- B. Use AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process.
- C. Create an SCP to deny access to costly services and components. Apply the SCP to the developer accounts.
- D. Create an IAM policy to deny access to costly services and components. Apply the IAM policy to the developer accounts.
- E. Create an AWS Budgets alert action to terminate services when the budgeted amount is reached. Configure the action to terminate all services.
- F. Create an AWS Budgets alert action to send an Amazon Simple Notification Service (Amazon SNS) notification when the budgeted amount is reached. Invoke an AWS Lambda function to terminate all services.

Correct Answer: BCF*Community vote distribution*

BCF (81%) Other

 **spd** Highly Voted 2 years, 10 months ago

Selected Answer: BCF

Clear - BCF - SCP is preferable over IAM
upvoted 20 times

 **kiran15789** Highly Voted 2 years, 10 months ago

Selected Answer: BCF

I prefer D over C as IAM cant be applied to Account
upvoted 16 times

 **AWSum1** 1 year, 3 months ago

Option D says apply it to the Developers accounts. Unnecessary operational overhead
upvoted 1 times

 **princajen** Most Recent 5 months, 2 weeks ago

Selected Answer: BCF

To enforce a fixed monthly budget for developer accounts:

Use AWS Budgets to define monthly cost thresholds (B).

Apply SCPs to developer accounts to restrict access to expensive services up front (C).

Use AWS Budgets alert actions to trigger SNS > Lambda workflows that can stop services once budget limits are reached (F).

This approach combines cost visibility, preventive controls, and automated enforcement — all without managing infrastructure manually.
upvoted 1 times

 **vda2024** 1 year, 1 month ago

Fixed monthly budget> implement AWS budget. hence B is correct.
Prevent running unnecessary services> implement SCP. hence C is correct.
on F: I'm just not sure why do we want to terminate all resources and why not just don't let them run additional.
upvoted 2 times

 **amministrazione** 1 year, 3 months ago

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.
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 1 times

 **MAZIADI** 1 year, 4 months ago

Selected Answer: BCF

Why Option C is Preferred to D :

Centralized Control: SCPs provide a centralized way to manage permissions across all accounts in an organization, ensuring consistent enforcement of policies.

Scalability: SCPs are easier to manage and scale when dealing with multiple accounts, as changes to the SCP will automatically apply to all accounts under the organization.

Compliance: SCPs help ensure compliance with organizational policies by preventing the use of restricted services across all accounts.

upvoted 2 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: BCF

BCF - SCP, budget and custom lambda to terminate services

upvoted 2 times

 **wooin992** 1 year, 9 months ago

Selected Answer: BDF

BDF

cannot apply scp in account, need to apply it in OU

upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

wrong, you can apply scp to an account

upvoted 2 times

 **8608f25** 1 year, 10 months ago

Selected Answer: BCF

B. Use AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process. AWS Budgets allows you to set custom cost and usage budgets that alert you when you exceed your thresholds.

C. Create an SCP to deny access to costly services and components. Apply the SCP to the developer accounts. By creating an SCP that specifically denies access to costly AWS services, the company can prevent developers from launching such services, thereby helping to keep costs within the fixed monthly budget.

F. Create an AWS Budgets alert action to send an Amazon Simple Notification Service (Amazon SNS) notification when the budgeted amount is reached. Invoke an AWS Lambda function to terminate all services. While AWS Budgets cannot directly terminate services when a budget is exceeded, you can configure an alert to trigger a notification. This notification can then invoke a Lambda function designed to assess and terminate services as necessary, based on the company's policies.

upvoted 2 times

 **duriselvan** 1 year, 11 months ago

Setting a monthly cost budget with a variable target amount, with each subsequent month growing the budget target by 5 percent. Then, you can configure your notifications for 80 percent of your budgeted amount and apply an action. For example, you could automatically apply a custom IAM policy that denies you the ability to provision additional resources within an account.

<https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html>

ans :bdf

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: BCF

A = SCP is used to limit permission that administrator can grant IAM users/roles, SCP cannot set a fixed monthly account usage limit

B = correct

C = correct

D = it could work, but it would require more work wrt SCP

E = Budget actions cannot terminate all kind of services, actually supports 3 types of actions 1/ apply IAM policy to IAM identities, 2/ apply SCP to an OU and 3/ terminate EC2 and RDS instances

F = correct

upvoted 3 times

 **jpa8300** 1 year, 12 months ago

Selected Answer: BDF

Although, C is correct, some people here says that SCP cannot be attached to an account, but it is not true, you can, the most common option when we want to deny permissions to an account is to use an IAM policy.

upvoted 1 times

 **rif** 2 years, 2 months ago

BCF.

In Option D, we can not apply IAM policy to an AWS Account.

upvoted 1 times

 **SK_Tyagi** 2 years, 4 months ago

Selected Answer: BDF

I'd go with BDF, since there's no mention of OU. As a rule of thumb, IAM policies to restrict are applied on Accounts, Users, Groups and SCP's on OU's.

upvoted 4 times

 **vn_thanh tung** 2 years, 4 months ago

IAM policies for user ? <https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies-overview.html>

upvoted 1 times

vn_thanh tung 2 years, 4 months ago

Sorry I mistake, IAM policies can applied on User.
upvoted 1 times

CuteRunRun 2 years, 4 months 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 2 times

NikkyDicky 2 years, 5 months ago

Selected Answer: BCF

It's a BCF
upvoted 2 times

PhuocT 2 years, 6 months ago

Selected Answer: BCF

C - SCP would be prefer to control the services could be used in Organization's AWS accounts.
upvoted 2 times

Question #67

Topic 1

A company has applications in an AWS account that is named Source. The account is in an organization in AWS Organizations. One of the applications uses AWS Lambda functions and stores inventory data in an Amazon Aurora database. The application deploys the Lambda functions by using a deployment package. The company has configured automated backups for Aurora.

The company wants to migrate the Lambda functions and the Aurora database to a new AWS account that is named Target. The application processes critical data, so the company must minimize downtime.

Which solution will meet these requirements?

- A. Download the Lambda function deployment package from the Source account. Use the deployment package and create new Lambda functions in the Target account. Share the automated Aurora DB cluster snapshot with the Target account.
- B. Download the Lambda function deployment package from the Source account. Use the deployment package and create new Lambda functions in the Target account. Share the Aurora DB cluster with the Target account by using AWS Resource Access Manager (AWS RAM). Grant the Target account permission to clone the Aurora DB cluster.
- C. Use AWS Resource Access Manager (AWS RAM) to share the Lambda functions and the Aurora DB cluster with the Target account. Grant the Target account permission to clone the Aurora DB cluster.
- D. Use AWS Resource Access Manager (AWS RAM) to share the Lambda functions with the Target account. Share the automated Aurora DB cluster snapshot with the Target account.

Correct Answer: B*Community vote distribution*

B (93%) 4%

✉  **masetromain**  2 years, 11 months ago

Selected Answer: B

The correct answer is option B. This solution uses a combination of AWS Resource Access Manager (RAM) and automated backups to migrate the Lambda functions and the Aurora database to the Target account while minimizing downtime.

In this solution, the Lambda function deployment package is downloaded from the Source account and used to create new Lambda functions in the Target account. The Aurora DB cluster is shared with the Target account using AWS RAM and the Target account is granted permission to clone the Aurora DB cluster, allowing for a new copy of the Aurora database to be created in the Target account. This approach allows for the data to be migrated to the Target account while minimizing downtime, as the Target account can use the cloned Aurora database while the original Aurora database continues to be used in the Source account.

upvoted 22 times

✉  **masetromain** 2 years, 11 months ago

Option A is not the best solution because it doesn't share the Aurora DB cluster with the Target account and this would cause data inconsistencies as the Source and Target accounts would not share the same data.

Option C is not the best solution because, it does not specify how the data will be migrated and it would cause downtime as the Source and Target accounts are not sharing the same data.

Option D is not the best solution because it does not specify how the Lambda function will be migrated and it would cause data inconsistencies as the Source and Target accounts are not sharing the same data.

upvoted 2 times

✉  **lxrdm** 2 years, 5 months 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 4 times

✉  **Simon523**  2 years, 4 months 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 18 times

 **princajen** Most Recent 5 months, 2 weeks ago

Selected Answer: B

To migrate Lambda functions and Aurora DB clusters to a new AWS account with minimal downtime:

Lambda Migration:

Export or reuse the deployment package from the Source account.

Recreate the Lambda function in the Target account.

Aurora Migration:

Use AWS Resource Access Manager (RAM) to share the Aurora DB cluster with the Target account.

Use cross-account cloning to create a copy of the DB cluster in the Target account.

This allows the original to remain active while the Target account prepares the new copy — minimizing downtime.

upvoted 1 times

 **JOJ09** 1 year ago

Selected Answer: A

Lambda function and Aurora cluster can NOT be shared with RAM!

upvoted 3 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: B

A is viable, but as AWS RAM can share Aurora clusters, B is faster. However, AWS RAM can't share lambdas, so C and D are out.

upvoted 3 times

 **mnsait** 1 year, 1 month ago

Option A is NOT viable. As @lxrdm has pointed out with documentation, it is not possible to share 'automated' db cluster snapshots.

upvoted 1 times

 **Dgix** 1 year, 9 months ago

B, C, and D are all out since AWS RAM cannot share either Lambdas or Aurora DB clusters. A is the only viable one - you must use a manual snapshot for the DB, share it, and redeploy any deployment package in the destination account. (The question tries to trip you up by its wording: lambda deployments can't be downloaded, but the same deployment packages used to deploy the lambdas can, for instance from S3 or from source)

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: B

Option B is the most accurate and efficient solution based on this AWS article content (https://aws.amazon.com/about-aws/whats-new/2019/07/amazon_aurora_supportscloningacrossawsaccounts-/). It correctly outlines the steps for Lambda migration and utilizes the Aurora DB cluster cloning feature across accounts via AWS RAM, which aligns with the article's description. This approach ensures minimal downtime and efficient migration by allowing direct cloning of the Aurora database.

Option C incorrectly suggests using AWS RAM to share Lambda functions, which is not supported yet based on latest sharable AWS resources: <https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

upvoted 2 times

 **master9** 1 year, 11 months ago

Selected Answer: C

AWS Resource Access Manager (RAM) to share AWS Lambda functions and Aurora DB clusters with another AWS account. AWS RAM allows you to share resources that are created and managed by other AWS services with individual AWS accounts or with the accounts in an organization or organizational units (OUs) in AWS Organizations.

To share a Lambda function with another AWS account, you can delegate access to an IAM user (or all users) in the other AWS account so that they can assume a role in your account and invoke the Lambda function in your account.

To share an Aurora DB cluster with another AWS account, you can create a resource share in AWS RAM and specify the Amazon Resource Name (ARN) of the Aurora DB cluster as the resource to share. You can then specify the AWS account IDs of the accounts with which you want to share the resource.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: B

A = you can share snapshot to restore DB, but this will introduce some downtime
B = correct (cloning a DB allows for very limited downtime)
C = if you only share Lambda you are not migrating it, also it appears the Lambda is not a RAM sharable resource
<https://docs.aws.amazon.com/ram/latest/userguide/getting-started-sharing.html>
D = it appears the Lambda is not a RAM sharable resource and you cannot directly share an automated snapshot, you need first to create a manual snapshot by copying the automated snapshot, and then share that copy
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-share-snapshot.html>

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

A is not correct as you cannot directly share an automated snapshot, you need first to create a manual snapshot by copying the automated snapshot, and then share that copy <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-share-snapshot.html>

upvoted 1 times

 **learnwithaniket** 1 year, 12 months ago

Selected Answer: B

There is limit on the number of resources you can share with AWS RAM.

AWS RAM does not support direct sharing of Lambda functions between accounts.

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

it's B.

In A - automated snapshots are not shareable

upvoted 2 times

 **Maria2023** 2 years, 6 months 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** 2 years, 6 months ago

Selected Answer: B

The correct answer is option B. This solution uses a combination of AWS Resource Access Manager (RAM) and automated backups to migrate the Lambda functions and the Aurora database to the Target account while minimizing downtime.

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months 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** 2 years, 6 months 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** 2 years, 7 months ago

Selected Answer: B

The question is about migration and not sharing, so the answer is how to use a RAM feature to help you on the migration. In option D they are not migrating anything, both Lambda and Aurora are being shared with the Target account and not migrated. In option C is a similar situation, the Lambda is not being migrated. Option A seems a good option but might cause a larger downtime. Hence option D is more appropriate because you can use the cluster share with the Target account and clone the database cluster into it. In my view this answer should contemplate in which moment the cutoff from Source to Target would occur.

upvoted 3 times

 **takecoffee** 2 years, 8 months ago

Selected Answer: B

You can share the following Amazon Aurora resources by using AWS RAM.

upvoted 2 times

Question #68

Topic 1

A company runs a Python script on an Amazon EC2 instance to process data. The script runs every 10 minutes. The script ingests files from an Amazon S3 bucket and processes the files. On average, the script takes approximately 5 minutes to process each file. The script will not reprocess a file that the script has already processed.

The company reviewed Amazon CloudWatch metrics and noticed that the EC2 instance is idle for approximately 40% of the time because of the file processing speed. The company wants to make the workload highly available and scalable. The company also wants to reduce long-term management overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the data processing script to an AWS Lambda function. Use an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure Amazon S3 to send event notifications to the SQS queue. Create an EC2 Auto Scaling group with a minimum size of one instance. Update the data processing script to poll the SQS queue. Process the S3 objects that the SQS message identifies.
- C. Migrate the data processing script to a container image. Run the data processing container on an EC2 instance. Configure the container to poll the S3 bucket for new objects and to process the resulting objects.
- D. Migrate the data processing script to a container image that runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Create an AWS Lambda function that calls the Fargate RunTaskAPI operation when the container processes the file. Use an S3 event notification to invoke the Lambda function.

Correct Answer: A

Community vote distribution

A (72%)

D (28%)

 **masetromain**  2 years, 11 months ago

Selected Answer: A

The correct answer is A, migrating the data processing script to an AWS Lambda function and using an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects. This solution meets the company's requirements of high availability and scalability, as well as reducing long-term management overhead, and is likely to be the most cost-effective option.

Option B involves creating an SQS queue and configuring S3 to send event notifications to it. The data processing script would then poll the SQS queue and process the S3 objects that the SQS message identifies. While this option also provides high availability and scalability, it is less cost-effective than using Lambda, as it requires additional resources such as an SQS queue and an EC2 Auto Scaling group.

upvoted 23 times

 **hamimelon** 2 years, 3 months ago

Agree. Also, it says the company does not wanna manage long-term overhead, which points to serverless.

upvoted 3 times

 **dpatra** 2 years, 2 months ago

SQS is out of the question because the script already has a built in logic that will prevent it to reprocess a message that's already been processed

upvoted 1 times

 **masetromain** 2 years, 11 months ago

Option C, migrating the data processing script to a container image and running it on an EC2 instance, would still require the company to manage the underlying EC2 instances and may not be as cost-effective as using Lambda.

Option D, migrating the data processing script to a container image that runs on Amazon ECS on AWS Fargate, would still require the company to manage the underlying infrastructure and may not be as cost-effective as using Lambda. Additionally, it introduces additional complexity by adding a Lambda function that calls the Fargate RunTask API operation.

upvoted 5 times

 **red_panda** 1 year, 9 months ago

ECS in Fargate mode you don't need to manage anything underling infra!

You're totally forgot about cost, for sure running an ECS Fargate has lower cost than running a Lambda for 5 minutes every 10 minutes!

Also the function to trigger the ECS workload (in option D), running for milliseconds (as need only to notify the doc upload in S3), so it's more correct the D answer.

Ask to any Gen AI model, you will have mine answer with more details :)

upvoted 1 times

 **NirvanaSNM** 1 year, 5 months ago

Use an S3 event notification to invoke the Lambda function to process the objects
upvoted 1 times

 **zhangyu20000**  2 years, 11 months ago

A is correct, it provide HA, scale, less management. Task only need 5 minutes
B: enen more complex
C: container still run on one EC2, not scale
d: need container, Farget and Lambda. Complex than A
upvoted 7 times

 **princajen**  5 months, 2 weeks ago

Selected Answer: A

AWS Lambda with S3 event notification is the most cost-effective, highly available, and scalable option for short-lived, event-driven tasks like file processing. It eliminates EC2 idle time, reduces operational overhead, and fits within Lambda's time and memory limits. This architecture minimizes cost while maximizing simplicity and resilience.

upvoted 1 times

 **5e8c031** 5 months, 3 weeks ago

Selected Answer: A

I ran the numbers in the cost calculator and it turns out D is 10 times more expensive than A...

upvoted 1 times

 **5e8c031** 5 months, 3 weeks ago

Selected Answer: A

Given the discussion here, I used the cost calculator to estimate the cost of A and D.

D is indeed much more costly than A

D: 44 USD

A: 3 USD

upvoted 1 times

 **RB100** 7 months ago

Selected Answer: A

The Lambda solution (Option A) provides the most efficient, cost-effective, and manageable solution while meeting all requirements for high availability and scalability with minimal operational overhead.

upvoted 1 times

 **albert_kuo** 9 months, 4 weeks ago

Selected Answer: A

```
+-----+
| Amazon S3 |
| (Stores Uploaded Files)|
+-----+
|
| (S3 Event Notification)
v
+-----+
| AWS Lambda |
| (Processes Files) |
+-----+
|
| (Processed Data)
v
+-----+
| Amazon S3 |
| (Stores Processed Data)|
```

upvoted 1 times

 **SIJUTHOMASP** 1 year, 1 month ago

Option with Lambda would be more reasonable because the rational behind the cost on the solution would be triggering lambda on the S3 event. The current behaviour is 40% of EC2 being not utilised so that Option D to run in ECS with Fargate would be costlier than Lambda option here

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

Selected Answer: A

instead of scheduled 10 min with multiple files processing (each takes 5 minutes) it will be event driven with lambda each time a file is uploaded --> Answer A

upvoted 1 times

 **zolthar_z** 1 year, 5 months ago

Selected Answer: A

A, the company wants to reduce management overhead not costs, we should stay with the question requirement, it doesn't say anything about cost, probably D will be cheaper but the solution must resolve the question necessity and is reduce long-term management overhead

upvoted 2 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: D

I vote D because the service is from EC2 to lambda and work is processing data. Without given how big is the data we can't assume that the data is always below the lambda ephemeral storage limit 0.5GB. Nowadays, a file can easily break 0.5GB.

While D is still EC2 based so whatever previous EC2 can do farget can do as well.

upvoted 1 times

 **Shenannigan** 1 year, 6 months ago

Selected Answer: A

The answer is A:

AWS Pricing Calculator

(using:

10,000 request per month,

300,000 ms which = 5 minutes

128 MB of Memory

512 MB of Storage

)

Amount of memory allocated: 128 MB x 0.0009765625 GB in a MB = 0.125 GB

Amount of ephemeral storage allocated: 512 MB x 0.0009765625 GB in a MB = 0.5 GB

Pricing calculations

10,000 requests x 300,000 ms x 0.001 ms to sec conversion factor = 3,000,000.00 total compute (seconds)

0.125 GB x 3,000,000.00 seconds = 375,000.00 total compute (GB-s)

375,000.00 GB-s x 0.0000166667 USD = 6.25 USD (monthly compute charges)

10,000 requests x 0.0000002 USD = 0.00 USD (monthly request charges)

0.50 GB - 0.5 GB (no additional charge) = 0.00 GB billable ephemeral storage per function

Lambda costs - Without Free Tier (monthly): 6.25 USD

For those thinking D is the cheaper option, do you really believe ECS Fargate would be cheaper?

upvoted 2 times

 **red_panda** 1 year, 9 months ago

Selected Answer: D

Ok I was thinking between A and D.

I'm pretty sure which is D our answer, see the details.

The requirements are:

- COST as much as possible low

- OPERATIONS as much as possible managed.

So at the first reading, the A option seems to be the correct option (because it's totally AWS managed), but here we're totally forgot the cost.

Running a Lambda function, for 5 minutes every 10 minutes, it's very very more expensive than a simple ECS task running continuously.

Finally, ECS in fargate mode is totally AWS managed, so we will have lower cost, and a serverless and HA environment, which auto-scale if we need more processing at time.

For me, option D is the correct answer.

upvoted 3 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A, use lambda function is much cost-effective than use ECS Margate

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: A

Option A is the most cost-effective and efficient solution. AWS Lambda allows for running code in response to triggers such as S3 event notifications without the need to manage servers, thereby directly addressing the requirement to reduce long-term management overhead. Since the script is only needed when new files are uploaded and takes about 5 minutes to process each file, Lambda's ability to scale automatically and its billing model based on actual compute time used make it an ideal solution. Lambda can process files immediately upon upload, maximizing efficiency and minimizing idle time.

Option D proposes using Amazon ECS on AWS Fargate with Lambda to trigger tasks. This solution introduces container orchestration, which can improve scalability and reduce some management overhead. However, it is not as cost-effective as directly invoking a Lambda function to process files, considering the lightweight nature of the task and the added complexity of managing container orchestration and Lambda functions together.

upvoted 1 times

 **LazyAutonomy** 1 year, 11 months ago

Selected Answer: D

100% the answer is D.

5 minutes to process EACH FILE? And the EC2 instance is processing files 60% of the time?

Lambda would be crazy expensive in this scenario. ECS/Fargate = cheaper for sure. See link in @covabix879 comment for proof of this.

Greyeye said something rather ridiculous: "If you get 1000 images, you will see 1000 tasks. That is not economical or cheap."

How can 1x EC2 instance running a script every 10 minutes process 1000 images with each one taking 5 minutes? Even if the script processed images in parallel, e.g. one image per vCPU at a time, that instance would need 500 vCPUs! For the EC2 instance to be idle 40% of the time, it would need 833 vCPUs. That's ridiculous.

But even if 1000 images suddenly appeared, the Lambda solution would still result in 1000 Lambdas all firing and running for 5 minutes each. Which is going to be more expensive than ECS/Fargate.

upvoted 2 times

Question #69

Topic 1

A financial services company in North America plans to release a new online web application to its customers on AWS. The company will launch the application in the us-east-1 Region on Amazon EC2 instances. The application must be highly available and must dynamically scale to meet user traffic. The company also wants to implement a disaster recovery environment for the application in the us-west-1 Region by using active-passive failover.

Which solution will meet these requirements?

- A. Create a VPC in us-east-1 and a VPC in us-west-1. Configure VPC peering. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs. Place the Auto Scaling group behind the ALB.
- B. Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC. Place the Auto Scaling group behind the ALB. Set up the same configuration in the us-west-1 VPC. Create an Amazon Route 53 hosted zone. Create separate records for each ALB enable health checks to ensure high availability between Regions.
- C. Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC. Place the Auto Scaling group behind the ALB. Set up the same configuration in the us-west-1 VPC. Create an Amazon Route 53 hosted zone. Create separate records for each ALB. Enable health checks and configure a failover routing policy for each record.
- D. Create a VPC in us-east-1 and a VPC in us-west-1. Configure VPC peering. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs. Place the Auto Scaling group behind the ALB. Create an Amazon Route 53 hosted zone. Create a record for the ALB.

Correct Answer: C

Community vote distribution

C (100%)

 **masetromain**  2 years, 11 months ago

Selected Answer: C

The correct answer is C. Choice C meets the requirements for the application to be highly available and to dynamically scale to meet user traffic, as well as implementing a disaster recovery environment in the us-west-1 Region through active-passive failover.

In choice C, the company creates a VPC in us-east-1 and a VPC in us-west-1, and sets up an Application Load Balancer (ALB) and Auto Scaling group in both VPCs. The ALB extends across multiple Availability Zones in each VPC, and the Auto Scaling group deploys the EC2 instances across these Availability Zones. The Auto Scaling group is placed behind the ALB, which allows for automatic scaling of the instances to meet user traffic.

An Amazon Route 53 hosted zone is also created, with separate records for each ALB. Health checks are enabled for each record, and a failover routing policy is configured. This allows for active-passive failover between the two regions, ensuring high availability for the application.

upvoted 19 times

 **masetromain** 2 years, 11 months ago

Choice A, B, and D do not fully meet the requirements of the disaster recovery environment in the us-west-1 Region and the failover routing policy because they do not include the necessary configurations for active-passive failover.

In choice A, the VPCs in us-east-1 and us-west-1 are peered and the Auto Scaling group and Application Load Balancer (ALB) are extended across multiple availability zones in both regions. However, there is no explicit failover routing policy configured, so it is not clear how the application would failover to the us-west-1 region in the event of an outage.

Choice B, the VPCs in us-east-1 and us-west-1 are separate, and the configuration is replicated in both regions but there is no explicit failover routing policy configured, so it is not clear how the application would failover to the us-west-1 region in the event of an outage.

upvoted 6 times

 **masetromain** 2 years, 11 months ago

Choice D is similar to choice A, the VPCs in us-east-1 and us-west-1 are peered and the Auto Scaling group and Application Load Balancer (ALB) are extended across multiple availability zones in both regions. However, there is no explicit failover routing policy configured, so it is not clear how the application would failover to the us-west-1 region in the event of an outage.

Choice C is the correct answer as it includes all the necessary components for a disaster recovery environment in the us-west-1 region. It creates separate VPCs, Application Load Balancer, and Auto Scaling Group in both regions, and it enables health checks

and configure 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 6 times

 **zozza2023**  2 years, 11 months ago

Selected Answer: C

active-passive failover==>a failover routing policy within route 53

upvoted 7 times

 **amministrazione**  1 year, 3 months ago

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.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

It's C

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

C for DR

upvoted 2 times

 **God_Is_Love** 2 years, 10 months 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 5 times

 **God_Is_Love** 2 years, 10 months 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 3 times

 **zhangyu20000** 2 years, 11 months ago

C is correct

upvoted 3 times

Question #70

A company has an environment that has a single AWS account. A solutions architect is reviewing the environment to recommend what the company could improve specifically in terms of access to the AWS Management Console. The company's IT support workers currently access the console for administrative tasks, authenticating with named IAM users that have been mapped to their job role.

The IT support workers no longer want to maintain both their Active Directory and IAM user accounts. They want to be able to access the console by using their existing Active Directory credentials. The solutions architect is using AWS IAM Identity Center (AWS Single Sign-On) to implement this functionality.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an organization in AWS Organizations. Turn on the IAM Identity Center feature in Organizations. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure IAM Identity Center and set the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.
- B. Create an organization in AWS Organizations. Turn on the IAM Identity Center feature in Organizations. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure IAM Identity Center and select the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.
- C. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure IAM Identity Center and select the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.
- D. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure IAM Identity Center and set the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.

Correct Answer: D*Community vote distribution*

D (78%)

B (20%)

 **masetromain**  2 years, 11 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/69172-exam-aws-certified-solutions-architect-professional-topic-1/>

You are correct, I apologize for the oversight. To meet the requirements of the IT support workers, option D would be the correct solution:

This option will first enable all features in AWS Organizations, then create and configure an AD Connector to connect to the company's on-premises Active Directory. Then, it will configure IAM Identity Center (AWS SSO) and set the AD Connector as the identity source, allowing the IT support workers to access the console using their existing Active Directory credentials. Finally, it will create permission sets and map them to the existing groups within the company's Active Directory. This solution will also be cost-effective as it does not involve creating a new directory in AWS Directory Service.

upvoted 23 times

 **dev112233xx**  2 years, 9 months 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 19 times

 **carpa_jo** 2 years ago

Source: <https://aws.amazon.com/iam/identity-center/faqs/#product-faqs#iam-identity-center-faqs#identity-sources-and-applications-support>

upvoted 1 times

 **d9iceguy**  1 week, 4 days ago

Selected Answer: B

Selected Answer: B

Lower cost compared to AWS Managed Microsoft AD, since AD Connector does not require an additional managed directory service. Also, answer D AWS Organizations does not require "all features" for IAM Identity Center to work with AD Connector. "All features" is needed for SCPs and governance, not for SSO setup.

upvoted 1 times

✉ **shmoeee** 11 months, 1 week ago

Selected Answer: D

"Need to turn on all features" didn't sound cost effective...but apparently it's a requirement to provide SSO

upvoted 1 times

✉ **JOJO9** 1 year ago

Selected Answer: B

Question asks "MOST cost-effectively". Turning on all features is free of charge but used resources will make up a cost.

D is wrong because: enabling All Features in AWS Organizations introduces governance tools that the company does not require, making it less cost-effective than B.

upvoted 3 times

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

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.

upvoted 1 times

✉ **pk0619** 1 year ago

You need to enable all features for the organization to set up single sign-on for accounts.

upvoted 1 times

✉ **gofavad926** 1 year, 9 months ago

Selected Answer: B

B, Turn on the IAM Identity Center feature in Organizations... similar to D, but without enabling directly the SSO, you can't configure it...

upvoted 2 times

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

just D

upvoted 1 times

✉ **8608f25** 1 year, 10 months ago

Selected Answer: D

Option D is the best because AWS FAQs asked the following question and answered: "Which AWS accounts can I connect to IAM Identity Center?

You can add any AWS account managed using AWS Organizations to IAM Identity Center. You need to enable all features in your organizations to manage your accounts single sign-on." Link: <https://aws.amazon.com/iam/identity-center/faqs/#product-faqs#iam-identity-center-faqs#identity-sources-and-applications-support>.

With the clarification that enabling all features in AWS Organizations is necessary for integrating with IAM Identity Center, Option D becomes the most accurate and compliant solution. It correctly combines the need to enable all features in AWS Organizations with the use of an AD Connector for a direct connection to the company's on-premises Active Directory, which remains the most cost-effective way to leverage existing Active Directory credentials for AWS console access.

upvoted 1 times

Question #71

Topic 1

A video streaming company recently launched a mobile app for video sharing. The app uploads various files to an Amazon S3 bucket in the us-east-1 Region. The files range in size from 1 GB to 10 GB.

Users who access the app from Australia have experienced uploads that take long periods of time. Sometimes the files fail to completely upload for these users. A solutions architect must improve the app's performance for these uploads.

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

- A. Enable S3 Transfer Acceleration on the S3 bucket. Configure the app to use the Transfer Acceleration endpoint for uploads.
- B. Configure an S3 bucket in each Region to receive the uploads. Use S3 Cross-Region Replication to copy the files to the distribution S3 bucket.
- C. Set up Amazon Route 53 with latency-based routing to route the uploads to the nearest S3 bucket Region.
- D. Configure the app to break the video files into chunks. Use a multipart upload to transfer files to Amazon S3.
- E. Modify the app to add random prefixes to the files before uploading.

Correct Answer: AD

Community vote distribution

AD (97%)

 **zozza2023**  2 years, 11 months ago

Selected Answer: AD

Transfer Accelerator + Multi-part uploads for files more 500MB
upvoted 12 times

 **OCHT**  2 years, 8 months 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 7 times

 **princajen**  5 months, 1 week ago

Selected Answer: AD

To improve upload performance for large (1–10 GB) files from distant regions like Australia to an S3 bucket in us-east-1, enable S3 Transfer Acceleration to reduce latency and use multipart upload to handle large files more reliably and efficiently. These two solutions directly address both performance and reliability concerns.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. Enable S3 Transfer Acceleration on the S3 bucket. Configure the app to use the Transfer Acceleration endpoint for uploads.
D. Configure the app to break the video files into chunks. Use a multipart upload to transfer files to Amazon S3.
upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: AD

A = correct (improve upload performance)
B = this could work along with C to improve performance, but this will not fix upload failure for files >5GB as you need multi-part upload
C = se answer B
D = correct (required to fix upload failures for >5GB files)
E = this could help with throttling which is not clearly stated as an issue
upvoted 1 times

 **chico2023** 2 years, 4 months 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 years, 5 months ago

Selected Answer: AD

its AD

upvoted 2 times

 **Maria2023** 2 years, 6 months ago

Selected Answer: AD

A and D satisfy the requirement

upvoted 1 times

 **SkyZeroZx** 2 years, 7 months ago

Selected Answer: AD

Transfer Accelerator + Multi-part uploads for files more 500MB

Question similar to AWS Certified Solutions Architect Associate

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: AD

AD all day

upvoted 2 times

 **aqiao** 2 years, 9 months ago

Selected Answer: AD

B is not suitable here, since it wants to improve upload experience, not download

upvoted 2 times

 **Musk** 2 years, 11 months ago

I like AD but I am unsure. If the users in US don't complain about issues, it must be because multi-part upload is already enabled, otherwise it would fail 50% of the times. If only Australia users complain, it must be something else... Maybe A+B is a better option, although B is not the most cost efficient certainly.

upvoted 2 times

 **zhangyu20000** 2 years, 11 months ago

AD is correct

upvoted 1 times

 **masetromain** 2 years, 11 months ago

Selected Answer: AD

<https://www.examtopics.com/discussions/amazon/view/74177-exam-aws-certified-solutions-architect-professional-topic-1/>

The correct answers would be A and D.

A. Enabling S3 Transfer Acceleration on the S3 bucket and configuring the app to use the Transfer Acceleration endpoint for uploads will improve the app's performance for users in Australia by providing a fast and secure way to transfer large files over the Internet.

D. Configuring the app to break the video files into chunks and using a multipart upload to transfer files to Amazon S3, will improve the app's performance for users in Australia by allowing them to upload large files in parallel, which can increase upload speed and reduce the risk of upload failures.

upvoted 4 times

 **masetromain** 2 years, 11 months ago

B. Configuring an S3 bucket in each Region to receive the uploads and using S3 Cross-Region Replication to copy the files to the distribution S3 bucket is not the most cost-effective solution for this specific use case.

C. Setting up Amazon Route 53 with latency-based routing to route the uploads to the nearest S3 bucket Region is not a solution that would improve the performance of the uploads specifically for users in Australia.

E. Modifying the app to add random prefixes to the files before uploading will not improve the app's performance for users in Australia.

upvoted 1 times

✉️  **hobokabobo** 2 years, 9 months 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

An application is using an Amazon RDS for MySQL Multi-AZ DB instance in the us-east-1 Region. After a failover test, the application lost the connections to the database and could not re-establish the connections. After a restart of the application, the application re-established the connections.

A solutions architect must implement a solution so that the application can re-establish connections to the database without requiring a restart.

Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL Serverless v1 DB instance. Migrate the RDS DB instance to the Aurora Serverless v1 DB instance. Update the connection settings in the application to point to the Aurora reader endpoint.
- B. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.
- C. Create a two-node Amazon Aurora MySQL DB cluster. Migrate the RDS DB instance to the Aurora DB cluster. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.
- D. Create an Amazon S3 bucket. Export the database to Amazon S3 by using AWS Database Migration Service (AWS DMS). Configure Amazon Athena to use the S3 bucket as a data store. Install the latest Open Database Connectivity (ODBC) driver for the application. Update the connection settings in the application to point to the Athena endpoint

Correct Answer: B

Community vote distribution

B (100%)

 **God_Is_Love** Highly Voted 2 years, 10 months 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 10 times

 **zhangyu20000** Highly Voted 2 years, 11 months ago

B is correct.

C: Aurora is useless, Proxy is pointing to existing RDS

upvoted 7 times

 **princajen** Most Recent 5 months, 1 week ago

Selected Answer: B

To ensure application connections automatically re-establish after an Amazon RDS Multi-AZ failover without requiring an app restart, use Amazon RDS Proxy. It manages and maintains connections to the database, handling transient interruptions like failovers gracefully.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **pangchn** 1 year, 8 months ago

Selected Answer: B

C is wrong since RDS proxy for Aurora cluster only support reader endpoint, where in question it doesn't mention the read-only as requirement

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: B

A = using Aurora MySQL Serverless will not fix the issue, also serverless V1 is not great with HA. If you are running a single instance (no read replicas) it will attempt to create a new DB Instance in the same AZ

B = correct (RDS Proxy in addition to pooling connections, makes applications more resilient to database failures by automatically connecting to a standby DB instance while preserving application connections and detects failover and routes requests to standby instance up to 66% faster failover time)

C = Creating and migrating to Aurora cluster is not needed, RDS Proxy is enough

D = this requires a lot of work

upvoted 5 times

✉  **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

it's a B

upvoted 1 times

✉  **SkyZeroZx** 2 years, 6 months ago

Selected Answer: B

keyword = RDS proxy

upvoted 1 times

✉  **mfsec** 2 years, 9 months ago

Selected Answer: B

Create an RDS proxy.

upvoted 1 times

✉  **klog** 2 years, 10 months ago

Selected Answer: B

proxy will be a buffer

upvoted 1 times

✉  **masetromain** 2 years, 11 months ago

Selected Answer: B

The correct solution is B. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.

An RDS proxy is a service that allows you to pool and share connections to an RDS database. By using an RDS proxy, your application can automatically reconnect to the database after a failover event, without the need to restart the application.

Solution A, migrating to Aurora Serverless, may not solve the problem because Aurora Serverless does not support Multi-AZ.

Solution C and D are not the correct solutions because it does not solve the problem of reconnecting to the database after a failover event.

upvoted 4 times

✉  **God_Is_Love** 2 years, 10 months ago

What?? Aurora does not support Multi AZ ? its a blunder !

upvoted 5 times

✉  **chikorita** 2 years, 6 months ago

was about to point this

upvoted 1 times

✉  **BabaP** 2 years, 6 months ago

they are copying the answers from chatgpt

upvoted 7 times

✉  **k8s_Seoul** 2 years, 3 months ago

masetromain ~> X

GPTromain ~> O lol

upvoted 1 times

✉  **SeemaDataReader** 2 years ago

Even if the person is copying from chatgpt, they are saving your time and giving some pointers.

upvoted 1 times

Question #73

A company is building a solution in the AWS Cloud. Thousands of devices will connect to the solution and send data. Each device needs to be able to send and receive data in real time over the MQTT protocol. Each device must authenticate by using a unique X.509 certificate.

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

- A. Set up AWS IoT Core. For each device, create a corresponding Amazon MQ queue and provision a certificate. Connect each device to Amazon MQ.
- B. Create a Network Load Balancer (NLB) and configure it with an AWS Lambda authorizer. Run an MQTT broker on Amazon EC2 instances in an Auto Scaling group. Set the Auto Scaling group as the target for the NLConnect each device to the NLB.
- C. Set up AWS IoT Core. For each device, create a corresponding AWS IoT thing and provision a certificate. Connect each device to AWS IoT Core.
- D. Set up an Amazon API Gateway HTTP API and a Network Load Balancer (NLB). Create integration between API Gateway and the NLB. Configure a mutual TLS certificate authorizer on the HTTP API. Run an MQTT broker on an Amazon EC2 instance that the NLB targets. Connect each device to the NLB.

Correct Answer: C

Community vote distribution

C (97%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: C

The correct solution is C. Set up AWS IoT Core. For each device, create a corresponding AWS IoT thing and provision a certificate. Connect each device to AWS IoT Core.

AWS IoT Core is a fully managed service that enables secure, bi-directional communication between internet-connected devices and the AWS Cloud. It supports the MQTT protocol and includes built-in device authentication and access control. By using AWS IoT Core, the company can easily provision and manage the X.509 certificates for each device, and connect the devices to the service with minimal operational overhead.

upvoted 23 times

 **masetromain** 2 years, 11 months ago

Option A, setting up Amazon MQ queues and connecting each device to a queue, would require significant operational overhead to manage the queues and ensure that each device is properly authenticated and connected.

Option B and D, using a Network Load Balancer (NLB) with a Lambda authorizer or an Amazon API Gateway HTTP API with a mutual TLS certificate authorizer and running an MQTT broker on EC2 instances, would also introduce more operational complexity and overhead compared to using AWS IoT Core.

upvoted 7 times

 **princajen** Most Recent 5 months, 1 week ago

Selected Answer: C

To support thousands of devices with real-time MQTT communication and X.509 certificate authentication with the least operational overhead, use AWS IoT Core. It is purpose-built for scalable device communication, handles certificate-based auth natively, and is fully managed—no need to manage infrastructure or scale brokers manually.

upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

Selected Answer: C

AWS IoT Core: This service is specifically designed for managing IoT devices and supports the MQTT protocol natively. It provides built-in support for device authentication using X.509 certificates.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C

C, use IoT Core

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: C

Option C is the most suitable solution as AWS IoT Core is specifically designed for IoT scenarios, including device management and secure communication. AWS IoT Core natively supports MQTT, a lightweight communication protocol ideal for IoT devices. It allows devices to connect securely with an individual X.509 certificate for authentication, significantly reducing operational overhead compared to managing a custom MQTT broker or other intermediate services. AWS IoT Core also simplifies device management and scaling, making it the best choice for the described use case.

upvoted 1 times

 **bjexamprep** 1 year, 11 months ago

Selected Answer: C

I don't like C, but C might be the preferred answer.

There are thousands of devices. If C is the real answer, there should be a way to automatically create IOT thing and provision certificate. The answer seems implying to create IOT thing and provision certificates manually. If IoT core doesn't have this automation feature, this definitely is not the right answer in real life.

If there is this automation way and the question designer is expecting the exam taker to know this detail, that might be too specific for the exam takers.

D is ugly, and usually is not a correct answer in most question designs. But it provides a feasible way in the real life comparing with C.

upvoted 3 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

it's C

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

I choose C

upvoted 1 times

 **zejou1** 2 years, 9 months ago

Selected Answer: C

<https://docs.aws.amazon.com/iot/latest/developerguide/attach-to-cert.html>

It is C, - you have to do this through IOT core, for the devices you need an AWS IOT "thing" and then provision a certificate for the thing. from there connect the device.

upvoted 2 times

 **forceli** 2 years, 9 months 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** 2 years, 9 months ago

Sorry I meant "C"

upvoted 2 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: C

C is correct (less op overhead than A)

upvoted 2 times

 **zhangyu20000** 2 years, 11 months ago

C is correct

upvoted 3 times

Question #74

A company is running several workloads in a single AWS account. A new company policy states that engineers can provision only approved resources and that engineers must use AWS CloudFormation to provision these resources. A solutions architect needs to create a solution to enforce the new restriction on the IAM role that the engineers use for access.

What should the solutions architect do to create the solution?

- A. Upload AWS CloudFormation templates that contain approved resources to an Amazon S3 bucket. Update the IAM policy for the engineers' IAM role to only allow access to Amazon S3 and AWS CloudFormation. Use AWS CloudFormation templates to provision resources.
- B. Update the IAM policy for the engineers' IAM role with permissions to only allow provisioning of approved resources and AWS CloudFormation. Use AWS CloudFormation templates to create stacks with approved resources.
- C. Update the IAM policy for the engineers' IAM role with permissions to only allow AWS CloudFormation actions. Create a new IAM policy with permission to provision approved resources, and assign the policy to a new IAM service role. Assign the IAM service role to AWS CloudFormation during stack creation.
- D. Provision resources in AWS CloudFormation stacks. Update the IAM policy for the engineers' IAM role to only allow access to their own AWS CloudFormation stack.

Correct Answer: C

Community vote distribution

C (98%)

 **God_Is_Love**  2 years, 10 months 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 18 times

 **rbm2023**  2 years, 7 months 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 12 times

 **princajen**  5 months, 1 week ago

Selected Answer: C

To enforce a policy where engineers can only provision approved resources via AWS CloudFormation, assign engineers IAM policies that only permit CloudFormation actions, and use a separate IAM service role for CloudFormation that allows only approved resource types. This setup ensures engineers cannot bypass restrictions, and provisioning is limited to approved services defined by the service role.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

C. Update the IAM policy for the engineers' IAM role with permissions to only allow AWS CloudFormation actions. Create a new IAM policy with permission to provision approved resources, and assign the policy to a new IAM service role. Assign the IAM service role to AWS CloudFormation during stack creation.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C

C, use the IAM service role to execute the stack

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: C

Option C is the most effective solution. It involves updating the engineers' IAM role to only allow actions related to AWS CloudFormation, effectively preventing direct provisioning or modification of AWS resources outside of CloudFormation. By creating a service role (with permissions to provision approved resources) that CloudFormation assumes when executing templates, you enforce the provisioning of only approved resources through CloudFormation. This setup provides a clear separation of permissions: engineers can manage CloudFormation stacks but cannot directly create resources unless defined in a CloudFormation template and permitted by the service

role.

Option B suggests updating the IAM policy to allow only the provisioning of approved resources and CloudFormation actions. This approach could theoretically work by explicitly listing allowed actions for specific AWS services in the IAM policy. However, it might be challenging to maintain and could inadvertently permit actions outside of CloudFormation, depending on the policy's specificity.

upvoted 2 times

 ninomfr64 1 year, 11 months ago

Selected Answer: C

A = doesn't prevent to have a CloudFormation template with non-approved resources deployed

B = this doesn't prevent engineers to provision resources from console or cli

C = correct

D = doesn't prevent to provision non-approved resources or to provision only via CloudFormation

upvoted 3 times

 subbupro 2 years ago

B would be created generally in organization. C is fine , but more restriction , the user can only use the cloud formation stack sets only which is not good for organization level.

upvoted 1 times

 severlight 2 years, 1 month ago

Selected Answer: C

with B engineer will be able to directly provision resources without using of CF

upvoted 2 times

 venvig 2 years, 4 months 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 2 years, 4 months ago

Selected Answer: C

I prefer C, because you need to give permission to cloud formation

upvoted 1 times

 NikkyDicky 2 years, 5 months ago

Selected Answer: C

C no doubt

upvoted 1 times

 mfsec 2 years, 9 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 2 years, 10 months ago

Selected Answer: C

C IAM policy is allowing to provision of approved resources.

upvoted 3 times

 Musk 2 years, 11 months ago

Selected Answer: C

B does not enforce CF, otherwise it would work.

upvoted 3 times

 Untamables 2 years, 11 months ago

Selected Answer: C

C

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/security-best-practices.html#use-iam-to-control-access>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html>

upvoted 3 times

 Nicocacik 2 years, 11 months ago

Selected Answer: C

You have to use a service role

upvoted 4 times

Question #75

A solutions architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices all around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted.

The solutions architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB.

Which storage strategy is the MOST cost-effective and meets the design requirements?

- A. Design the application to store each incoming record as a single .csv file in an Amazon S3 bucket to allow for indexed retrieval. Configure a lifecycle policy to delete data older than 120 days.
- B. Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoDB Time to Live (TTL) feature to delete records older than 120 days.
- C. Design the application to store each incoming record in a single table in an Amazon RDS MySQL database. Run a nightly cron job that runs a query to delete any records older than 120 days.
- D. Design the application to batch incoming records before writing them to an Amazon S3 bucket. Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadata search feature to retrieve the data. Configure a lifecycle policy to delete the data after 120 days.

Correct Answer: B

Community vote distribution

B (76%)

D (24%)

✉  **masetromain**  2 years, 11 months ago

Selected Answer: B

The most cost-effective and efficient solution that meets the design requirements would be option B, Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoDB Time to Live (TTL) feature to delete records older than 120 days.

DynamoDB is a NoSQL key-value store designed for high scale and performance. It is fully managed by AWS and can easily handle millions of small records per minute. Additionally, with the TTL feature, you can set an expiration time for each record, so that the data can be automatically deleted after the specified time period.

upvoted 24 times

✉  **masetromain** 2 years, 11 months ago

Option A, storing each incoming record as a single .csv file in an Amazon S3 bucket, would not be a good option because it would be difficult to retrieve individual records from the .csv files, and will likely increase the cost of data retrieval.

Option C, storing each incoming record in a single table in an Amazon RDS MySQL database, would be a more expensive option as RDS is typically more expensive than DynamoDB. Additionally, running a cron job to delete old data could lead to additional operational overhead.

Option D, storing incoming records in batches in an S3 bucket, would be a less efficient option as it would require additional processing and parsing of the data to retrieve individual records.

upvoted 7 times

✉  **dkx**  2 years, 5 months 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 6 times

✉  **ahhatem** 1 year ago

Actually, the limit you mentioned for point D is per prefix or path.... Not the whole bucket. With proper data distribution across prefixes it can accommodate easily for the load mentioned.

upvoted 2 times

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

Selected Answer: B

While S3 (Option D) is more cost-effective, it does not satisfy the low-latency retrieval requirement. Amazon DynamoDB (Option B) offers low-latency access, scales to millions of records per minute, and supports TTL for automatic data expiration, making it the most appropriate solution that meets all design requirements, even if it comes at a higher cost.

upvoted 1 times

✉ **AI8282** 5 months, 3 weeks ago

Selected Answer: D

D because it did ask for THE MOST cost-effective and D still meets the minimum requirements. It did ask for 'low latency' and Dynamo is for sure less latency but this workload seems like it would be fine for writes and reads. it only discusses writes, not reads so I think it wants to focus on it being fast enough. It didn't mention that you would optimize prefixes and such though which concerns me.

upvoted 1 times

✉ **jimee11** 7 months, 3 weeks ago

Selected Answer: B

Read the requirements: MOST cost-effective and meets the design requirements. Note "retrieved with low latency". DynamoDB latency is single digits, whereas S3 is 100-200 milliseconds.

upvoted 1 times

✉ **vmia159** 9 months, 2 weeks ago

Selected Answer: D

For those who said B, how many WCU is needed for dynamoDB?

Given:

1 million records per minute

4KB per record

This translates to approximately 16,667 records per second (1,000,000 / 60)

For DynamoDB WCU calculation:

1 WCU = 1 write per second for items up to 1KB

For items larger than 1KB, the WCU is rounded up to the next 1KB

For 4KB items, each write will consume 4 WCUs

Therefore:

WCUs needed = (Records per second) × (Item size in KB rounded up)

WCUs = 16,667 × 4

WCUs = 66,668 WCUs

First, you need to increase the quotas for that table by submitting a support ticket.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/ServiceQuotas.html>

Second, this is very expensive.

Obviously, combine it with kinesis data agent and firehose that write to S3 will be much reliable options but it will increase the cost significantly. But still cheaper than the dynamo db options.

<https://calculator.aws/#/estimate?id=87f1df21449660b0b9d61a6c1153632b1983d2e4>

upvoted 1 times

✉ **5e8c031** 5 months, 3 weeks ago

...but it does not meet the requirement "can be retrieved with low latency"

upvoted 1 times

✉ **soulation** 9 months, 4 weeks ago

Selected Answer: D

Option B is too expensive.

upvoted 1 times

✉ **sergza** 1 year ago

Selected Answer: D

If you really think about being cost effective than Option D is the right choice

upvoted 1 times

✉ **Heman31in** 1 year ago

Selected Answer: D

Why Option D Might Be Cost-Effective:

Lower Storage Costs:

S3 storage is generally cheaper than DynamoDB when dealing with large amounts of data (e.g., \$0.023/GB/month for S3 Standard vs. \$0.25/GB/month for DynamoDB on-demand).

Batching Reduces API Call Costs:

By batching multiple records into a single object, you reduce the number of PUT requests to S3. This can lead to lower API costs compared to writing each record individually to DynamoDB.

Lifecycle Policies for Data Expiry:

S3 lifecycle policies automatically clean up data older than 120 days, similar to DynamoDB's TTL feature.

upvoted 1 times

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

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.

upvoted 1 times

✉ **ahhatem** 1 year, 6 months ago

Selected Answer: B

Obviously it is DynamoDB. Although as a side note I would say it is probably a very bad choice as it would be astronomically expensive for millions of writes per minute.... A Kinesis Data Streams would make much more sense especially that the data is only needed for 3 months...

upvoted 2 times

 **ahhatem** 1 year ago

After a second thought, I am not sure it is B. D would be much cheaper if it means that objects buffered and combined before write. But the word "batch" doesn't make me comfortable, batching means writing the objects in one go... nothing implies the objects would be combined ...

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: B

B, dynamodb is the best option

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: B

For small records less than 4 KB, DynamoDB can efficiently handle the ingestion of millions of records per minute from devices around the world, meeting the application's design requirements for low-latency data access. Additionally, DynamoDB's Time to Live (TTL) feature allows for automatic deletion of items after a specific period, aligning with the requirement to store data for only 120 days.

upvoted 1 times

 **0dc6cac** 6 months, 1 week ago

What about costs? you'd get a gigantic bill at the end of the month

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: B

A = S3 is not great with small files and searching for data based on index (a common pattern is to store object metadata in a database like DDB, OpenSearch or RDS/Aurora). Many small files can lead to high costs for retrieval

B = correct

C = single-table design, high volume write/retrieval of small object and no need for complex query are better served and cost less with DDB rather than RDS

D = more efficient than A, but still S3 metadata search feature is limited

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: B

see uC6rW1aB's answer

upvoted 1 times

 **vjp_training** 2 years, 3 months ago

Selected Answer: B

B is the best for cost-effective.

D is more cost for S3 request

upvoted 1 times

 **uC6rW1aB** 2 years, 3 months ago

Selected Answer: B

Ref: <https://aws.amazon.com/dynamodb/pricing/on-demand/>

DynamoDB read requests can be either strongly consistent, eventually consistent, or transactional. A strongly consistent read request of up to 4 KB requires one read request unit. For items larger than 4 KB, additional read request units are required.

upvoted 3 times

 **uC6rW1aB** 2 years, 3 months 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 5 times

Question #76

A retail company is hosting an ecommerce website on AWS across multiple AWS Regions. The company wants the website to be operational at all times for online purchases. The website stores data in an Amazon RDS for MySQL DB instance.

Which solution will provide the HIGHEST availability for the database?

- A. Configure automated backups on Amazon RDS. In the case of disruption, promote an automated backup to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source.
- B. Configure global tables and read replicas on Amazon RDS. Activate the cross-Region scope. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- C. Configure global tables and automated backups on Amazon RDS. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- D. Configure read replicas on Amazon RDS. In the case of disruption, promote a cross-Region and read replica to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source.

Correct Answer: D

Community vote distribution

D (94%)	6%
---------	----

 **zejou1** Highly Voted 2 years, 9 months 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 15 times

 **princajen** Most Recent 5 months, 1 week ago

Selected Answer: D

Automated Backups: Good for recovery, but restoring from backup is slow and not instant.

Read Replicas: Can be in another Region. You can promote a read replica to be a standalone DB in case of a failover.

Global Tables: Only available for DynamoDB, not RDS — this rules out any option mentioning global tables in the context of RDS.
upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: D

A = you cannot promote an automated backup to a standalone DB (you restore a backup into a new DB instance instead). Creating a read replica could help in this scenario in case it is cross-region. This is not specified

B = RDS does not support global table, copying a read replicas from a region to another make no sense to me

C = see B

D = correct

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: D

D for sure

upvoted 1 times

 **rbm2023** 2 years, 7 months 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** 2 years, 9 months ago

Selected Answer: D

D makes the most sense

upvoted 1 times

 **God_Is_Love** 2 years, 10 months 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** 2 years, 10 months 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 2 times

 **sambb** 2 years, 10 months 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** 2 years, 11 months ago

Selected Answer: D

for B,C, Amazon RDS does not support global tables yet. Only Aurora supports.

upvoted 4 times

 **AlanKrish** 2 years, 10 months ago

Is Aurora not part of RDS? You can choose Aurora's compatibility with MySQL and PostgreSQL).

upvoted 1 times

 **zhangyu20000** 2 years, 11 months ago

D is correct

upvoted 3 times

 **masetromain** 2 years, 11 months ago

<https://www.examtopics.com/discussions/amazon/view/69438-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

 **masetromain** 2 years, 11 months ago

It is possible that some people may think that option D. Configure read replicas on Amazon RDS. In the case of disruption, promote a cross-Region and read replica to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source. is the best solution, as it also utilizes read replicas and cross-Region promotion to minimize downtime. However, it is important to consider that while this solution provides high availability, it doesn't provide the same level of automatic replication that global tables do. In case of a disruption, there is a risk of data loss during the manual switchover.

and also with option D, you are still working with a single point of failure, the primary database, while in option B you have multiple copies of your data distributed across different regions, so in case of a failure you can switch over to one of the replicas without loss of data.

upvoted 2 times

 **Shahul75** 2 years, 10 months ago

B is not right. Only Aurora has global tables. RDS don't

upvoted 1 times

 **masetromain** 2 years, 11 months ago

Selected Answer: B

The correct answer is option B. Configuring global tables and read replicas on Amazon RDS with the cross-Region scope enabled provides the highest availability for the database. In case of disruption, the company can use AWS Lambda to copy the read replicas from one Region to another Region, ensuring that the website remains operational at all times. This solution provides automatic failover across multiple regions and allows for fast recovery in case of a disruption.

Option A involves promoting an automated backup to be a standalone DB instance and creating a replacement read replica that has the promoted DB instance as its source. This solution is less efficient since it requires manual intervention and additional steps to promote the backup and create a replacement read replica.

upvoted 2 times

 **Sarutobi** 2 years, 10 months 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** 2 years, 11 months ago

Option C involves configuring global tables and automated backups on Amazon RDS. This solution is less efficient since it does not provide automatic failover across multiple regions and requires additional steps to copy the read replicas from one Region to another Region using AWS Lambda.

Option D involves configuring read replicas on Amazon RDS. In the case of disruption, promoting a cross-Region and read replica to be a standalone DB instance. This solution is less efficient than Option B since it does not provide automatic failover across multiple regions and requires manual intervention to promote the read replica to a standalone instance.

upvoted 1 times

✉  **btx** 2 years, 6 months 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 2 times

Question #77

Example Corp. has an on-premises data center and a VPC named VPC A in the Example Corp. AWS account. The on-premises network connects to VPC A through an AWS Site-To-Site VPN. The on-premises servers can properly access VPC A. Example Corp. just acquired AnyCompany, which has a VPC named VPC B. There is no IP address overlap among these networks. Example Corp. has peered VPC A and VPC B.

Example Corp. wants to connect from its on-premise servers to VPC B. Example Corp. has properly set up the network ACL and security groups.

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

- A. Create a transit gateway. Attach the Site-to-Site VPN, VPC A, and VPC B to the transit gateway. Update the transit gateway route tables for all networks to add IP range routes for all other networks.
- B. Create a transit gateway. Create a Site-to-Site VPN connection between the on-premises network and VPC B, and connect the VPN connection to the transit gateway. Add a route to direct traffic to the peered VPCs, and add an authorization rule to give clients access to the VPCs A and B.
- C. Update the route tables for the Site-to-Site VPN and both VPCs for all three networks. Configure BGP propagation for all three networks. Wait for up to 5 minutes for BGP propagation to finish.
- D. Modify the Site-to-Site VPN's virtual private gateway definition to include VPC A and VPC B. Split the two routers of the virtual private gateway between the two VPCs.

Correct Answer: A*Community vote distribution*

A (91%)	6%
---------	----

 **rbm2023** Highly Voted 2 years, 7 months ago

Selected Answer: A

https://docs.aws.amazon.com/pt_br/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-vpn.html
Transit gateway is an AWS managed high availability and scalability regional network transit hub used to interconnect VPCs and customer networks. AWS Transit Gateway + VPN, using the Transit Gateway VPN Attachment, provides the option of creating an IPsec VPN connection between your remote network and the Transit Gateway over the internet, as shown in the following picture.
<https://docs.aws.amazon.com/images/whitepapers/latest/aws-vpc-connectivity-options/images/image4.png>
Option A is the correct answer since the transit gateway will allow both VPCs to connect to the on-premises network.
Option B suggests the same feature but is using the Transit Gateway in an incorrect way. The sole purpose of the gateway is to have point for interconnectivity.

upvoted 11 times

 **Tunstim** Highly Voted 2 years, 8 months 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 5 times

 **chikorita** 2 years, 3 months ago

please reply to him

upvoted 2 times

 **princajen** Most Recent 5 months, 1 week ago

Selected Answer: A

To enable on-premises connectivity to both VPC A and VPC B with the least operational effort and highest scalability, use AWS Transit Gateway. Attach the existing Site-to-Site VPN, VPC A, and VPC B to the TGW and update TGW route tables to allow traffic between all three networks. This provides transitive routing, simplifies network management, and is AWS-recommended for multi-VPC architectures.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **jcelest1** 1 year, 4 months ago

After all, what is the right answer A or D?

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A, Transit Gateway

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: A

Option A is the most straightforward and effective solution. A transit gateway acts as a cloud router that simplifies network topology and connectivity between on-premises networks, VPCs, and other AWS services. By attaching both VPCs (A and B) and the Site-to-Site VPN to a single transit gateway and updating the route tables accordingly, Example Corp. can enable seamless communication between its on-premises network and both VPCs. This approach minimizes operational effort by centralizing network management and eliminating the need for complex routing configurations or multiple VPN connections.

Option D proposes modifying the Site-to-Site VPN's virtual private gateway to include both VPC A and VPC B. However, a virtual private gateway cannot be directly shared or split between VPCs in the manner described. This option misunderstands the architecture of AWS networking components and their capabilities.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: A

A = correct

B = if you setup a second VPN you do not need a TGW

C = peering does not allow edge-to-edge routing (aka VPC B cannot access on-premise via VPC A and vice versa)

D = Virtual Private Gateway is specific to a single VPC

upvoted 2 times

 **Russ99** 2 years, 4 months ago

Selected Answer: A

reluctantly selecting option A. these answers do not take into consideration that the On-promises already has a peered connection to VPC A through the existing site to site

upvoted 2 times

 **CuteRunRun** 2 years, 4 months ago

Selected Answer: A

I think A is right, I do not know why other guys select D

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

surely A

upvoted 1 times

 **Parsons** 2 years, 8 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** 2 years, 9 months ago

Selected Answer: A

Solution A is the only one possible solution

upvoted 1 times

 **Arnaud92** 2 years, 9 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

 **Arnaud92** 2 years, 9 months ago

A : the best (and the only one possible) answer : When you have 2 VPC, you have multiple solutions 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 answers

upvoted 4 times

 **mfsec** 2 years, 9 months ago

Selected Answer: A

A. Create a transit gateway. Attach the Site-to-Site VPN

upvoted 1 times

✉ **dev112233xx** 2 years, 9 months ago

Selected Answer: A

A makes sense to me

upvoted 1 times

✉ **taer** 2 years, 9 months ago

Selected Answer: A

A for me

upvoted 1 times

✉ **God_Is_Love** 2 years, 10 months 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** 2 years, 10 months ago

oops this is wrong..VPN can be attached...

upvoted 1 times

✉ **God_Is_Love** 2 years, 10 months ago

Moderator, please delete this comment..

upvoted 1 times

✉ **God_Is_Love** 2 years, 10 months 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** 2 years, 9 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

Question #78

A company recently completed the migration from an on-premises data center to the AWS Cloud by using a replatforming strategy. One of the migrated servers is running a legacy Simple Mail Transfer Protocol (SMTP) service that a critical application relies upon. The application sends outbound email messages to the company's customers. The legacy SMTP server does not support TLS encryption and uses TCP port 25. The application can use SMTP only.

The company decides to use Amazon Simple Email Service (Amazon SES) and to decommission the legacy SMTP server. The company has created and validated the SES domain. The company has lifted the SES limits.

What should the company do to modify the application to send email messages from Amazon SES?

- A. Configure the application to connect to Amazon SES by using TLS Wrapper. Create an IAM role that has ses:SendEmail and ses:SendRawEmail permissions. Attach the IAM role to an Amazon EC2 instance.
- B. Configure the application to connect to Amazon SES by using STARTTLS. Obtain Amazon SES SMTP credentials. Use the credentials to authenticate with Amazon SES.
- C. Configure the application to use the SES API to send email messages. Create an IAM role that has ses:SendEmail and ses:SendRawEmail permissions. Use the IAM role as a service role for Amazon SES.
- D. Configure the application to use AWS SDKs to send email messages. Create an IAM user for Amazon SES. Generate API access keys. Use the access keys to authenticate with Amazon SES.

Correct Answer: B*Community vote distribution*

B (87%)

12%

 scuzzy2010  2 years, 10 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 20 times

 God_Is_Love 2 years, 9 months 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 6 times

 Untamables  2 years, 11 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 9 times

 princajen  5 months ago

Selected Answer: B

The correct answer is B because Amazon SES requires STARTTLS for SMTP, and it authenticates using SMTP credentials, not IAM roles or API keys. Since the application supports only SMTP and not API/SDK, STARTTLS is the only compatible secure option.
 upvoted 1 times

 amministrazione 1 year, 3 months ago

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.
 upvoted 1 times

 8608f25 1 year, 10 months ago

Selected Answer: B

Here's why option B is the correct choice:
 STARTTLS Support: Amazon SES supports STARTTLS, a protocol command used to upgrade an existing insecure connection to a secure connection using TLS (Transport Layer Security). This is crucial since the legacy SMTP server does not support TLS, and STARTTLS can be used to initiate a secure connection.

SMTP Credentials: Amazon SES requires authentication to send emails through its SMTP interface. This is achieved by using SMTP credentials, which are different from AWS access keys. SMTP credentials can be obtained from the Amazon SES console and are used to authenticate with the Amazon SES SMTP endpoint.

Operational Simplicity: This approach allows the application to continue using SMTP for sending emails, which aligns with the application's existing capabilities. By using STARTTLS, the application can upgrade its connection to Amazon SES to a secure one, ensuring compliance with security best practices without significant changes to the application's email sending functionality.

upvoted 2 times

 **LazyAutonomy** 1 year, 11 months ago

Selected Answer: A

Terrible Q. All answers are wrong.

A is wrong because you cannot send emails through SES SMTP using SMTP credentials derived from temporary STS tokens (ie IAM roles). Must use an IAM user access keys to derive creds.

B is wrong because the question imposes a constraint that prevents us from selecting an answer that requires upgrading or modifying the application itself. Could you just offload SMTP STARTTLS/AUTH to the local sendmail/postfix daemon? Maybe, if it were Linux, but what if it's Windows? Cygwin? WSL?

C & D - wrong, for a similar rationale as B.

But the question designer OBVIOUSLY doesn't know that IAM roles can't be used for SES SMTP auth, because these questions are written by inexperienced, unqualified people who are not themselves architects or engineers.

upvoted 2 times

 **LazyAutonomy** 1 year, 11 months ago

To be fair, the question says this:

"The legacy SMTP server does not support TLS encryption and uses TCP port 25. The application can use SMTP only."

The question doesn't say the application cannot handle STARTTLS or SMTP AUTH. In theory, if an application claims to support SMTP, then it should support all features of SMTP, which includes STARTTLS and AUTH. It only says the legacy SMTP server cannot handle TLS. So I suppose perhaps B is correct after all :-)

upvoted 3 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: B

A = this sends email via SES API while application can use SMTP only

B = correct

C = this sends email via SES API while application can use SMTP only

D = this sends email via SES SDK (API) while application can use SMTP only

upvoted 2 times

 **ninomfr64** 1 year, 11 months ago

Need to correct my comment on A. This is a TLS Wrapper (A) vs STARTTLS (B), where STARTTLS allows initiating an encrypted connection by first establishing an unencrypted connection. While TLS Wrapper is a means of initiating an encrypted connection without first establishing an unencrypted connection (it's the client's responsibility to connect to the endpoint using TLS, and to continue using TLS for the entire conversation). As our app can only work with SMTP we should go for B

upvoted 2 times

 **edder** 2 years, 1 month ago

Selected Answer: B

The correct answer is B.

A: We are unable to obtain authentication information.

C,D: Does not meet SMTP requirements.

B: This is the correct procedure.

<https://repost.aws/knowledge-center/ses-set-up-connect-smtp>

<https://docs.aws.amazon.com/ses/latest/dg/security-protocols.html>

upvoted 1 times

 **totten** 2 years, 2 months ago

Selected Answer: B

Here's why option B is the correct choice:

SMTP Protocol: The legacy SMTP server uses the SMTP protocol, and Amazon SES provides an SMTP interface for sending email, which is suitable for your application.

STARTTLS: Using STARTTLS ensures that your communication with Amazon SES is encrypted, which is a best practice for secure email transmission.

SMTP Credentials: Amazon SES SMTP credentials are required to authenticate your application with Amazon SES when sending emails. These credentials include an SMTP username and password.

upvoted 2 times

 **totten** 2 years, 2 months ago

Option A mentions TLS Wrapper, which isn't a standard approach when using Amazon SES for sending email. Amazon SES supports STARTTLS for secure communication.

Option C suggests using the SES API, which is a valid approach but requires code modifications to use the SES API instead of SMTP.

Since your application can only use SMTP, this option might involve significant code changes.

Option D mentions using AWS SDKs and IAM users, which is more suitable for programmatic access to SES but not for legacy SMTP applications that can only send via SMTP.

Therefore, Option B is the most appropriate choice for configuring your application to send email messages from Amazon SES while preserving the SMTP protocol and ensuring secure communication.

upvoted 4 times

 **CuteRunRun** 2 years, 4 months ago

Selected Answer: A

I selecte A

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

It's B - to preserve SMTP protocol

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months 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** 2 years, 7 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/big-data/query-and-visualize-aws-cost-and-usage-data-using-amazon-athena-and-amazon-quicksight/>

upvoted 1 times

 **rbm2023** 2 years, 7 months ago

Selected Answer: B

Option A states that the company would require to do more changes in the application than a replatform migration strategy where we are supposed to migrate the application with minimal changes. In Option A using the TLS wrapper would require an additional layer of software (stunnel) to be installed and configured on the EC2 instance, which may introduce additional complexity and management overhead.

In option B, we need to configure the application to connect to SES using STARTTLS using SMTP credentials, since the legacy SMTP server does not support TLS encryption. This would require minimal change to the application.

upvoted 3 times

 **Cassa** 2 years, 8 months ago

Selected Answer: B

To set up a STARTTLS connection, the SMTP client connects to the Amazon SES SMTP endpoint on port 25, 587, or 2587, issues an EHLO command, and waits for the server to announce that it supports the STARTTLS SMTP extension. The client then issues the STARTTLS command, initiating TLS negotiation. When negotiation is complete, the client issues an EHLO command over the new encrypted connection, and the SMTP session proceeds normally

To set up a TLS Wrapper connection, the SMTP client connects to the Amazon SES SMTP endpoint on port 465 or 2465. The server presents its certificate, the client issues an EHLO command, and the SMTP session proceeds normally.

upvoted 2 times

 **mfsec** 2 years, 9 months ago

Selected Answer: B

B. Configure the application to connect to Amazon SES by using STARTTLS.

upvoted 1 times

 **Dimidrol** 2 years, 9 months ago

Selected Answer: B

B , <https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>

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.

Correct Answer: A

Community vote distribution

A (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: A

The correct solution is A.

Creating an AWS Cost and Usage Report for the organization and defining tags and cost categories in the report will allow for detailed cost reporting for the different companies that have been consolidated into one organization. By creating a table in Amazon Athena and an Amazon QuickSight dataset based on the Athena table, the finance team will be able to easily query and generate reports on the costs for all the companies. The dataset can then be shared with the finance team for them to use for their reporting needs.

Option B is not correct because it does not provide a way to query and generate reports on the costs for all the companies.

Option C is not correct because it only provides spending information from the AWS Price List Query API and does not provide detailed cost reporting for the different companies.

Option D is not correct because it only uses the AWS Price List Query API and does not provide a way to query and generate reports on the costs for all the companies.

upvoted 14 times

 **moota** Highly Voted 2 years, 10 months ago

Selected Answer: A

I can customize reporting in Cost Explorer but cannot find how to do templates.

upvoted 7 times

 **princajen** Most Recent 5 months ago

Selected Answer: A

The best solution is A because it uses the Cost and Usage Report (CUR) to gather detailed organization-wide cost data, leverages tags and cost categories for meaningful grouping (e.g., by team or company), and integrates with Athena and QuickSight for querying and visual reporting. This setup supports self-managed applications and provides the finance team with flexible access to comprehensive cost data.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: A

A = correct

B = there isn't specialized templates in AWS Cost Explorer. It provides default reports, but also enables you to change the filters and constraints used to create the reports. You can save the reports that you made as a bookmark, download the CSV file, or save them as a report

C & D = AWS Price List provides a catalog of the products and prices for AWS services that you can purchase on AWS, not cost of your resources

upvoted 3 times

 **CuteRunRun** 2 years, 4 months ago

Selected Answer: A

I prefer A

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

its n A

upvoted 1 times

 **Maria2023** 2 years, 6 months 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 2 times

 **F_Eldin** 2 years, 7 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/big-data/query-and-visualize-aws-cost-and-usage-data-using-amazon-athena-and-amazon-quicksight/>

upvoted 3 times

 **mfsec** 2 years, 9 months ago

Selected Answer: A

A. Create an AWS Cost and Usage Report for the organization.

upvoted 1 times

 **zhangyu20000** 2 years, 11 months ago

A is correct

B: no such template for cost explorer

CD: Price List Query API is for list price, not for usage

upvoted 2 times

Question #80

Topic 1

A company runs an IoT platform on AWS. IoT sensors in various locations send data to the company's Node.js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume.

The number of sensors the company has deployed in the field has increased over time, and is expected to grow significantly. The API servers are consistently overloaded and RDS metrics show high write latency.

Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? (Choose two.)

- A. Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS.
- B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas.
- C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data.
- D. Use AWS X-Ray to analyze and debug application issues and add more API servers to match the load.
- E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance.

Correct Answer: CE

Community vote distribution

CE (61%)	BC (29%)	5%
----------	----------	----

 **masetromain**  2 years, 11 months ago

Selected Answer: CE

C and E are the correct answers.

Option C: Leveraging Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data would help to resolve the issues with the API servers being consistently overloaded. By using Kinesis, the data can be ingested and processed in real-time, allowing the API servers to handle the increased load. Using Lambda to process the data can also help to improve the overall performance and scalability of the platform.

Option E: Re-architecting the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance would help to resolve the issues with high write latency. DynamoDB is a NoSQL database that is designed for high performance and scalability, making it a good fit for this use case. Additionally, DynamoDB supports auto-scaling, which can help to ensure that the database can handle the expected growth in the number of sensors.

upvoted 21 times

 **OCHT** 2 years, 8 months 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

 **masetromain** 2 years, 11 months ago

Option A, Resizing the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS will not solve the problem, as the problem is not just related to storage size but also high write latency.

Option B, Re-architecting the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and adding read replicas would help to improve the read performance, but it won't help in reducing write latency.

Option D, Using AWS X-Ray to analyze and debug application issues and adding more API servers to match the load, would help in identifying the problem and resolving it, but it will not help in reducing the load on the servers.

upvoted 3 times

 **SuperP43** 2 years, 10 months 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 9 times

 **tromyunpak** 2 years, 6 months 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

 **tromyupak** 2 years, 6 months ago

also rds proxy is not used (sorry typo) to handle write operations properly
upvoted 1 times

 **kamaro** 2 years, 9 months ago

I agree with you.

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_AuroraOverview.html

Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

Aurora includes a high-performance storage subsystem. Its MySQL- and PostgreSQL-compatible database engines are customized to take advantage of that fast distributed storage. The underlying storage grows automatically as needed. An Aurora cluster volume can grow to a maximum size of 128 tebibytes (TiB).

upvoted 2 times

 **zejou1** 2 years, 9 months 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 2 times

 **Sarutobi** 2 years, 7 months ago

I think this is the big point in this question and that DynamoDB is being position by AWS for IoT very hard. Although is technically possible to migrate with DMS from SQL to DynamoDB, is hard, but harder yet is the change of model inside the application or service.

upvoted 1 times

 **Gmail78** 2 years, 4 months ago

not the best but not impossible <https://aws.amazon.com/blogs/big-data/near-zero-downtime-migration-from-mysql-to-dynamodb/>
upvoted 2 times

 **princajen** Most Recent 5 months ago

Selected Answer: CE

C (Kinesis + Lambda): Scales ingestion and offloads API servers. Ideal for IoT. Serverless and cost-efficient.

E (DynamoDB): High write throughput and autoscaling. Purpose-built for sensor data, resolving high write latency permanently.

Together, C and E provide a durable, scalable, and cost-efficient solution for IoT data ingestion and storage, supporting long-term growth without overloading compute or database layers.

upvoted 2 times

 **Kaps443** 6 months, 3 weeks ago

Selected Answer: CE

C + E provide the most scalable, cost-efficient, and future-proof architecture for the company's IoT platform.

upvoted 1 times

 **eesa** 7 months, 2 weeks ago

Selected Answer: BD

B. Rediseñar a Amazon Aurora + réplicas de lectura

→ Sí.

Aurora es mucho más escalable y eficiente que MySQL RDS normal.

Puedes crear réplicas de lectura automáticas para distribuir carga sin mucho esfuerzo manual.

Permite crecimiento masivo de forma rentable porque Aurora gestiona réplicas y escalado de manera serverless si quieres (Aurora Serverless v2).

C. Kinesis Data Streams + Lambda para ingesta

→ Sí.

Si los sensores envían muchísimos datos en tiempo real, meterlos directo en EC2+RDS satura todo.

Kinesis puede recibir millones de eventos por segundo de forma masiva, almacenar temporalmente y procesarlos por lotes (batching) con Lambda, desacoplando la presión sobre tus APIs y la base de datos.

Escala automáticamente y es muy rentable.

upvoted 1 times

 **Paul123456789** 8 months, 4 weeks ago

Selected Answer: CE

A. will not fix the problem

B. read replicas will not fix the high write latency

D. is for debugging, not a solution

This make it C and E

upvoted 1 times

 **hhiguita** 9 months, 1 week ago

Selected Answer: BC

Write performance will be improved by switch RDS to Aurora. RDS to Aurora is smooth transition without too much on the application side. Answer E will application side not just backend DB.

upvoted 1 times

 **29fb203** 9 months, 2 weeks ago

Selected Answer: BC

B. Re-architect the database tier to use Amazon Aurora and add read replicas

Aurora automatically scales storage up to 128 TB without manual resizing.

Faster writes and lower read latency than standard RDS MySQL.

C. Use Amazon Kinesis Data Streams and AWS Lambda for ingestion and processing

Decouples IoT data ingestion from database writes

Kinesis Data Streams ingests large volumes of sensor data without overloading API servers.

Scales automatically with the number of sensors.

Not E because DynamoDB is NoSQL and doesn't support MySQL.

upvoted 1 times

 **bhanus** 12 months ago

Selected Answer: BC

B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas.

Amazon Aurora is a managed database service compatible with MySQL, designed for high performance and scalability.

Aurora provides better write performance and supports read replicas to handle increased read traffic as the platform grows. This will address the high write latency issue and enable horizontal scaling.

C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data.

Using Amazon Kinesis Data Streams for data ingestion offloads traffic from the API servers, reducing their load and improving scalability. AWS Lambda can process the raw data in real time and pass it to the database or other systems, providing a cost-effective and scalable solution for data processing.

upvoted 1 times

 **Heman31in** 1 year ago

Selected Answer: CE

By combining C (Kinesis + Lambda) with E (DynamoDB), you're preparing the platform to handle exponential growth in sensor data while ensuring high availability, scalability, and low latency for both data processing and storage. This solution directly addresses the need for a robust, future-proof architecture capable of supporting massive data volumes without bottlenecks, making it well-suited for the IoT platform's growth.

upvoted 1 times

 **wem** 1 year ago

Selected Answer: BC

E would require a shift from relational to a no-sql table - what if there are multiple tables?

upvoted 1 times

 **koniczny69** 1 year, 1 month ago

Selected Answer: CE

C is straightforward.

I go for E rather than B, because db shows heavy write latency, not limit. Replacing with Aurora will speed up thing up until a limit. Goal is to deal with it once and for all

upvoted 2 times

 **0b43291** 1 year, 1 month ago

Selected Answer: BC

By combining options B and C, the company can address the current performance and scalability issues while enabling future growth as more sensors are deployed. Amazon Aurora provides a scalable and high-performance relational database, while Kinesis Data Streams and Lambda offer a serverless and cost-effective solution for ingesting and processing the raw data streams.

Option A may provide temporary relief by increasing IOPS, but it doesn't address the scalability and performance limitations of RDS MySQL.

Option D can help identify application issues but doesn't solve the underlying database problems.

Option E is not ideal as DynamoDB is a NoSQL database, and the existing application is likely designed for a relational database like MySQL or Aurora, requiring significant changes to the application code and data modeling.

upvoted 2 times

 **amministrazione** 1 year, 3 months ago

C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data.

E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance.

upvoted 1 times

 **zolthar_z** 1 year, 5 months ago

Selected Answer: CE

What discards B is "Add read replicas", the problem is writing the new data in the DB, adding Read replicas will increase the cost and this is not what question requests "maintain cost"

upvoted 2 times

 **Helpnose** 1 year, 6 months ago

Selected Answer: BC

Write performance will be improved by switch RDS to Aurora. RDS to Aurora is smooth transition without too much on the application side. Answer E will application side not just backend DB.

upvoted 2 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: CE

Option CE and BC. The only reason I choose E over B because said SO. Per AWS, DynamoDB is suitable for IoT (Sensor data and log ingestion)

<https://docs.aws.amazon.com/whitepapers/latest/best-practices-for-migrating-from-rdbms-to-dynamodb/suitable-workloads.html>

upvoted 3 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: CE

CE, kinesis + lambda & Dynamodb

upvoted 1 times

Question #81

A company is building an electronic document management system in which users upload their documents. The application stack is entirely serverless and runs on AWS in the eu-central-1 Region. The system includes a web application that uses an Amazon CloudFront distribution for delivery with Amazon S3 as the origin. The web application communicates with Amazon API Gateway Regional endpoints. The API Gateway APIs call AWS Lambda functions that store metadata in an Amazon Aurora Serverless database and put the documents into an S3 bucket. The company is growing steadily and has completed a proof of concept with its largest customer. The company must improve latency outside of Europe.

Which combination of actions will meet these requirements? (Choose two.)

- A. Enable S3 Transfer Acceleration on the S3 bucket. Ensure that the web application uses the Transfer Acceleration signed URLs.
- B. Create an accelerator in AWS Global Accelerator. Attach the accelerator to the CloudFront distribution.
- C. Change the API Gateway Regional endpoints to edge-optimized endpoints.
- D. Provision the entire stack in two other locations that are spread across the world. Use global databases on the Aurora Serverless cluster.
- E. Add an Amazon RDS proxy between the Lambda functions and the Aurora Serverless database.

Correct Answer: AC

Community vote distribution

AC (59%)	CD (29%)	5%
----------	----------	----

✉  **masetromain**  2 years, 11 months ago

Selected Answer: AC

A and C are correct answers.

- A. Enable S3 Transfer Acceleration on the S3 bucket and ensure that the web application uses the Transfer Acceleration signed URLs will accelerate the uploads of documents to S3 bucket, this will help to reduce the latency for users outside of Europe.
- C. Change the API Gateway Regional endpoints to edge-optimized endpoints will help the company to improve the latency by caching the responses of the API Gateway closer to the users.

upvoted 25 times

✉  **bcx** 2 years, 6 months 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 4 times

✉  **Sab** 2 years, 3 months ago

Users of S3 are not lambda, lambda is used only for writing to serverless database. Also, Aurora serverless global database only writes in one cluster and the other region cluster are used only for reads. So no matter from which location you upload, the metadata will be written to cluster in Central Europe . If it was Global DynamoDB table then it could have helped to reduce latency.

upvoted 2 times

✉  **ninomfr64** 1 year, 11 months ago

"web app uses CloudFront distribution for delivery with Amazon S3 as the origin" and "Lambda functions that store metadata in an Amazon Aurora Serverless database and put the documents into an S3 bucket" these 2 sentences let me think that users are not uploading via CloudFront into the S3 bucket at its origin, rather docs are uploaded from the Lambda

upvoted 3 times

✉  **masetromain** 2 years, 11 months ago

- B. Creating an accelerator in AWS Global Accelerator and attaching it to the CloudFront distribution will not help in this scenario as it only helps to route the traffic to the optimal endpoint based on the location of the user.
- D. Provisioning the entire stack in two other locations that are spread across the world and using global databases on the Aurora Serverless cluster will help to reduce the latency but it would be more complex to implement and manage.
- E. Adding an Amazon RDS proxy between the Lambda functions and the Aurora Serverless database will not help in this scenario because it is only used to improve connection management and load balancing for Amazon RDS databases, but not for Aurora Serverless databases.

upvoted 5 times

✉  **masetromain** 2 years, 11 months ago

<https://www.examtopics.com/discussions/amazon/view/69470-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

✉  **Japanese1** 2 years, 1 month ago

Complexity is not evidence against option D.

Furthermore, option D is correct because the question statement also suggests that costs can be incurred.

On the other hand, A is not a method to eliminate geographical factors.

upvoted 1 times

 **hussainbaloch1002** 11 months, 3 weeks ago

D does not mention how to route traffic

upvoted 1 times

 **e4bc18e** 1 year, 8 months ago

A is wrong because why would you enable transfer acceleration when transfer acceleration uses the CloudFront distribution system. It makes no sense

upvoted 1 times

 **zolthar_z** 1 year, 5 months ago

S3 Global acceleration is used to upload files, so, the users can upload faster the documents in any part of the world

upvoted 1 times

 **phmeeeeee** Most Recent 1 month ago

Selected Answer: BC

"API Gateway APIs call AWS Lambda functions that store metadata in an Amazon Aurora Serverless database and put the documents into an S3 bucket."

User -> API GW -> Lambda -> Aurora for metadata + S3 for files upload

upvoted 1 times

 **Chris_W_1234** 2 months, 2 weeks ago

Selected Answer: BC

The application running on user devices interacts with AWS in two ways: Download static assets via CloudFront, and make API calls against the API GW. Per scenario description, it is the Lambda functions that interact with S3, not the application itself. So, in order to reduce latency incurred by the application, communication with CloudFront and API GW need to be reduced. Answers B and C.

upvoted 2 times

 **princajen** 5 months ago

Selected Answer: AC

A (S3 Transfer Acceleration): Uses CloudFront edge locations to speed up S3 uploads globally. Great for improving document upload performance from users outside Europe.

C (Edge-optimized API Gateway): Replaces regional endpoints to leverage AWS's global edge network, reducing API latency for global users.

Together, these improve performance for global users without major architectural changes or cost increases.

upvoted 1 times

 **AI8282** 5 months, 1 week ago

Selected Answer: CD

Although A will help make uploads faster by uploading the file to the closest edge node in S3 then syncing it in the background slower, D will give them a faster more consistent user experience on all other layers. Going with C and D.

upvoted 1 times

 **caputmundi666** 9 months ago

Selected Answer: CD

CD - for me. I don't understand why S3 Transfer Acceleration is better than D since the transfer from lambda is already on AWS's backbone.

upvoted 1 times

 **ParamD** 9 months, 2 weeks ago

Selected Answer: AC

A is correct because it is with signed url option, lambda will facilitate signed url generation and file will be uploaded directly to S3 with transfer acceleration

upvoted 1 times

 **zolthar_z** 1 year, 5 months ago

Selected Answer: AC

AC will improve latency using AWS edge locations worldwide, adding 2 locations will only benefit those 2 locations

upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

A, C for sure.

B is wrong; AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

upvoted 2 times

 **red_panda** 1 year, 8 months ago

Selected Answer: AC

A and C for me are the correct answers.

D is not so useful as we are recreating the entire stack and increase a lot the costs. As first approach, A and C are the most appropriate upvoted 2 times

 **failexamonly** 1 year, 9 months ago

Selected Answer: AC

Aurora serverless does not support global database. search DB instance class requirements in <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database-getting-started.html>

upvoted 3 times

 **bacharbhouri** 1 year, 7 months ago

it does in V2.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.html#aurora-serverless-v2.advantages> : Using Aurora Serverless v2 - Advantages of Aurora Serverless v2

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: AC

By elimination: B is pointless, as CF already does geo proximity. D is impossible as global DBs aren't supported by Aurora Serverless. E doesn't really help.

Remaining: A and C, which are sensible and will do the trick.

upvoted 2 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: AC

AC, s3 transfer acceleration + edge-optimised api gateway

upvoted 2 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: CD

This is tricky. Here is my take having in mind that the question is "The company must improve latency outside of Europe".

A = Transfer Acceleration improves upload/downlad time, but we have already CloudFront that can also be used to speedup upload. This will not further improve. Also I don't know how to combine TA with CF

B = This will not help and also I don't know how to combine GA with CF

C = correct

D = correct

E = RDS Proxy do not improve latency

upvoted 2 times

 **djeong95** 1 year, 10 months ago

Looks like D is wrong because you don't use global databases on the Aurora Serverless cluster. That is just not a feature given by Aurora Serverless (even v2). However, it does support using Aurora Serverless in global databases. "The secondary clusters" in the link below is a reference to Aurora Global Database.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html#aurora-serverless.ha>: You can use Aurora Serverless v2 capacity in the secondary clusters so they're ready to take over during disaster recovery.

upvoted 1 times

 **djeong95** 1 year, 9 months ago

In addition, we are more likely to get latency from Lambda functions loading documents into S3 from API Gateway calls than we are from Lambda functions loading metadata into Aurora Serverless DB.

<https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

upvoted 1 times

 **grumpysloth** 1 year ago

"Aurora Serverless v2 supports all manner of database workloads. Examples include development and test environments, websites, and applications that have infrequent, intermittent, or unpredictable workloads to the most demanding, business critical applications that require high scale and high availability. It supports the full breadth of Aurora features, including global database, Multi-AZ deployments, and read replicas. Aurora Serverless v2 is available for the Amazon Aurora MySQL-Compatible Edition and PostgreSQL-Compatible Edition."

upvoted 1 times

 **JMAN1** 2 years ago

Selected Answer: CD

Tricky Tricky.

A. Enable S3 Transfer Acceleration on the S3 bucket. Ensure that the web application uses the Transfer Acceleration signed URLs. -> Wrong. No such thing like TA signed URLs.

B. Create an accelerator in AWS Global Accelerator. Attach the accelerator to the CloudFront distribution. -> Wrong GA does not support CF.

C. Change the API Gateway Regional endpoints to edge-optimized endpoints.

D. Provision the entire stack in two other locations that are spread across the world. Use global databases on the Aurora Serverless cluster.
E. Add an Amazon RDS proxy between the Lambda functions and the Aurora Serverless database. -> Wrong. It is not related with latency.
upvoted 3 times

✉ **jpa8300** 1 year, 11 months ago

Yes there is, <https://stackoverflow.com/questions/37437782/aws-transfer-acceleration-with-pre-signed-urls-using-javascript-sdk>
upvoted 1 times

✉ **JMAN1** 1 year, 11 months ago

Sorry. I was wrong. Answer is A C.
serverless does not support global database and RDS proxy.
upvoted 1 times

✉ **JMAN1** 1 year, 11 months ago

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless.html#aurora-serverless.limitations>
upvoted 1 times

✉ **bacharbhouri** 1 year, 7 months ago

it does in V2.
[] <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.html#aurora-serverless-v2.advantages> : Using Aurora Serverless v2 - Advantages of Aurora Serverless v2
upvoted 1 times

✉ **severlight** 2 years, 1 month ago

Selected Answer: AC

see Sab answer
upvoted 1 times

✉ **wookchan** 2 years, 2 months ago

"The company must improve latency outside of Europe."
Then in where are you going to provision an additional stack? It only says "outside of Europe."
USA? Asia? Where?
You have to consider an overall latency.
I'll go for AC
upvoted 1 times

Question #82

An adventure company has launched a new feature on its mobile app. Users can use the feature to upload their hiking and rafting photos and videos anytime. The photos and videos are stored in Amazon S3 Standard storage in an S3 bucket and are served through Amazon CloudFront.

The company needs to optimize the cost of the storage. A solutions architect discovers that most of the uploaded photos and videos are accessed infrequently after 30 days. However, some of the uploaded photos and videos are accessed frequently after 30 days. The solutions architect needs to implement a solution that maintains millisecond retrieval availability of the photos and videos at the lowest possible cost.

Which solution will meet these requirements?

- A. Configure S3 Intelligent-Tiering on the S3 bucket.
- B. Configure an S3 Lifecycle policy to transition image objects and video objects from S3 Standard to S3 Glacier Deep Archive after 30 days.
- C. Replace Amazon S3 with an Amazon Elastic File System (Amazon EFS) file system that is mounted on Amazon EC2 instances.
- D. Add a Cache-Control: max-age header to the S3 image objects and S3 video objects. Set the header to 30 days.

Correct Answer: A

Community vote distribution

A (97%)

✉️  **masetromain** [Highly Voted] 2 years, 5 months ago

Selected Answer: A

The correct answer is A. Configure S3 Intelligent-Tiering on the S3 bucket.

Amazon S3 Intelligent-Tiering is a storage class that automatically moves objects between two access tiers based on changing access patterns. Objects that are accessed frequently are stored in the frequent access tier and objects that are accessed infrequently are stored in the infrequent access tier. This allows for cost optimization without requiring manual intervention. This makes it an ideal solution for the scenario described, as it can automatically move objects that are infrequently accessed after 30 days to a lower-cost storage tier while still maintaining millisecond retrieval availability.

upvoted 16 times

✉️  **masetromain** 2 years, 5 months ago

Option B is not correct as it only moves data to S3 Glacier Deep Archive after 30 days, which would still require additional steps to retrieve the data.

Option C is not correct because Amazon Elastic File System (Amazon EFS) is a file storage service for use with Amazon EC2 instances, it does not provide a cost-effective solution for storing and retrieving large amounts of data.

Option D is not correct because adding a Cache-Control: max-age header only controls the caching behavior of the objects and does not address the cost optimization requirements.

upvoted 3 times

✉️  **jhonivy** 2 years, 5 months ago

Option D works for the reduction cost on retrieval request

upvoted 1 times

✉️  **youngprinceton** 2 years, 5 months ago

take the test then tell us if your answers are valid, if they are share them with us ;)

upvoted 1 times

✉️  **princajen** [Most Recent] 5 months ago

Selected Answer: A

A (S3 Intelligent-Tiering) is the best solution because it automatically transitions objects between storage tiers based on actual access patterns.

It maintains millisecond retrieval, supports unpredictable access patterns, and minimizes storage cost with no operational overhead.

upvoted 1 times

✉️  **Vsos_in29** 1 year, 4 months ago

A is right

B S3 Glacier Deep Archive after 30 days is not correct, retrieval takes time so incorrect.

upvoted 1 times

✉️  **ParamD** 9 months, 2 weeks ago

Another option with S3 Glacier instant retrieval would have made the question very interesting.

upvoted 1 times

✉  **Sandeep_B** 1 year, 8 months ago

Selected Answer: A

millisecond retrieval availability

upvoted 1 times

✉  **wookchan** 1 year, 8 months ago

A, no brainer

upvoted 2 times

✉  **uC6rW1aB** 1 year, 9 months 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 year, 10 months ago

Selected Answer: A

A is right

upvoted 1 times

✉  **aviathor** 1 year, 11 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** 1 year, 12 months ago

Selected Answer: A

A of course

upvoted 1 times

✉  **Maria2023** 2 years 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** 2 years, 3 months ago

Selected Answer: A

A - easy question

upvoted 1 times

✉  **dev112233xx** 2 years, 3 months ago

Selected Answer: A

A - S3 Intelligent-Tiering can fit the requirement

upvoted 1 times

✉  **God_Is_Love** 2 years, 3 months 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** 2 years, 3 months ago

*I meant even after 30 days (not downloads in above comment)

upvoted 1 times

✉  **JungMun** 2 years, 4 months 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** 2 years, 4 months ago

There are lots of wrong types. Please forgive me. English is not familiar with me yet.

upvoted 2 times

✉  **c73bf38** 2 years, 4 months ago

The keyword is millisecond retrieval time, which rules everything out except A.

upvoted 2 times

✉  **klog** 2 years, 4 months 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** 2 years, 5 months ago

Selected Answer: A

typico A S3 Intelligent-Tiering

upvoted 2 times

✉  **jhonivy** 2 years, 5 months ago

D it will reduce the cost on retrieval requests

upvoted 1 times

Question #83

A company uses Amazon S3 to store files and images in a variety of storage classes. The company's S3 costs have increased substantially during the past year.

A solutions architect needs to review data trends for the past 12 months and identify the appropriate storage class for the objects.

Which solution will meet these requirements?

- A. Download AWS Cost and Usage Reports for the last 12 months of S3 usage. Review AWS Trusted Advisor recommendations for cost savings.
- B. Use S3 storage class analysis. Import data trends into an Amazon QuickSight dashboard to analyze storage trends.
- C. Use Amazon S3 Storage Lens. Upgrade the default dashboard to include advanced metrics for storage trends.
- D. Use Access Analyzer for S3. Download the Access Analyzer for S3 report for the last 12 months. Import the .csv file to an Amazon QuickSight dashboard.

Correct Answer: C

Community vote distribution

C (78%) 12% 9%

 **zejou1** Highly Voted 2 years, 9 months 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 15 times

 **Untamables** Highly Voted 2 years, 11 months ago

Selected Answer: C

Both B and C are good.
I guess AWS wants clients to use S3 Storage Lens... Hence I vote C.
upvoted 7 times

 **zozza2023** 2 years, 11 months ago

agree with u gess aws want us to know about Lens
upvoted 3 times

 **princajen** Most Recent 5 months ago

Selected Answer: C

C (S3 Storage Lens with advanced metrics) is the best solution because it offers historical trends, storage class breakdowns, and actionable insights to optimize S3 costs across buckets and regions.

Unlike other tools, it supports up to 15 months of history, meeting the requirement to review 12 months of trends and make informed storage class decisions.

upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

C, for sure.
upvoted 1 times

 **naylinu** 1 year, 7 months ago

B ..S3 Storage Class Analysis is specifically designed to help you analyze storage access patterns. It monitors the access patterns of objects and provides insights into when it is appropriate to transition objects to different storage classes .
upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C

C, S3 Storage Lens offers comprehensive visibility into storage usage and activity trends across the AWS Organization, facilitating informed decisions on cost optimization and storage efficiency

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: C

Option C refers to using Amazon S3 Storage Lens, which provides organization-wide visibility into object storage usage and activity trends. By upgrading to include advanced metrics and recommendations, users can access detailed insights that help optimize storage costs across their S3 resources. S3 Storage Lens offers dashboard views and metrics that can directly inform on the appropriate storage class based on actual usage patterns, making it a comprehensive solution for the stated requirements.

upvoted 1 times

 **AWSPro1234** 1 year, 11 months ago

Amazon S3 Storage Class Analysis:

Amazon S3 provides a Storage Class Analysis tool that helps you analyze access patterns to your S3 objects over time. You can enable it on your S3 bucket to collect data on object access patterns.

upvoted 1 times

 **AWSPro1234** 1 year, 11 months ago

Answer is B.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: C

To me here the key sentence is "review data trends for the past 12 months"

A = CUR provides detailed usage data but it is not the best tool for this job

B = S3 storage class analysis provides recommendation for Standard and Standard IA storage classes, but does not provide data trends

C = correct

D = Access Analyzer provides visibility for buckets that are configured to allow access to anyone on the internet or other AWS accounts

upvoted 1 times

 **Nicoben** 2 years ago

Selected Answer: B

B is the right answer, because it suffices a bucket analysis --> <https://docs.aws.amazon.com/AmazonS3/latest/userguide/analyticss-storage-class.html>

C instead is a solution for a more organization-wide analysis of bucket -->

https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens.html

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: C

see AMohanty answer

upvoted 1 times

 **Simon523** 2 years, 3 months ago

Selected Answer: B

S3 Storage Class Analysis enables you to monitor access patterns across objects to help you decide when to transition data to the right storage class to optimize costs.

upvoted 2 times

 **jpa8300** 1 year, 11 months ago

Storage Class is only used for recommendation for Standard to Standard IA

upvoted 1 times

 **AMohanty** 2 years, 3 months ago

C

Storage Class is only used for recommendation for Standard to Standard IA

upvoted 4 times

 **uC6rW1aB** 2 years, 3 months 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 3 times

 **YodaMaster** 2 years, 5 months 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 years, 5 months ago

Selected Answer: C

a hard one ... I guess C, but could be B :/

upvoted 1 times

Question #84

A company has its cloud infrastructure on AWS. A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts.

What should the solutions architect do to meet these requirements?

- A. Use AWS CloudFormation templates. Add IAM policies to control the various accounts, Deploy the templates across the multiple Regions.
- B. Use AWS Organizations. Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts.
- C. Use AWS Organizations and AWS CloudFormation StackSets. Deploy a Cloud Formation template from an account that has the necessary IAM permissions.
- D. Use nested stacks with AWS CloudFormation templates. Change the Region by using nested stacks.

Correct Answer: C

Community vote distribution

C (100%)

✉  **masetromain**  2 years, 5 months ago

Selected Answer: C

The correct answer is C. Use AWS Organizations and AWS CloudFormation StackSets.

AWS Organizations allows the management of multiple AWS accounts as a single entity and AWS CloudFormation StackSets allows creating, updating, and deleting stacks across multiple accounts and regions in an organization. This solution allows creating a single CloudFormation template that can be deployed across multiple accounts and regions, and also allows for the management of access and permissions for the different accounts through the use of IAM roles and policies in the management account.

upvoted 17 times

✉  **masetromain** 2 years, 5 months ago

Option A and D both use AWS CloudFormation, but do not take into account the management of multiple accounts and regions. Option B uses AWS Organizations but doesn't include the use of CloudFormation StackSets, which is necessary for managing deployments across multiple accounts and regions.

upvoted 6 times

✉  **jpa8300** 1 year, 5 months ago

I agree with what you say here, C is a good choice, but in B they mention Control Tower which is also used to manage multiple accounts, couldn't it be a correct answer also?

upvoted 1 times

✉  **princajen**  5 months ago

Selected Answer: C

C (AWS Organizations + CloudFormation StackSets) is the best solution because StackSets allow automated, centralized deployment of CloudFormation templates across multiple accounts and Regions, which fits the business's expansion and IaC goals.

It enables scalable, governable, and repeatable deployments aligned with AWS best practices.

upvoted 1 times

✉  **nynomfr64** 1 year, 5 months ago

Selected Answer: C

A = cloud work but it is hard

B = Control Tower cannot manage stack deployments across accounts

C = correct

D = nested stack allows to provision resources by using different CloudFormation templates

upvoted 3 times

✉  **totten** 1 year, 8 months ago

Selected Answer: C

Option C is the most suitable. Here's why:

AWS Organizations: AWS Organizations helps you centrally manage multiple AWS accounts, which is especially useful when dealing with multiple Regions and accounts. You can organize your accounts into an organizational structure, apply policies across accounts, and manage billing.

AWS CloudFormation StackSets: StackSets is a CloudFormation feature that enables you to deploy CloudFormation stacks across multiple accounts and Regions with a single CloudFormation template. This simplifies the process of deploying and managing infrastructure consistently across your organization.

upvoted 1 times

✉  **NikkyDicky** 1 year, 12 months ago

Selected Answer: C

C no doubt

upvoted 2 times

✉  **SkyZeroZx** 2 years ago

Selected Answer: C

keywords = AWS Organizations && AWS CloudFormation StackSets.

upvoted 1 times

✉  **rbm2023** 2 years, 1 month 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** 2 years, 3 months ago

Selected Answer: C

Use AWS Organizations and AWS CloudFormation StackSets

upvoted 2 times

✉  **zozza2023** 2 years, 5 months ago

Selected Answer: C

The correct answer is C

upvoted 4 times

Question #85

A company has its cloud infrastructure on AWS. A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts.

What should the solutions architect do to meet these requirements?

- A. Use AWS CloudFormation templates. Add IAM policies to control the various accounts, Deploy the templates across the multiple Regions.
- B. Use AWS Organizations. Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts.
- C. Use AWS Organizations and AWS CloudFormation StackSets. Deploy a Cloud Formation template from an account that has the necessary IAM permissions.
- D. Use nested stacks with AWS CloudFormation templates. Change the Region by using nested stacks.

Correct Answer: C

Community vote distribution

C (100%)

 **masetromain** Highly Voted 1 year, 11 months ago

same question of "Questions #84"

upvoted 18 times

 **yorkicurke** Highly Voted 1 year, 1 month ago

These Site Moderators getting lazy boy!

upvoted 7 times

 **NikkyDicky** Most Recent 1 year, 5 months ago

Selected Answer: C

C. a dup question

upvoted 2 times

 **rbm2023** 1 year, 7 months 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** 1 year, 7 months ago

C:

<https://sanderknape.com/2017/07/cloudformation-stacksets-automated-cross-account-region-deployments/#:~:text=A%20StackSet%20is%20a%20set,deploying%20to%20multiple%20accounts%2Fregions.>

upvoted 1 times

 **Nguyen25183** 1 year, 8 months ago

Thought that my internet was interrupted. then i was wrong =)))

upvoted 4 times

 **Musk** 1 year, 11 months ago

This is repeated :-(

upvoted 2 times

 **tatdatpham** 1 year, 11 months ago

Selected Answer: C

Duplicate question with #84

upvoted 3 times

 **zhangyu20000** 1 year, 11 months ago

C is correct answer

upvoted 3 times

Question #86

Topic 1

A company plans to refactor a monolithic application into a modern application design deployed on AWS. The CI/CD pipeline needs to be upgraded to support the modern design for the application with the following requirements:

- It should allow changes to be released several times every hour.
- It should be able to roll back the changes as quickly as possible.

Which design will meet these requirements?

- A. Deploy a CI/CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances.
- B. 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.
- C. 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.
- D. Roll out the application updates as part of an Auto Scaling event using prebuilt AMIs. Use new versions of the AMIs to add instances, and phase out all instances that use the previous AMI version with the configured termination policy during a deployment event.

Correct Answer: B

Community vote distribution

B (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: B

The correct answer is B. Specifying AWS Elastic Beanstalk to stage in a secondary environment as the deployment target for the CI/CD pipeline of the application and swapping the staging and production environment URLs. This approach allows the company to deploy updates several times an hour and quickly roll back changes as needed.

Option A, Deploying a CI/CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances, while it may provide a way to roll back changes by replacing instances with previous versions, it may not allow for rapid deployment of updates multiple times per hour.

upvoted 19 times

 **masetromain** 2 years, 11 months ago

Option C, Using AWS Systems Manager to re-provision the infrastructure for each deployment. Updating the Amazon EC2 user data to pull the latest code artifact from Amazon S3 and using Amazon Route 53 weighted routing to point to the new environment, would require more time-consuming steps and may not be able to roll back changes as quickly.

Option D, Rolling out the application updates as part of an Auto Scaling event using prebuilt AMIs. Using new versions of the AMIs to add instances and phasing out all instances that use the previous AMI version with the configured termination policy during a deployment event, while it may be a way to roll back changes, it doesn't allow for rapid deployment of updates multiple times per hour.

upvoted 5 times

 **jpa8300** 1 year, 11 months ago

Good explanation, but concerning option C it is not quite right, you say that 'may not be able to roll back changes as quickly.', but since it is using Route 53 weighted configuration, in case of failure of the new instances, you just need to change again the weighted configuration to point 100% to the old instances while you replace again the new instances by old instances.

upvoted 1 times

 **princajen** Most Recent 5 months ago

Selected Answer: B

B (Elastic Beanstalk with staging and URL swapping) is the best solution because it supports fast, automated blue/green deployments, allowing for multiple releases per hour and quick rollback via environment URL swapping.

It simplifies CI/CD and aligns well with a modern application design on AWS.

upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

Selected Answer: B

B, for sure.

Using AWS Elastic Beanstalk environment Swap.

<https://docs.aws.amazon.com/whitepapers/latest/blue-green-deployments/swap-the-environment-of-an-elastic-beanstalk-application.html>

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: B

A = replacing existing EC2 instances does not allow for roll back the changes as quickly as possible
B = correct (tough Beanstalk is not the best service for releasing several times every hour)
C = could work, but here you are combining SSM and user data to achieve what beanstalk does natively
D = this would not work as you need to build AMIs (AMI Builder not mentioned) and also rapid rollback is better achieved avoiding termination of old AMI version

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

probably B

upvoted 1 times

 **rbm2023** 2 years, 7 months 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** 2 years, 9 months ago

Selected Answer: B

B. Specify AWS Elastic Beanstalk

upvoted 1 times

 **Untamables** 2 years, 11 months ago

Selected Answer: B

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 3 times

Question #87

A company has an application that runs on Amazon EC2 instances. A solutions architect is designing VPC infrastructure in an AWS Region where the application needs to access an Amazon Aurora DB Cluster. The EC2 instances are all associated with the same security group. The DB cluster is associated with its own security group.

The solutions architect needs to add rules to the security groups to provide the application with least privilege access to the DB Cluster.

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

- A. Add an inbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the source over the default Aurora port.
- B. Add an outbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the destination over the default Aurora port.
- C. Add an inbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the source over the default Aurora port.
- D. Add an outbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the destination over the default Aurora port.
- E. Add an outbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the destination over the ephemeral ports.

Correct Answer: BC*Community vote distribution*

BC (80%)

AC (20%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: BC

The correct combination of steps to meet these requirements is B and C.

B. Add an outbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the destination over the default Aurora port. This allows the instances to make outbound connections to the DB cluster on the default Aurora port.

C. Add an inbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the source over the default Aurora port. This allows connections to the DB cluster from the EC2 instances on the default Aurora port.

upvoted 33 times

 **masetromain** 2 years, 11 months ago

A. Adding an inbound rule to the EC2 instances' security group would allow incoming connections to the instances on the default Aurora port, but it would not allow the instances to connect to the DB cluster.

D. Adding an outbound rule to the DB cluster's security group would allow the DB cluster to make outbound connections to the EC2 instances on the default Aurora port, but it would not allow connections to the DB cluster from the instances.

E. Adding an outbound rule to the DB cluster's security group specifying the EC2 instances' security group as the destination over the ephemeral ports would allow the DB cluster to make outbound connections to the instances on ephemeral ports, but it would not allow connections to the DB cluster from the instances on the default Aurora port.

upvoted 3 times

 **vjp_training** 2 years, 3 months ago

Security group is stateful. So you just need to set up inbound

upvoted 3 times

 **HussamShokr** 2 years, 6 months ago

why we should add an outbound rule to the EC2 instances' security group??? it is already allowed by default in the EC2 security group because all outbound ports are allowed by default.

upvoted 3 times

 **jainparag1** 2 years, 1 month ago

wow..then in that case your EC2 instance can talk to anything. No SG rule is required. You need to establish a connectivity route first.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

it is the other way around, all connection are denied and you can only allow connection. You need outbound from EC2 to Aurora to allow the app initiate a connection to the database instance

upvoted 2 times

 **c73bf38** Highly Voted 2 years, 10 months ago

Selected Answer: AC

To provide the application with least privilege access to the Aurora DB cluster, the solutions architect should add inbound rules to both the security groups.

For the EC2 instances' security group, an inbound rule should be added that allows traffic from the DB cluster's security group over the default Aurora port. This will allow the EC2 instances to communicate with the Aurora DB cluster.

For the Aurora DB cluster's security group, an inbound rule should be added that allows traffic from the EC2 instances' security group over the default Aurora port. This will allow the Aurora DB cluster to communicate with the EC2 instances.

By default all outbound rules are open, it's only the ingress that needs to allow traffic.

upvoted 12 times

 **c73bf38** 2 years, 10 months ago

B&C after doing a recreate in the AWS Console, stand corrected.

upvoted 7 times

 **c73bf38** 2 years, 10 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 3 times

 **b0969fd** Most Recent 2 months, 1 week ago

Selected Answer: BC

For those choosing A, at what point does a database initiate the network call first before the application? It's always the application the first to initiate the network call so EC2 -> Outbound SG ->DB and DB <- Inbound <- EC2

upvoted 1 times

 **princajen** 5 months ago

Selected Answer: BC

B: Allows EC2 to send traffic to Aurora over the correct port — outbound rule.

C: Allows Aurora to receive traffic from EC2 — inbound rule.

Together, these provide least privilege access, only enabling the EC2 instances to initiate DB connections over the required port.

upvoted 1 times

 **penguins2** 1 year, 1 month ago

BC. The steps are clearly stated here: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/tutorial-ec2-rds-option3.html#option3-task3-connect-rds-database-to-ec2-instance>

upvoted 1 times

 **nimbus_00** 1 year, 2 months ago

Selected Answer: BC

NB. The DB cluster doesn't need to initiate connections to the EC2 instances.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: BC

BC, ec2 -> bd; ec2 outbound rule to allow access to bd; db inbound rule to allow access from ec2

upvoted 2 times

 **igor12ghsj577** 1 year, 10 months ago

Selected Answer: BC

Tricky question. They say with least privileges, so I think they don't want to use default (allow-all) rule, but limit as much as possible and allow only specific traffic to DB)

"By default, a security group includes an outbound rule that allows all outbound traffic. We recommend that you remove this default rule and add outbound rules that allow specific outbound traffic only."

<https://docs.aws.amazon.com/quicksight/latest/user/vpc-security-groups.html>

upvoted 3 times

 **cox1960** 1 year, 11 months ago

CE

- A and B are nonsense, since they talk about aurora port on ec2 SGs. In SG you always put rules on the local ports.
- C obvious
- E over D, always ephemeral on outbound, but at the condition we replace the existing all open rule

upvoted 1 times

✉  **jpa8300** 1 year, 11 months ago

Selected Answer: BC

I believe that C is enough, we don't need to define the outbound from EC2 to DB, but since we have to choose two, the only other option that is correct is B. And someone say below that have tested this configuration, so I hope he tested defining only what is mentioned in C, to see if it is enough or not. It would be nice.

upvoted 3 times

✉  **shaaam80** 2 years ago

Selected Answer: BC

Answer - B&C

Outbound rule to the EC2 SG with DB SG as destination

Inbound rule to the DB SG with EC2 SG as source

upvoted 1 times

✉  **eurriola10** 2 years ago

Selected Answer: AC

Security Groups are stateful, that means you don't need to specify an outbound rule if you have an inbound rule that permit access to the resource. <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html#security-group-basics>

In other hand, the outbound traffic rules typically don't apply to DB clusters. Outbound traffic rules apply only if the DB cluster acts as a client.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Overview.RDSSecurityGroups.html#Overview.RDSSecurityGroups.VPC.Sec>.

Because of that B, D and E are wrong answers

upvoted 1 times

✉  **uC6rW1aB** 2 years, 3 months ago

Selected Answer: AC

By default, AWS Security Groups allow all outbound traffic. Therefore, in most cases, there's no need to configure outbound rules unless you have specific security requirements.

Add an inbound rule to the EC2 instance's security group, setting the DB cluster's security group as the source over Aurora's default port. This enables interaction between the DB Cluster and the EC2 instances. Corresponds to Option A.

Add an inbound rule to the DB Cluster's security group, setting the EC2 instance's security group as the source over Aurora's default port. This allows the EC2 instances to interact with the DB Cluster. Corresponds to Option C.

upvoted 2 times

✉  **uC6rW1aB** 2 years, 3 months ago

By the way, the outbound rules are unnecessary in this case because the database cluster does not need to access any data from the application. The database cluster only needs to receive traffic from the application so that the application can read and write to the database.

upvoted 1 times

✉  **eurriola10** 2 years ago

my two cents.

Agree AC are the correct answer.

Security Groups are stateful, that means you don't need to specify an outbound rule if you have an inbound rule that permit access to the resource. <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html#security-group-basics>

In other hand, the outbound traffic rules typically don't apply to DB clusters. Outbound traffic rules apply only if the DB cluster acts as a client.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Overview.RDSSecurityGroups.html#Overview.RDSSecurityGroups.VPC.Sec>

upvoted 1 times

✉  **vjp_training** 2 years, 4 months ago

Selected Answer: AC

By default, all outbound rules are allow

upvoted 1 times

✉  **vn_thanh tung** 2 years, 3 months ago

Don't provide wrong answer. Answer is B,C

upvoted 1 times

✉  **jainparag1** 2 years, 1 month ago

you are providing the wrong answer. The correct answer is AC. Inbound rules are supposed to be added.

upvoted 1 times

✉  **vn_thanh tung** 2 years, 3 months 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 years, 5 months ago

Selected Answer: BC

BC of course
upvoted 2 times

 **jainparag1** 2 years, 1 month ago
AC is correct.
upvoted 1 times

 **bcx** 2 years, 6 months 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** 2 years, 7 months ago

Selected Answer: BC

"My choice relays 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

Question #88

Topic 1

A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overall cloud spending with the head of each business unit. The company uses AWS Organizations to manage the separate AWS accounts for each business unit. The existing tagging standard in Organizations includes the application, environment, and owner. The cloud governance team wants a centralized solution so each business unit receives monthly reports on its cloud spending. The solution should also send notifications for any cloud spending that exceeds a set threshold.

Which solution is the MOST cost-effective way to meet these requirements?

- A. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in each account to create monthly reports for each business unit.
- B. Configure AWS Budgets in the organization's management account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's management account to create monthly reports for each business unit.
- C. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit.
- D. Enable AWS Cost and Usage Reports in the organization's management account and configure reports grouped by application, environment, and owner. Create an AWS Lambda function that processes AWS Cost and Usage Reports, sends budget alerts, and sends monthly reports to each business unit's email list.

Correct Answer: B

Community vote distribution

B (100%)

 **masetromain** Highly Voted 1 year, 11 months ago

Selected Answer: B

B. Configure AWS Budgets in the organization's management account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's management account to create monthly reports for each business unit.

This option is the most cost-effective because it utilizes the organization's management account to set budgets and configure alerts for all accounts in the organization, rather than having to configure budgets and alerts individually in each account. Additionally, using Cost Explorer in the management account allows the cloud governance team to view the consolidated spending for all accounts in the organization and create reports for each business unit. This eliminates the need to access each individual account to view costs and create reports.

upvoted 26 times

 **masetromain** 1 year, 11 months ago

Option A is not the most cost-effective solution because it requires configuring budgets and reports in multiple accounts, which increases the complexity and cost of managing the cloud spending for each business unit.

Option C is not the most cost-effective solution because it requires the cloud governance team to access the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit, which increases the complexity and cost of managing the cloud spending for each business unit.

Option D is not the most cost-effective solution because it requires creating an AWS Lambda function to process AWS Cost and Usage Reports, which increases the complexity and cost of managing the cloud spending for each business unit.

upvoted 6 times

 **princaben** Most Recent 5 months ago

Selected Answer: B

B provides a centralized, low-maintenance, and cost-effective approach by using:

AWS Budgets and Cost Explorer in the management account

Tag-based tracking (application, environment, owner)

SNS alerts for overspend thresholds

Monthly report generation in one place

upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: B

B for sure

upvoted 1 times

 **Maria2023** 1 year, 6 months 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 year, 4 months ago

Billing > Budgets > Create budget > Customize (advanced) > Budget scope > Filter specific AWS cost dimensions

upvoted 1 times

 **SkyZeroZx** 1 year, 6 months ago

Selected Answer: B

keyword = AWS Budgets in the organization's management
other more overhead each by account

upvoted 2 times

 **yama234** 1 year, 8 months 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 4 times

 **mfsec** 1 year, 9 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.

Correct Answer: A

Community vote distribution

A (86%)

14%

 **zejou1**  2 years, 9 months 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 17 times

 **princajen**  5 months ago

Selected Answer: A

A (`DeletionPolicy`) is the correct answer because it is the native CloudFormation mechanism for retaining critical resources like RDS databases and EBS volumes when a stack is deleted.

You can set `DeletionPolicy`: `Retain` or `Snapshot` depending on the resource and desired behavior, ensuring data is not lost even if the stack is removed.

upvoted 1 times

 **nimbus_00** 1 year, 2 months ago

Selected Answer: A

By adding the `DeletionPolicy` attribute to the CloudFormation template for RDS and EBS resources, you can specify actions to be taken when a stack is deleted. Setting the `DeletionPolicy` to `Retain` ensures that the RDS and EBS resources are not deleted when the CloudFormation stack is deleted.

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: A

Option A is the correct approach because CloudFormation allows you to specify a `DeletionPolicy` attribute for resources within your templates. This attribute can prevent resources like Amazon RDS databases and Amazon EBS volumes from being deleted when the stack is deleted. You can set the `DeletionPolicy` to "Retain" for specific resources, ensuring they are not automatically removed alongside the stack.

upvoted 1 times

 **Maygam** 2 years ago

Selected Answer: B

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/protect-stack-resources.html>

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

A, basic `DeletionPolicy` use case

upvoted 2 times

 **aviathor** 2 years, 3 months ago

Yes but should be supplemented with deletion protection on the database.

upvoted 2 times

 **Maria2023** 2 years, 6 months ago

Selected Answer: A

Although that I would preferably use both A and B - this is an exam and the truth is in the wording - "important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted" - we don't care if the resources are deleted but the data, which makes me believe they want us to set up a deletion policy at a resource level to "Retain"

upvoted 2 times

 **zak340** 2 years, 6 months ago

Selected Answer: B

Explanation:

Stack policies are a powerful feature of AWS CloudFormation that allows you to control fine-grained permissions for resources within a stack. By configuring a stack policy that disallows the deletion of RDS and EBS resources, you can prevent users from accidentally deleting these critical resources and the associated data.

Option A (Modifying CloudFormation templates with DeletionPolicy attribute) is not the best solution in this case. While the DeletionPolicy attribute can be used to control resource behavior during stack deletion, it is not applicable to Amazon RDS instances or Amazon EBS volumes.

upvoted 2 times

 **bcox** 2 years, 6 months ago

The correct answer is A, not because what you say is wrong, but because the question states that the stacks can be deleted, you cannot prevent the deletion of the stack (as required by the question). So the DeletionPolicy will let you delete the stack and retain or take a snapshot of the Database/BUCKET/... (whichever is applicable). You will not lose any data in that case and the stack would have been successfully deleted.

upvoted 3 times

 **fartosh** 1 year, 7 months ago

> the DeletionPolicy attribute [...] is not applicable to Amazon RDS instances or Amazon EBS volumes.

This statement is false. From <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html>

Retain

[...] You can add this deletion policy to any resource type.

Snapshot

Resources that support snapshots include:

[...]

- AWS::EC2::Volume

[...]

- AWS::RDS::DBInstance

upvoted 1 times

 **rbm2023** 2 years, 7 months ago

Selected Answer: A

Check the differences and use cases where to use a stack policy or add a deletion policy (retain):

Stack policy and deletion policy are both ways to protect resources created by CloudFormation stacks, but they have different functions. Stack policy is a feature that allows you to specify a JSON policy document that restricts what actions can be taken on a CloudFormation stack. Stack policies are used to prevent accidental or intentional updates or deletions of critical resources in your stack, by specifying which resources can be modified and by whom. Stack policies can be used to allow specific teams or individuals to modify specific resources in a stack while preventing them from modifying others.

upvoted 3 times

 **rbm2023** 2 years, 7 months ago

Deletion policy, on the other hand, is a property of certain AWS resources that determines what happens to the resource when the stack is deleted. The deletion policy can be set to one of three values: "Delete", "Retain", or "Snapshot". When the deletion policy is set to "Delete", the resource is deleted when the stack is deleted. When the deletion policy is set to "Retain", the resource is not deleted when the stack is deleted, but must be deleted manually. When the deletion policy is set to "Snapshot", the resource is deleted when the stack is deleted, but a snapshot of the resource is retained.

In summary, stack policies are used to control what changes can be made to a stack, while deletion policies are used to determine what happens to resources when a stack is deleted.

upvoted 1 times

 **OCHT** 2 years, 8 months ago

Selected Answer: B

option 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** 2 years, 8 months 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** 2 years, 9 months ago

Selected Answer: A

A for sure

upvoted 2 times

 **kiran15789** 2 years, 9 months 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** 2 years, 9 months 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** 2 years, 10 months ago

Selected Answer: A

Clear A

upvoted 1 times

 **lunt** 2 years, 10 months 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** 2 years, 10 months ago

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/protect-stack-resources.html>

upvoted 1 times

 **AC1984** 2 years, 10 months 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** 2 years, 10 months 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

Question #90

Topic 1

A company has VPC flow logs enabled for its NAT gateway. The company is seeing Action = ACCEPT for inbound traffic that comes from public IP address 198.51.100.2 destined for a private Amazon EC2 instance.

A solutions architect must determine whether the traffic represents unsolicited inbound connections from the internet. The first two octets of the VPC CIDR block are 203.0.

Which set of steps should the solutions architect take to meet these requirements?

- A. Open the AWS CloudTrail console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- B. Open the Amazon CloudWatch console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- C. Open the AWS CloudTrail console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- D. Open the Amazon CloudWatch console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.

Correct Answer: B*Community vote distribution*

B (58%)

D (42%)

 **vsk12** Highly Voted 2 years, 11 months ago

I would go with option B. Source will be public IP like 198.51.100.2.
upvoted 23 times

 **kiran15789** Highly Voted 2 years, 9 months 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 21 times

 **zejou1** 2 years, 9 months ago

For those that are choosing D - this is why D is incorrect and needs to be B
upvoted 2 times

 **sashenka** 1 year, 1 month ago

To determine whether the traffic represents unsolicited inbound connections from the internet, use 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". This approach helps you analyze the VPC flow logs to identify if the inbound traffic to the private EC2 instance is expected return traffic or unsolicited. The stats command can be used to filter the sum of bytes transferred by the source address and the destination address, providing insight into the traffic patterns and ensuring network security.

upvoted 1 times

 **sashenka** 1 year, 1 month ago

It has to be D as it only includes unsolicited traffic. Option B includes both.

upvoted 1 times

 **vinalt** Most Recent ⓘ 1 month ago

Selected Answer: D

we have to check if this is unsolicited connection. the only way to check that is if there was no initial request from vpc to destination. If there was, the accept in the flow log is for return traffic. if there is none, we can safely assume it is unsolicited request. you would see all unsolicited requests as accepted on flow logs and then they will get dropped.

upvoted 1 times

 **princajen** 5 months ago

Selected Answer: B

Use Amazon CloudWatch Logs to query VPC flow logs (not CloudTrail).

To verify if a public IP (198.51.100.2) initiated unsolicited inbound traffic, filter for:

source = 198.51.100.2

destination = internal CIDR 203.0.x.x

This shows whether the traffic originated externally, and whether the internal host initiated it or not.

upvoted 1 times

 **papan83** 7 months, 3 weeks ago

Selected Answer: D

Step-by-Step Approach:

You already have this log entry:

srcaddr = 198.51.100.2

dstaddr = 203.0.x.x

action = ACCEPT

Now, query CloudWatch Logs for the reverse flow:

srcaddr = 203.0.x.x (your EC2 instance)

dstaddr = 198.51.100.2 (the public IP)

If you find outbound traffic from your instance to the public IP before the inbound traffic, then the connection is solicited (i.e. it's a reply).

If you do not find any outbound flow to that public IP, then the traffic is unsolicited — a potentially unexpected or malicious inbound attempt that should have been blocked.

upvoted 6 times

 **BennyMao** 9 months, 3 weeks ago

Selected Answer: D

The NAT gateway allows outbound internet traffic from private instances but does not accept unsolicited inbound connections.

If 198.51.100.2 is contacting the private instance, we need to determine if this is a response to an existing outbound request from the private instance.

upvoted 1 times

 **BennyMao** 9 months, 3 weeks ago

Selected Answer: D

The NAT gateway allows outbound internet traffic from private instances but does not accept unsolicited inbound connections.

If 198.51.100.2 is contacting the private instance, we need to determine if this is a response to an existing outbound request from the private instance.

upvoted 2 times

 **grumpysloth** 1 year ago

Selected Answer: D

we need to check if the request starts from ec2 instances outbound, not the other way round.

upvoted 1 times

 **youonebe** 1 year, 1 month ago

Correct answer is D.

This is for NAT traffic analysis, so the focus is outbound.

VPC Flow Logs are published to CloudWatch Logs, not CloudTrail1. This immediately eliminates options A and C.

To determine if the traffic is unsolicited inbound connections:

We need to check if the private EC2 instance (starting with 203.0) initiated the connection to 198.51.100.2

If the source IP is from the VPC (203.0) and the destination is 198.51.100.2, this indicates the connection was initiated from inside the VPC. This would mean the ACCEPT traffic is a response to an outbound request, not unsolicited inbound traffic.

upvoted 3 times

 **tural_nasirov** 1 year, 1 month ago

Selected Answer: B

The answer is B.

This is not about an IP but about a port. If the packet from outside to inside has the source port which is well known and the destination port dynamic, it means that the connection was initiated from inside, if the packet from outside to inside has a source port dynamic and destination port well known, it means that the traffic was originated from outside :)

upvoted 1 times

 **sashenka** 1 year, 1 month ago

Selected Answer: D

Why Option B is Problematic:

```
// Example CloudWatch Logs Insights Query for Option B
fields @timestamp, sourceAddress, destinationAddress, action, bytes
| filter destinationAddress like "203.0"
| filter sourceAddress like "198.51.100.2"
| stats sum(bytes) by sourceAddress, destinationAddress
```

1. Incorrect Traffic Direction

- It looks for traffic where source = 198.51.100.2 (internet) and destination = 203.0.x.x (VPC)

This only shows successful inbound connections (ACCEPT)

It doesn't reveal whether these connections were solicited or unsolicited

2. Missing Context

- Doesn't show the initial outbound connection that would indicate a solicited response
- Cannot differentiate between legitimate responses and actual unsolicited connections
- Lacks the temporal relationship between outbound and inbound flows

upvoted 3 times

 **sashenka** 1 year, 1 month ago

Better Approach (Option D)

sql

```
// Example CloudWatch Logs Insights Query for Option D
fields @timestamp, sourceAddress, destinationAddress, action, bytes
| filter sourceAddress like "203.0"
| filter destinationAddress like "198.51.100.2"
| stats sum(bytes) by sourceAddress, destinationAddress
```

This query would:

Show outbound traffic from VPC to the internet

Help establish if the private instance initiated communication

Allow correlation between outbound requests and inbound responses

Key Concept

With NAT gateway connections:

Legitimate traffic follows a request-response pattern

Outbound request must exist before inbound response

Looking only at inbound traffic (Option B) misses this crucial relationship

Therefore, Option D provides the necessary visibility to determine if the inbound connections were truly unsolicited by examining the outbound traffic first.

upvoted 2 times

 **sammyhaj** 1 year, 1 month ago

D, we need to see if the internal origin was first used

upvoted 3 times

 **NirvanaSNM** 1 year, 5 months ago

Selected Answer: B

destination address set as "like 203.0" and the source address set as "like 198.51.100.2"

upvoted 1 times

 **mns0173** 1 year, 5 months ago

Of course it is D. What useful info will you get from B? You need to check original request which in case of NAT is always EC2, not something in the internet.

upvoted 2 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: B

I vote B. Because the network traffic to check is unsolicited inbound connection. IT is initiated from the internet to internal EC2. The source is public IP address and the target is internal IP.

upvoted 1 times

 **higashikumi** 1 year, 6 months ago

Selected Answer: B

To determine whether the traffic represents unsolicited inbound connections from the internet, use 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". This approach helps you analyze the VPC flow logs to identify if the inbound traffic to the private EC2 instance is expected return traffic or unsolicited. The stats

command can be used to filter the sum of bytes transferred by the source address and the destination address, providing insight into the traffic patterns and ensuring network security.

upvoted 1 times

 **Vongolatt** 1 year, 8 months ago

Selected Answer: D

the solution architect want to check if it's unsolicited traffic or not, so we need to check the if the request is sent by us. which means 198.51.100.2 should be the destination.

upvoted 3 times

Question #91

A company consists of two separate business units. Each business unit has its own AWS account within a single organization in AWS Organizations. The business units regularly share sensitive documents with each other. To facilitate sharing, the company created an Amazon S3 bucket in each account and configured low-way replication between the S3 buckets. The S3 buckets have millions of objects.

Recently, a security audit identified that neither S3 bucket has encryption at rest enabled. Company policy requires that all documents must be stored with encryption at rest. The company wants to implement server-side encryption with Amazon S3 managed encryption keys (SSE-S3).

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

- A. Turn on SSE-S3 on both S3 buckets. Use S3 Batch Operations to copy and encrypt the objects in the same location.
- B. Create an AWS Key Management Service (AWS KMS) key in each account. Turn on server-side encryption with AWS KMS keys (SSE-KMS) on each S3 bucket by using the corresponding KMS key in that AWS account. Encrypt the existing objects by using an S3 copy command in the AWS CLI.
- C. Turn on SSE-S3 on both S3 buckets. Encrypt the existing objects by using an S3 copy command in the AWS CLI.
- D. Create an AWS Key Management Service (AWS KMS) key in each account. Turn on server-side encryption with AWS KMS keys (SSE-KMS) on each S3 bucket by using the corresponding KMS key in that AWS account. Use S3 Batch Operations to copy the objects into the same location.

Correct Answer: A*Community vote distribution*

A (90%)	7%
---------	----

 **testingaws123** Highly Voted 2 years, 9 months ago

Selected Answer: A

Answer is A

Keyword is "The S3 buckets have millions of objects"

If there are million of objects then you should use Batch operations.

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

upvoted 29 times

 **forceli** 2 years, 9 months ago

good point, changing my answer to A

upvoted 1 times

 **princajen** Most Recent 5 months ago

Selected Answer: A

Current Setup:

Two AWS accounts (1 per business unit), under a single AWS Organization.

Each account has its own S3 bucket.

Buckets replicate data between each other.

Buckets have millions of objects.

SSE is not enabled.

New Requirement:

Use SSE-S3 (Amazon S3-managed encryption keys, not SSE-KMS).

Must encrypt existing objects as well (not just new ones).

Needs to be operationally efficient.

The most operationally efficient way to enable encryption at rest with SSE-S3 on existing S3 buckets containing millions of objects is to enable SSE-S3 on the buckets and use S3 Batch Operations to copy the objects in place, which triggers automatic encryption during the copy.

upvoted 1 times

 **mnsait** 1 year, 1 month ago

This is outdated now.

"Amazon S3 now applies server-side encryption with Amazon S3 managed keys (SSE-S3) as the base level of encryption for every bucket in Amazon S3. Starting January 5, 2023, all new object uploads to Amazon S3 are automatically encrypted at no additional cost and with no impact on performance."

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html>

upvoted 1 times

 **nimbus_00** 1 year, 2 months ago

Selected Answer: A

S3 Batch Operations can be used to efficiently apply changes to a large number of objects in a bucket, including copying and encrypting them in place. This is ideal for retroactively encrypting millions of existing objects without needing to manually handle them one by one.

upvoted 1 times

 **ajeeshb** 1 year, 9 months ago

I understand S3 Batch operations is required. But why no one is choosing SSE-KMS?

upvoted 1 times

 **StevePace** 1 year, 9 months ago

Because the question states the company wants to use SSE-S3, nowhere does it mention SSE-KMS

upvoted 3 times

 **TonytheTiger** 1 year, 9 months ago

To encrypt your existing unencrypted Amazon S3 objects, you can use Amazon S3 Batch Operations. You provide S3 Batch Operations with a list of objects to operate on, and Batch Operations calls the respective API to perform the specified operation. You can use the Batch Operations Copy operation to copy existing unencrypted objects and write them back to the same bucket as encrypted objects. A single Batch Operations job can perform the specified operation on billions of objects.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html>

upvoted 2 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: A

A = correct (see <https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>)

B = KMS is for SSE-KMS not for the requested SSE-S3

C = CLI is less efficient than S3 Batch

D = see answer B

upvoted 4 times

 **career360guru** 2 years ago

Selected Answer: A

A is the right answer

upvoted 1 times

 **jainparag1** 2 years, 1 month ago

Selected Answer: A

Correct answer should be A. But this question seem too old to be true now since SSE-S3 based encryption is by default enabled and can't be disabled (you can change however) since Jan 2023.

upvoted 4 times

 **covabix879** 2 years, 2 months ago

Selected Answer: D

Since SSE-S3 does not support cross-account replication, answer should be D

upvoted 2 times

 **deivid83** 2 years, 3 months ago

In a cross-account scenario, where the source and destination buckets are owned by different AWS accounts, you can use a KMS key to encrypt object replicas. However, the KMS key owner must grant the source bucket owner permission to use the KMS key.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html#replication-kms-cross-acct-scenario>

S3 Batch operation:

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

upvoted 3 times

 **uC6rW1aB** 2 years, 3 months ago

Selected Answer: A

S3 Batch operation is the MOST operationally efficient way for millions objects

upvoted 1 times

 **sachstarinfoaws** 2 years, 5 months ago

Selected Answer: A

Answer is A

upvoted 1 times

✉  **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

A more efficient

upvoted 1 times

✉  **Maria2023** 2 years, 6 months ago

Selected Answer: A

I vote for A. Batch operations is better for such a high number of objects

upvoted 1 times

✉  **rbm2023** 2 years, 7 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

The launch of S3 default encryption feature automate the work of encrypting new objects, and you asked for similar, straightforward ways to encrypt existing objects in your buckets. While tools and scripts exist to do this work, each one requires some development work to set up. S3 batch operations gives you a solution for encrypting large number of archived files.

This can also be done by CLI, Option C, however, the same article refers to Batch Operations in case you have a large bucket with millions of objects.

<https://aws.amazon.com/blogs/storage/encrypting-existing-amazon-s3-objects-with-the-aws-cli/>

Option A should be the most efficient, even though it has more operational cost to implement but the question is the about efficiency, it would take to much time to complete this using CLI (Option C).

upvoted 2 times

✉  **mfsec** 2 years, 9 months ago

Selected Answer: A

A is much more efficient

upvoted 1 times

Question #92

A company is running an application in the AWS Cloud. The application collects and stores a large amount of unstructured data in an Amazon S3 bucket. The S3 bucket contains several terabytes of data and uses the S3 Standard storage class. The data increases in size by several gigabytes every day.

The company needs to query and analyze the data. The company does not access data that is more than 1 year old. However, the company must retain all the data indefinitely for compliance reasons.

Which solution will meet these requirements MOST cost-effectively?

- A. Use S3 Select to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- B. Use Amazon Redshift Spectrum to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- C. Use an AWS Glue Data Catalog and Amazon Athena to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- D. Use Amazon Redshift Spectrum to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Intelligent-Tiering.

Correct Answer: C

Community vote distribution

C (93%)	5%
---------	----

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: C

The correct answer is C. Use an AWS Glue Data Catalog and Amazon Athena to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.

This solution allows you to use Amazon Athena and the AWS Glue Data Catalog to query and analyze the data in an S3 bucket. Amazon Athena is a serverless, interactive query service that allows you to analyze data in S3 using SQL. The AWS Glue Data Catalog is a managed metadata repository that can be used to store and retrieve table definitions for data stored in S3. Together, these services can provide a cost-effective way to query and analyze large amounts of unstructured data. Additionally, by using an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive, you can retain the data indefinitely for compliance reasons while also reducing storage costs.

upvoted 21 times

 **masetromain** 2 years, 11 months ago

The other options are not correct because:

A. Using S3 Select is good for filtering data in S3, but it may not be a suitable solution for querying and analyzing large amounts of data.

B. Amazon Redshift Spectrum can be used to query data stored in S3, but it may not be as cost-effective as using Amazon Athena for querying unstructured data

D. Using Amazon Redshift Spectrum with S3 Intelligent-Tiering could be a good solution, but S3 Intelligent-Tiering is designed to optimize storage costs based on access patterns and it would not be the best solution for compliance reasons as S3 Intelligent-Tiering will move data to other storage classes according to access patterns.

upvoted 9 times

 **Japanese1** 2 years ago

This is a nonsense explanation.

In the first place, Redshift cannot handle unstructured data.

upvoted 4 times

 **dankositzke** 1 year, 10 months ago

Amazon Redshift is designed for structured data. However, Amazon Redshift Spectrum enables you to run queries against exabytes of unstructured data in Amazon S3, with no loading or ETL required.

upvoted 3 times

 **Untamables** Highly Voted 2 years, 11 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 7 times

princajen Most Recent 5 months ago

Selected Answer: C

Why C is the best:
Amazon Athena:

Serverless SQL engine that queries data directly from S3, great for unstructured data (e.g., CSV, JSON, Parquet).

Works seamlessly with AWS Glue Data Catalog, which helps define schema and manage metadata.

No need to load data into a separate DB, saving time and cost.

S3 Lifecycle + Glacier Deep Archive:

Data older than 1 year is rarely accessed → S3 Glacier Deep Archive is the cheapest option for long-term storage.

Data is retained indefinitely at very low cost.

This combo meets both the analytics need and long-term cost optimization.

upvoted 1 times

GabrielShiao 1 year, 2 months ago

Selected Answer: C

B, C seem both acceptable. The reason C is selected is because redshift spectrum need Glue Data Catalog as well which is not mentioned there.

upvoted 1 times

gofavad926 1 year, 9 months ago

Selected Answer: C

C, aws glue + amazon athena

upvoted 1 times

AimarLeo 1 year, 11 months ago

Many comments were not convincing of not using Redshift Spectrum.. the only reason I see it to exclude that option is a Redshift Spectrum MUST have a Redshift Cluster available to start the query to S3..

upvoted 1 times

djeong95 1 year, 9 months ago

This question is actually pretty difficult since both Redshift Spectrum and AWS Glue + Athena could query unstructured data. Redshift Spectrum and Athena actually cost about the same per TB. However, with Athena, you could lower the cost by compressing the data. Glue doesn't seem to cost that much either.

<https://aws.amazon.com/redshift/pricing/>
<https://aws.amazon.com/athena/pricing/>
<https://aws.amazon.com/glue/pricing/>

upvoted 1 times

ninomfr64 1 year, 11 months ago

Selected Answer: C

A = S3 Select good for filtering and retrieve subset of data, not enough to analyze

B = need a Redshift instance that is expensive

C = correct (Glue Data Catalog can help putting some structure to data and Athena is good for both query and analytics, transition to Deep Archive after 1 year)

D = see answer B + Intelligent-Tiering not the best option here

upvoted 2 times

nzin4x 1 year, 11 months ago

redshift spectrum vs athena: <https://www.upsolver.com/blog/aws-serverless-redshift-spectrum-athena>

Both are good solutions to query s3 data. However, redshift spectrum is useful for joining S3 data with other data in Redshift, and if the data is only in S3, it would be preferable to choose athena.

upvoted 1 times

career360guru 2 years ago

Selected Answer: C

C is the right answer as Data needs to be queried and Analyzed.

upvoted 2 times

subupro 2 years ago

Athena and aws glue is more cost , so better go with A . and what is the purpose for aws glue here. AWS glue is for ETL purpose unnecessary

upvoted 1 times

Andy16240 2 years, 1 month ago

C correct: S3 copy command in AWS CLI is less operational processes than the batch operation.

upvoted 1 times

 **uC6rW1aB** 2 years, 3 months ago

Selected Answer: C

In this particular scenario, using Amazon Athena and AWS Glue Data Catalog might be a better fit due to the large amount of data stored in S3 buckets and growing every day. Athena can query data across an entire S3 bucket or across multiple buckets, which is useful when parsing multiple files and large amounts of data.

upvoted 2 times

 **chico2023** 2 years, 4 months ago

Selected Answer: C

Answer: C

Criminally tricky question. S3 Select does the same thing as Athena but there are some differences. The key here is "...a large amount of unstructured data..."

If wasn't this, S3 Select hands down.

upvoted 3 times

 **chico2023** 2 years, 4 months ago

Using an Olabiba to explain the differences between the two:

1. Query Capability: Amazon Athena is a fully managed interactive query service that allows you to run SQL queries directly on your data in S3. It supports complex queries, joins, aggregations, and even nested data structures. Athena is designed for ad-hoc querying and analysis of large datasets.

On the other hand, S3 Select is a feature of Amazon S3 that allows you to retrieve a subset of data from an object using SQL expressions. It is primarily used for selective retrieval of specific data within an object, rather than running complex queries across multiple objects.

upvoted 2 times

 **chico2023** 2 years, 4 months ago

2. Data Format: Amazon Athena supports various data formats such as CSV, JSON, Parquet, Avro, and more. It can automatically infer the schema of your data or you can provide a schema explicitly. Athena can handle structured, semi-structured, and unstructured data.

S3 Select, on the other hand, is limited to querying CSV, JSON, and Parquet files. It requires the data to be in a specific format and does not support nested data structures.

upvoted 2 times

 **chico2023** 2 years, 4 months ago

3. Performance: Amazon Athena is optimized for running queries on large datasets and can parallelize the query execution across multiple nodes. It automatically scales resources based on the query complexity and data size, providing fast and efficient query performance.

S3 Select, on the other hand, is designed for retrieving a subset of data from an object. It can significantly reduce the amount of data transferred over the network and improve query performance by only retrieving the necessary data.

4. Cost: Both Amazon Athena and S3 Select have different pricing models. Amazon Athena charges based on the amount of data scanned by your queries, while S3 Select charges based on the amount of data selected and returned by your queries. The cost will depend on the size of your data and the complexity of your queries.

upvoted 3 times

 **Jonalb** 2 years, 5 months ago

Selected Answer: C

its a C , true question!

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

C for sure

upvoted 1 times

 **johnballs221** 2 years, 7 months ago

Selected Answer: B

redshift spectrum can run sql queries directly on s3

upvoted 1 times

 **rxhan** 2 years, 6 months ago

Not the best for cost.

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

C is the best choice for unstructured data

upvoted 3 times

Question #93

Topic 1

A video processing company wants to build a machine learning (ML) model by using 600 TB of compressed data that is stored as thousands of files in the company's on-premises network attached storage system. The company does not have the necessary compute resources on premises for ML experiments and wants to use AWS.

The company needs to complete the data transfer to AWS within 3 weeks. The data transfer will be a one-time transfer. The data must be encrypted in transit. The measured upload speed of the company's internet connection is 100 Mbps. and multiple departments share the connection.

Which solution will meet these requirements MOST cost-effectively?

- A. Order several AWS Snowball Edge Storage Optimized devices by using the AWS Management Console. Configure the devices with a destination S3 bucket. Copy the data to the devices. Ship the devices back to AWS.
- B. Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.
- C. Create a VPN connection between the on-premises network attached storage and the nearest AWS Region. Transfer the data over the VPN connection.
- D. Deploy an AWS Storage Gateway file gateway on premises. Configure the file gateway with a destination S3 bucket. Copy the data to the file gateway.

Correct Answer: A

Community vote distribution

A (100%)

 **masetromain** Highly Voted 2 years, 5 months ago

Selected Answer: A

The correct answer is A. Order several AWS Snowball Edge Storage Optimized devices by using the AWS Management Console. Configure the devices with a destination S3 bucket. Copy the data to the devices. Ship the devices back to AWS.

This option will meet the requirements to complete the data transfer within 3 weeks, as the Snowball Edge devices can transfer large amounts of data quickly and securely. The data will be encrypted in transit and at rest. The company's internet connection speed is not a bottleneck as the data transfer will happen on the devices and not over the internet.

upvoted 11 times

 **masetromain** 2 years, 5 months ago

Option B is not a cost-effective solution, as setting up and maintaining a 10 Gbps Direct Connect connection can be quite expensive, especially if it's only needed for a one-time data transfer.

Option C is not a cost-effective solution, as creating a VPN connection between the on-premises storage and the nearest AWS region would require significant networking configuration and maintenance, and would likely be more expensive than using Snowball Edge devices.

Option D is not a cost-effective solution, as deploying an AWS Storage Gateway file gateway on premises would require additional hardware and ongoing maintenance costs, and may not be necessary for a one-time data transfer.

upvoted 3 times

 **princajen** Most Recent 5 months ago

Selected Answer: A

Why A is Best:

AWS Snowball Edge:

Designed for large-scale offline transfers (up to 80 TB usable per device)

Encryption in transit and at rest

No reliance on network bandwidth

Fits the one-time, time-sensitive transfer need

Cost-Effective:

Cheaper than setting up high-speed networking (e.g., Direct Connect)

No long-term infrastructure needed

Meets 3-week window:

Ordering, shipping, copying, and returning can all be completed within 2-3 weeks if planned properly
upvoted 1 times

 **ninomfr64** 1 year, 5 months ago

Selected Answer: A

A = correct
B = takes a month or more to setup DX
C = this would take more than 3 weeks for transferring data
D = this would take more than 3 weeks for transferring data
upvoted 2 times

 **career360guru** 1 year, 6 months ago

Selected Answer: A

Option A
upvoted 1 times

 **yorkicurke** 1 year, 8 months ago

Selected Answer: A

wish all the questions were like this. happy days :)
upvoted 1 times

 **xplusfb** 1 year, 10 months ago

Selected Answer: A

as we know snowball storage optimized NVMe up to 210 TB <3 A is the best and easy answer
upvoted 4 times

 **xplusfb** 1 year, 10 months ago

like several sorry for any confision :)
upvoted 1 times

 **chikorita** 1 year, 10 months ago

several thanks too :)
upvoted 1 times

 **NikkyDicky** 1 year, 12 months ago

Selected Answer: A

A - basic snowball use case
upvoted 1 times

 **Maria2023** 2 years ago

Selected Answer: A

Given the deadline (3 weeks) and the amount of data I would use Snowball Edge
upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: A

A obviously
upvoted 3 times

 **God_Is_Love** 2 years, 3 months 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** 2 years, 5 months ago

Selected Answer: A

3 weeks + cost effective ==> Snowball Edge Storage
upvoted 1 times

Question #94

Topic 1

A company has migrated its forms-processing application to AWS. When users interact with the application, they upload scanned forms as files through a web application. A database stores user metadata and references to files that are stored in Amazon S3. The web application runs on Amazon EC2 instances and an Amazon RDS for PostgreSQL database.

When forms are uploaded, the application sends notifications to a team through Amazon Simple Notification Service (Amazon SNS). A team member then logs in and processes each form. The team member performs data validation on the form and extracts relevant data before entering the information into another system that uses an API.

A solutions architect needs to automate the manual processing of the forms. The solution must provide accurate form extraction, minimize time to market, and minimize long-term operational overhead.

Which solution will meet these requirements?

- A. Develop custom libraries to perform optical character recognition (OCR) on the forms. Deploy the libraries to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster as an application tier. Use this tier to process the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data into an Amazon DynamoDB table. Submit the data to the target system's API. Host the new application tier on EC2 instances.
- B. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use artificial intelligence and machine learning (AI/ML) models that are trained and hosted on an EC2 instance to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.
- C. Host a new application tier on EC2 instances. Use this tier to call endpoints that host artificial intelligence and machine learning (AI/ML) models that are trained and hosted in Amazon SageMaker to perform optical character recognition (OCR) on the forms. Store the output in Amazon ElastiCache. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.
- D. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.

Correct Answer: D

Community vote distribution

D (100%)

 **masetromain**  2 years, 5 months ago

Selected Answer: D

The correct answer is D. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.

This solution meets the requirements of accurate form extraction, minimal time to market, and minimal long-term operational overhead. Amazon Textract and Amazon Comprehend are fully managed and serverless services that can perform OCR and extract relevant data from the forms, which eliminates the need to develop custom libraries or train and host models. Using AWS Step Functions and Lambda allows for easy automation of the process and the ability to scale as needed.

upvoted 16 times

 **masetromain** 2 years, 5 months ago

Option A:

This option would require significant development and maintenance effort and would not take advantage of fully managed services, resulting in increased operational overhead.

Option B:

This option is similar to option A in that it would require significant development and maintenance effort to train and host the models, and would not take advantage of fully managed services resulting in increased operational overhead.

Option C:

This option is similar to option B in that it would require significant development and maintenance effort to train and host the models, and would not take advantage of fully managed services resulting in increased operational overhead.

upvoted 3 times

 **princajen** Most Recent 5 months ago

Selected Answer: D

Amazon Textract:

Fully managed OCR service optimized for form data extraction

Handles structured and unstructured documents accurately

No need to train ML models

Amazon Comprehend:

Extracts entities, key phrases, and insights from text

Enhances accuracy when interpreting extracted form content

AWS Step Functions + Lambda:

Serverless and scalable

Low operational overhead — no EC2 to manage

Easily orchestrates Textract → Comprehend → API steps

Time to market:

All services are fully managed, no custom training or model hosting

Easy to plug into an existing architecture

upvoted 1 times

 **gofavad926** 1 year, 3 months ago

Selected Answer: D

D. This solution meets the requirements of accurate form extraction, minimal time to market, and minimal long-term operational overhead

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: D

Option D

upvoted 1 times

 **NikkyDicky** 1 year, 12 months ago

Selected Answer: D

D - basic use case for Textract

upvoted 1 times

 **Maria2023** 2 years ago

Selected Answer: D

An easy one - if AWS has a service for something - do not reinvent the wheel - use Textract and Comprehend

upvoted 2 times

 **SkyZeroZx** 2 years ago

Selected Answer: D

D : Managed AWS Services

upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: D

Amazon Textract..

upvoted 1 times

 **God_Is_Love** 2 years, 3 months 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** 2 years, 3 months ago

Selected Answer: D

D : Managed AWS Services

upvoted 2 times

Question #95

A company is refactoring its on-premises order-processing platform in the AWS Cloud. The platform includes a web front end that is hosted on a fleet of VMs, RabbitMQ to connect the front end to the backend, and a Kubernetes cluster to run a containerized backend system to process the orders. The company does not want to make any major changes to the application.

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

- A. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up Amazon MQ to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.
- B. Create a custom AWS Lambda runtime to mimic the web server environment. Create an Amazon API Gateway API to replace the front-end web servers. Set up Amazon MQ to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.
- C. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up Amazon MQ to replace the on-premises messaging queue. Install Kubernetes on a fleet of different EC2 instances to host the order-processing backend.
- D. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up an Amazon Simple Queue Service (Amazon SQS) queue to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.

Correct Answer: A*Community vote distribution*

A (94%)	6%
---------	----

masetromain Highly Voted 2 years, 11 months ago

Selected Answer: A

Option A is the correct answer. In this solution, the company creates an Amazon Machine Image (AMI) of the web server VM, which can be used to launch EC2 instances that are identical to the on-premises web servers. The company then creates an EC2 Auto Scaling group that uses the AMI and an Application Load Balancer (ALB) to provide automatic scaling and high availability for the web front end. The company also replaces the on-premises messaging queue (RabbitMQ) with Amazon MQ, which is a managed message broker service that is fully compatible with RabbitMQ. Finally, the company uses Amazon Elastic Kubernetes Service (EKS) to host the order-processing backend, which allows them to run their existing Kubernetes cluster in the AWS cloud without making any major changes to the application. This approach allows the company to lift and shift their existing platform with minimal operational overhead.

upvoted 21 times

pk0619 1 year ago

AMI is an AWS EC2 specific, I am confused on how to create an AMI of an on-premise VM and launch instance from it ?

upvoted 1 times

pk0619 1 year ago

Looking back, it seems the intent might have been to use VM Import/Export or the AWS Application Migration Service (MGN) to create an AMI. However, it is a significant oversimplification to skip those critical steps and simply state "create an AMI," as this assumes the process is straightforward without addressing the necessary prerequisites and tools.

upvoted 1 times

masetromain 2 years, 11 months ago

Option B, using a custom AWS Lambda runtime and Amazon API Gateway, would require significant changes to the application and may not be compatible with the current codebase.

Option C, installing Kubernetes on a fleet of different EC2 instances, would also require significant changes to the application and may not be compatible with the current codebase.

Option D, using Amazon Simple Queue Service (Amazon SQS) instead of Amazon MQ, would not provide the same level of messaging capabilities as Amazon MQ and may not be sufficient for the needs of the order-processing platform.

upvoted 4 times

sambb 2 years, 9 months 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 10 times

AimarLeo Highly Voted 1 year, 11 months ago

AWS exams got more 'sarcastic' with the ways of formulating questions.. E.g here: 'A company is refactoring its on-premises order-processing platform in the AWS Cloud'

BUT '

The company does not want to make any major changes to the application.

Replatforming and Rehosting is not real refactoring.. but the closest answer as an architect with least operational overhead is A obvisouly.. aws questions sometimes can be ultra vague

upvoted 6 times

 **princajen** Most Recent 5 months ago

Selected Answer: A

Why A is the Best Option:

"No major changes": Re-using existing components and patterns is crucial here.

AMI of VM + EC2 Auto Scaling + ALB:

Keeps the web frontend architecture nearly unchanged

Easy to lift-and-shift with minimal rework

Amazon MQ:

Fully managed message broker service compatible with RabbitMQ

Allows reusing RabbitMQ-based code without modifications

Amazon EKS:

Fully managed Kubernetes service

Minimizes operational burden (no need to manage K8s control plane)

Supports containerized backend as-is

This solution replicates the existing architecture with minimal refactoring while reducing ops overhead through managed services.

upvoted 1 times

 **madeesha** 1 year, 6 months ago

Selected Answer: A

answer is A

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A, is the only option to don't involve a rearchitected solution

upvoted 1 times

 **jpa8300** 1 year, 11 months ago

Selected Answer: A

A better explanation to choose between option A and D is that Amazon MQ responds to the requirement of not changing the app, because it accepts the same protocol as RabbitMQ (Supports AMQP, MQTT, STOMP, OpenWire, and JMS) while SQS has its own API, so it would need more changes to the app.

upvoted 3 times

 **career360guru** 2 years ago

Selected Answer: A

Option A

upvoted 1 times

 **Mikado211** 2 years, 1 month ago

Selected Answer: A

a bunch of keywords for this migration here :

Kubernetes == EKS

RabbitMQ == Amazon MQ

A fleet of VM == AMI + ec2 instances

The answer A proposes all thoses points, so it's perfect here.

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

A no doubt

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: A

A is the best choice.

upvoted 1 times

 Musk 2 years, 10 months 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 2 years, 10 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 6 times

Question #96

A solutions architect needs to implement a client-side encryption mechanism for objects that will be stored in a new Amazon S3 bucket. The solutions architect created a CMK that is stored in AWS Key Management Service (AWS KMS) for this purpose.

The solutions architect created the following IAM policy and attached it to an IAM role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DownloadUpload",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::BucketName/*"
    },
    {
      "Sid": "KMSAccess",
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:kms:Region:Account:key/Key ID"
    }
  ]
}
```

During tests, the solutions architect was able to successfully get existing test objects in the S3 bucket. However, attempts to upload a new object resulted in an error message. The error message stated that the action was forbidden.

Which action must the solutions architect add to the IAM policy to meet all the requirements?

- A. kms:GenerateDataKey
- B. kms:GetKeyPolicy
- C. kms:GetPublicKey
- D. kms:Sign

Correct Answer: A

Community vote distribution

A (100%)

 **masetromain** Highly Voted 2 years, 5 months ago

Selected Answer: A

A. kms:GenerateDataKey

The solutions architect needs to add the "kms:GenerateDataKey" action to the IAM policy in order to generate a data key for client-side encryption. Without this action, the IAM role does not have the necessary permissions to generate a data key, which causes the error message when attempting to upload a new object.

upvoted 16 times

 **masetromain** 2 years, 5 months ago

The other options are not correct because they are not required for this use case. kms:GetKeyPolicy allows for the retrieval of the key policy for a CMK but it does not have any relation to client-side encryption of S3 objects, kms:GetPublicKey allows for the retrieval of the public key of a CMK, but it does not have any relation to client-side encryption of S3 objects and kms:Sign allows for signing a message using a CMK but it does not have any relation to client-side encryption of S3 objects.

upvoted 2 times

 **princajen** Most Recent 5 months ago

Selected Answer: A

For client-side encryption, especially when using the AWS SDK with KMS, the client performs the following steps:

Requests a data key from KMS via kms:GenerateDataKey

Uses the plaintext key to encrypt the object

Stores the encrypted key and the encrypted object in S3

Thus, kms:GenerateDataKey is essential for enabling the client to encrypt before uploading.

upvoted 1 times

altonh 11 months, 2 weeks ago

Selected Answer: A

The answers don't make sense. The requirement is that it will be client-side encryption, which means the object is already encrypted when sent to S3. S3 will not do any encryption, so S3 does not need to access the KMS key,

upvoted 1 times

ninomfr64 1 year, 5 months ago

Selected Answer: A

A = correct (you encrypt data with KMS Data Key and not KMS Key directly, unless data is < 4K)

B = getting the policy would allow to get the data key needed for encryption

C = client side encryption uses symmetric key not asymmetric keys

D = sign allows for signing messages, API calls, etc.

upvoted 3 times

career360guru 1 year, 6 months ago

Selected Answer: A

Option A

upvoted 1 times

NikkyDicky 1 year, 12 months ago

Selected Answer: A

A - need data key for client-side encr

upvoted 1 times

Jesuisleon 2 years, 1 month ago

I don't understand since it's client side encryption, it means both encryption and key and tools are maintained in client side before submitting to aws s3, why we need add kms:GenerateDatakey? We don't need kms to do anything since it's client-side encryption all is done outside of aws.

upvoted 4 times

venvig 1 year, 10 months 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 11 times

venvig 1 year, 10 months ago

Of course the answer is A

upvoted 1 times

btx 2 years ago

Indeed, the question says client side encryption but the answer is all about S3-KMS.

upvoted 2 times

mfsec 2 years, 3 months ago

Selected Answer: A

A for sure

upvoted 1 times

Untamables 2 years, 5 months ago

Selected Answer: A

<https://docs.aws.amazon.com/kms/latest/cryptographic-details/client-side-encryption.html>

upvoted 3 times

masssa 2 years, 5 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

A company has developed a web application. The company is hosting the application on a group of Amazon EC2 instances behind an Application Load Balancer. The company wants to improve the security posture of the application and plans to use AWS WAF web ACLs. The solution must not adversely affect legitimate traffic to the application.

How should a solutions architect configure the web ACLs to meet these requirements?

- A. Set the action of the web ACL rules to Count. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Count to Block.
- B. Use only rate-based rules in the web ACLs, and set the throttle limit as high as possible. Temporarily block all requests that exceed the limit. Define nested rules to narrow the scope of the rate tracking.
- C. Set the action of the web ACL rules to Block. Use only AWS managed rule groups in the web ACLs. Evaluate the rule groups by using Amazon CloudWatch metrics with AWS WAF sampled requests or AWS WAF logs.
- D. Use only custom rule groups in the web ACLs, and set the action to Allow. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Allow to Block.

Correct Answer: A

Community vote distribution

A (100%)

 **God_Is_Love** Highly Voted 2 years, 3 months 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 23 times

 **masetromain** Highly Voted 2 years, 5 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/74273-exam-aws-certified-solutions-architect-professional-topic-1/>

The correct answer is A. Set the action of the web ACL rules to Count. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Count to Block.

This approach allows for monitoring of the incoming traffic and its behavior before taking any action that can affect the legitimate traffic. By setting the action to count, the web ACL will only log the requests that match the conditions of the rules, but it will not block them. This way, the company can analyze the requests and check for any false positives. Once they identify and correct any false positives, they can gradually change the action of the web ACL rules from count to block, thus improving the security posture of the application without adversely affecting legitimate traffic.

upvoted 6 times

 **masetromain** 2 years, 5 months ago

Option B is not correct because using only rate-based rules can lead to false positives and blocking of legitimate traffic. Option C is not correct because using only AWS managed rule groups can limit the flexibility and specificity of the web ACLs. Option D is not correct because using only custom rule groups with action set to allow can lead to security vulnerabilities.

upvoted 1 times

 **princajen** Most Recent 5 months ago

Selected Answer: A

Why A is the Best:
Start with "Count" mode:

Allows you to monitor and evaluate rule behavior without blocking traffic

Helps identify false positives before enforcement

Enable WAF logging:

Lets you analyze traffic patterns and validate that rules behave as expected

Gradual transition to "Block":

Once confident, change individual rules from Count → Block

Minimizes risk of blocking legitimate users

This approach is the safest and most controlled way to deploy WAF protections.

upvoted 1 times

 **gofavad926** 1 year, 3 months ago

Selected Answer: A

A, configure the rules on COUNT

upvoted 1 times

 **Explorer_30** 1 year, 10 months ago

vote A

upvoted 1 times

 **NikkyDicky** 1 year, 12 months ago

Selected Answer: A

Its an A

upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: A

A. Set the action of the web ACL rules to Count. Enable AWS WAF logging.

upvoted 1 times

 **Untamables** 2 years, 5 months ago

Selected Answer: A

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing.html>

upvoted 1 times

Question #98

A company has an organization that has many AWS accounts in AWS Organizations. A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization.

The company has a common set of IP CIDR ranges in an allow list in each AWS account to allow access to and from the company's on-premises network. Developers within each account are responsible for adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list.

The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Set up an Amazon Simple Notification Service (Amazon SNS) topic in the security team's AWS account. Deploy an AWS Lambda function in each AWS account. Configure the Lambda function to run every time an SNS topic receives a message. Configure the Lambda function to take an IP address as input and add it to a list of security groups in the account. Instruct the security team to distribute changes by publishing messages to its SNS topic.
- B. Create new customer-managed prefix lists in each AWS account within the organization. Populate the prefix lists in each account with all internal CIDR ranges. Notify the owner of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups. Instruct the security team to share updates with each AWS account owner.
- C. Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.
- D. Create an IAM role in each account in the organization. Grant permissions to update security groups. Deploy an AWS Lambda function in the security team's AWS account. Configure the Lambda function to take a list of internal IP addresses as input, assume a role in each organization account, and add the list of IP addresses to the security groups in each account.

Correct Answer: C

Community vote distribution

C (89%)	11%
---------	-----

 **masetromain** Highly Voted 2 years, 5 months ago

Selected Answer: C

C. Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.

This solution meets the requirements with the least amount of operational overhead as it requires the security team to create and maintain a single customer-managed prefix list, and share it with the organization using AWS Resource Access Manager. The owners of each AWS account are then responsible for allowing the prefix list in their security groups, which eliminates the need for the security team to manually notify each account owner when changes are made. This solution also eliminates the need for a separate AWS Lambda function in each account, reducing the overall complexity of the solution.

upvoted 11 times

 **masetromain** 2 years, 5 months ago

Option A is not correct because it requires setting up an SNS topic in the security team's AWS account, and deploying an AWS Lambda function in each AWS account. This increases the operational overhead as it requires setting up and maintaining the SNS topic, and deploying and configuring the Lambda function in each account.

Option B is not correct because it requires creating new customer-managed prefix lists in each AWS account within the organization, which increases the operational overhead as it requires the security team to create and maintain multiple prefix lists.

Option D is not correct because it requires creating an IAM role in each account in the organization, which increases the operational overhead as it requires the security team to set up and maintain multiple roles. Additionally, it also deploys an AWS Lambda function in the security team's AWS account, which increases complexity and operational overhead.

upvoted 2 times

 **bur4an** Highly Voted 1 year, 9 months ago

masetromain is ChatGPT and might have outdated answers since it doesn't know AWS latest update to services

upvoted 8 times

 **princajen** Most Recent 5 months ago

Selected Answer: C

Why C is Best:

Prefix lists allow you to define a group of CIDRs once and reference them in security group rules

By using AWS Resource Access Manager (RAM), the central security team can share a single prefix list with the whole organization

Developers in other accounts just reference the shared prefix list ID — no need to hardcode IPs

When the security team updates the prefix list, all security groups using it are updated automatically

Minimal ongoing ops: one central place to manage, no cross-account Lambda or custom logic needed

upvoted 1 times

 **AlbertC** 1 year, 3 months ago

Human cost is major overhead. I will go A. This is one time setup.

upvoted 1 times

 **StevePace** 1 year, 3 months ago

Selected Answer: C

Centralised management and standard use case for prefix lists and RAM

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: C

Option C

upvoted 1 times

 **NikkyDicky** 1 year, 12 months ago

Selected Answer: C

C - basic RAM use case

upvoted 1 times

 **bcx** 2 years 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** 2 years ago

Selected Answer: C

KEYWORD = AWS Resource Access Manager

Then C

upvoted 1 times

 **johnballs221** 2 years ago

Selected Answer: D

operational overhead

upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: C

Prefix lists + RAM

upvoted 2 times

 **God_Is_Love** 2 years, 3 months ago

Prefix lists + Resource Access Manager RAM is the solution.

upvoted 5 times

 **Musk** 2 years, 4 months ago

Selected Answer: C

Clearly

upvoted 1 times

 **zozza2023** 2 years, 5 months ago

Selected Answer: C

Create a new customer-managed prefix list in the security team's AWS account

upvoted 1 times

 **Untamables** 2 years, 5 months ago

Selected Answer: C

<https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html>

upvoted 3 times

 **zhangyu20000** 2 years, 5 months ago

C is correct. The prefix list is managed by security team and shared with other accounts. Other accounts can directly use it.
upvoted 1 times

 **masetromain** 2 years, 5 months ago

Selected Answer: D

The correct answer is D.

Option D creates an IAM role in each account in the organization which grants permissions to update security groups. Then, it deploys an AWS Lambda function in the security team's AWS account, this lambda function is able to assume the IAM roles in each account and update the security groups with the new IP CIDR ranges. This solution allows the security team to easily distribute and update the common set of IP CIDR ranges across all accounts with minimal operational overhead.

Option A, uses an SNS topic, where the security team would need to notify all account owners every time an update is made to the allow list and would require the developers in each account to run a Lambda function which updates the security group. This solution would require a lot of manual work, and is not automated.

upvoted 2 times

 **masetromain** 2 years, 5 months ago

Option B, requires the security team to notify the owners of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups, this solution would not provide a centralized control of the IP CIDR ranges and would require a lot of manual work.

Option C, uses a customer-managed prefix list in the security team's AWS account. But, it still requires the owners of each account to allow the new customer-managed prefix list ID in their security groups, this solution would not provide a centralized control of the IP CIDR ranges and would require a lot of manual work.

upvoted 1 times

 **God_Is_Love** 2 years, 3 months ago

Create an IAM role in each account in the organization. this does not add up to operational overhead right.

upvoted 1 times

 **BabaP** 2 years ago

It's ChatGPT talking

upvoted 1 times

Question #99

A company has introduced a new policy that allows employees to work remotely from their homes if they connect by using a VPN. The company is hosting internal applications with VPCs in multiple AWS accounts. Currently, the applications are accessible from the company's on-premises office network through an AWS Site-to-Site VPN connection. The VPC in the company's main AWS account has peering connections established with VPCs in other AWS accounts.

A solutions architect must design a scalable AWS Client VPN solution for employees to use while they work from home.

What is the MOST cost-effective solution that meets these requirements?

- A. Create a Client VPN endpoint in each AWS account. Configure required routing that allows access to internal applications.
- B. Create a Client VPN endpoint in the main AWS account. Configure required routing that allows access to internal applications.
- C. Create a Client VPN endpoint in the main AWS account. Provision a transit gateway that is connected to each AWS account. Configure required routing that allows access to internal applications.
- D. Create a Client VPN endpoint in the main AWS account. Establish connectivity between the Client VPN endpoint and the AWS Site-to-Site VPN.

Correct Answer: B*Community vote distribution*

B (54%)

C (46%)

 **hexie** Highly Voted 2 years, 5 months 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 38 times

 **aka1177** 1 month, 1 week ago

100% Agree! We already have such architecture with TGW and this is best practice in AWS when you need scalable approach.

upvoted 1 times

 **artazar** 9 months, 3 weeks ago

Direct link from the docs for the scenario:

<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/how-it-works.html#scenario-peered>

Transitive peering is VPC A <-peer-> VPC B <-peer-> VPC C ---> here VPC A cannot communicate to VPC C. But Client VPN is not a peering connection.

upvoted 1 times

 **vn_thanh tung** 2 years, 3 months 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 13 times

 **Impromptu** 2 years ago

The question asks a scalable Client VPN solution (i.e. no openvpn on an EC2 instance or something like that), and asks for the most cost-effective. So AWS Client VPN is the scalable option. Reusing the current VPC peering is the most cost-effective compared to the far more expensive transit gateway solution.

I do agree that the peering does not support transitive peering. But for AWS Client VPN you get an ENI in the main account VPC and using the ENI you can access the VPCs over the VPC peering. So that does really work (in contrast to the Site-To-Site VPN): <https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html>

upvoted 13 times

 **_Jassybang_** 1 year, 4 months ago

Most cost effective - Transit gateway option is more costlier then B

upvoted 3 times

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/80782-exam-aws-certified-solutions-architect-professional-topic-1/>

B. Create a Client VPN endpoint in the main AWS account. Configure required routing that allows access to internal applications is the MOST cost-effective solution that meets these requirements. This solution allows employees to connect to the main AWS account using a Client VPN endpoint, and then use peering connections established with other AWS accounts to access the internal applications. This eliminates the need for additional Client VPN endpoints in each AWS account, reducing costs.

Option A, creating a Client VPN endpoint in each AWS account, would be more expensive as it would require multiple endpoints.

Option C, creating a transit gateway, would also add unnecessary costs.

Option D, connecting the Client VPN endpoint to the Site-to-Site VPN, may not provide a scalable solution for remote employees.
upvoted 25 times

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

Selected Answer: B

it should be COST EFFECTIVE then cannot be C

Option C: Client VPN + Transit Gateway

Higher cost: Adds Transit Gateway fees (\$36/month + \$0.02 per GB processed)

Unnecessary complexity: VPC peering already provides connectivity

Overkill: Transit Gateway benefits not needed for this scenario

upvoted 1 times

 **3967974** 4 months, 3 weeks ago

Selected Answer: C

Got to be C.

upvoted 1 times

 **princajen** 5 months ago

Selected Answer: B

Why B is the Best:

Single Client VPN endpoint = low operational and cost overhead

Main account already has VPC peering with other VPCs → traffic can be routed

Use route tables and security groups to allow traffic from VPN clients to flow to other VPCs

No need for Transit Gateway, which adds cost unless scalability or future expansion is needed

Easy to scale VPN access centrally and enforce policy from a single location

upvoted 3 times

 **antoniohdez** 5 months, 1 week ago

Selected Answer: B

Not necessary to provision a Transit Gateway since main VPC already has connectivity with the other VPCs

upvoted 2 times

 **Kaps443** 6 months, 3 weeks ago

Selected Answer: C

Option C is the BEST solution: it provides a centralized, scalable, and cost-effective VPN access architecture using AWS Client VPN + Transit Gateway to allow secure access across multiple AWS accounts and VPCs.

upvoted 1 times

 **jimee11** 7 months ago

Selected Answer: C

Transitive will cause issues trying to connect to her VPCs.

upvoted 1 times

 **eesa** 7 months, 2 weeks ago

Selected Answer: B

B. Crear un Client VPN endpoint en la cuenta principal y configurar enrutamiento

Muy buena opción:

Un solo Client VPN compartido para todos los usuarios.

Como la cuenta principal ya tiene peering con otras cuentas/VPCs, puedes simplemente rutar el tráfico hacia ellas desde el Client VPN.

Esto es sencillo, escalable y muy rentable.

upvoted 2 times

 **BennyMao** 9 months, 3 weeks ago

Selected Answer: C

This provides a scalable and centralized routing solution to connect VPCs across multiple AWS accounts.

upvoted 1 times

✉  **Liliwood** 11 months, 2 weeks ago

Selected Answer: B

Option B is the most cost-effective solution as it only requires creating a single Client VPN endpoint in the main AWS account and configuring the required routing to access the internal applications across the VPC peering connections.

Option C would involve additional costs for provisioning a transit gateway and connecting it to each AWS account, which is not necessary in this scenario since the VPCs are already peered.

upvoted 2 times

✉  **henrikhmkhitaryan59** 1 year, 1 month ago

Selected Answer: B

Option B is the MOST cost-effective solution that meets the requirements.

upvoted 3 times

✉  **Hibiki761** 1 year, 1 month ago

Selected Answer: B

VPC peering is enough

upvoted 2 times

✉  **0b43291** 1 year, 1 month ago

Selected Answer: B

By choosing option B, you can provide a scalable and cost-effective solution for remote employees to access internal applications hosted in multiple AWS accounts, while leveraging the existing VPC peering connections and minimizing the number of AWS resources required.

The other options are either more complex, less cost-effective, or introduce unnecessary components:

- A. Creating a Client VPN endpoint in each AWS account would be more expensive and harder to manage, as you would need to configure and maintain multiple endpoints.
- C. Provisioning a Transit Gateway in addition to the Client VPN endpoint would introduce an additional service and associated costs, which may not be necessary if the existing VPC peering connections are sufficient.
- D. Establishing connectivity between the Client VPN endpoint and the AWS Site-to-Site VPN would introduce unnecessary complexity, as the Site-to-Site VPN is intended for connecting the on-premises office network, not individual remote employees.

upvoted 2 times

✉  **youonebe** 1 year, 1 month ago

answer is B, should take advantage of existing VPC peering connections which works with current network topology

upvoted 1 times

✉  **Halliphax** 1 year, 1 month ago

Selected Answer: B

B.

It asks for a scalable solution and it has to be cost effective. Adding Transit Gateway is not cost effective and also not required as the main AWS account has peering connections to VPCs in other accounts already.

upvoted 2 times

✉  **sammyhaj** 1 year, 1 month ago

Selected Answer: B

No tgw needed

upvoted 3 times

Question #100

Topic 1

A company is running an application in the AWS Cloud. Recent application metrics show inconsistent response times and a significant increase in error rates. Calls to third-party services are causing the delays. Currently, the application calls third-party services synchronously by directly invoking an AWS Lambda function.

A solutions architect needs to decouple the third-party service calls and ensure that all the calls are eventually completed.

Which solution will meet these requirements?

- A. Use an Amazon Simple Queue Service (Amazon SQS) queue to store events and invoke the Lambda function.
- B. Use an AWS Step Functions state machine to pass events to the Lambda function.
- C. Use an Amazon EventBridge rule to pass events to the Lambda function.
- D. Use an Amazon Simple Notification Service (Amazon SNS) topic to store events and Invoke the Lambda function.

Correct Answer: A*Community vote distribution*

A (100%)

 **masetromain** Highly Voted  2 years, 11 months ago

Selected Answer: A

The correct answer is A. Using an Amazon Simple Queue Service (SQS) queue to store events and invoke the Lambda function is a good solution to decouple the third-party service calls and ensure that all the calls are eventually completed. SQS is a fully managed, reliable, and highly scalable message queuing service that allows applications to send, store, and receive messages between distributed components. By sending the third-party service calls to an SQS queue, it allows the application to continue processing without waiting for the third-party services to respond, which can result in faster response times and lower error rates.

upvoted 5 times

 **masetromain** 2 years, 11 months ago

Other options like AWS Step Functions state machine, Amazon EventBridge, and Amazon Simple Notification Service (SNS) topic are not appropriate for this use case. AWS Step Functions is a service that makes it easy to coordinate the components of distributed applications and microservices using visual workflows. Amazon EventBridge is a serverless event bus that makes it easy to connect applications together using data from your own applications, integrated SaaS applications, and AWS services. Amazon SNS is a fully managed messaging service for both application-to-application and application-to-person (A2P) communication. These services are not focused on providing message queues and would not be the best fit for this use case.

upvoted 1 times

 **princajen** Most Recent  5 months ago

Selected Answer: A

Why A is the Best Solution:

Amazon SQS:

Provides a fully managed message queue

Enables asynchronous decoupling between the app and third-party service

Guarantees durable message storage and eventual processing

Lambda can poll the queue and retry failed calls automatically

Helps smooth out traffic spikes and manage backpressure

This solution is ideal for handling intermittent third-party service slowness and ensures no data loss, satisfying the requirement that all calls are eventually completed.

upvoted 1 times

 **GabrielShiao** 11 months, 2 weeks ago

Selected Answer: A

while polling a, c is another solution accomodating the requirement. In the real case, i would pick c for a large scale eda app scenario

upvoted 1 times

 **AWSum1** 1 year, 2 months ago

Selected Answer: A

Decoupling = SQS

upvoted 1 times

 **nimbus_00** 1 year, 2 months ago

Selected Answer: A

SQS Queue = Decoupling the service calls + Eventual completion + Error handling and retries (DLQ)

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. Use an Amazon Simple Queue Service (Amazon SQS) queue to store events and invoke the Lambda function.

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: A

Option A

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: A

Option A

upvoted 2 times

 **HC888** 2 years, 1 month ago

Selected Answer: A

SQS support dead letter queue and retry if the event processed fails

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

A no brainer

upvoted 1 times

 **rbm2023** 2 years, 7 months ago

Selected Answer: A

Step functions would not help on the decoupling if you are not using an asynchronous element in this architecture which is SQS. The application need to have the ability to move out from synchronous calls to the third party services. correct answer is A.

upvoted 2 times

 **hpirit** 2 years, 9 months ago

Selected Answer: A

A : SQS QUEUE

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: A

SQS for decoupling

upvoted 2 times

 **c73bf38** 2 years, 10 months ago

Selected Answer: A

SQS ---> Lambda is the correct option

upvoted 2 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: A

decouple ==> SQS

upvoted 1 times

 **Untamables** 2 years, 11 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** 2 years, 11 months ago

I vote for C - use Step Functions with its callback feature to throttle the third party api call.

upvoted 1 times

Question #101

A company is running applications on AWS in a multi-account environment. The company's sales team and marketing team use separate AWS accounts in AWS Organizations.

The sales team stores petabytes of data in an Amazon S3 bucket. The marketing team uses Amazon QuickSight for data visualizations. The marketing team needs access to data that the sales team stores in the S3 bucket. The company has encrypted the S3 bucket with an AWS Key Management Service (AWS KMS) key. The marketing team has already created the IAM service role for QuickSight to provide QuickSight access in the marketing AWS account. The company needs a solution that will provide secure access to the data in the S3 bucket across AWS accounts.

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

- A. Create a new S3 bucket in the marketing account. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing account. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket.
- B. Create an SCP to grant access to the S3 bucket to the marketing account. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sales account with the marketing account. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- C. Update the S3 bucket policy in the marketing account to grant access to the QuickSight role. Create a KMS grant for the encryption key that is used in the S3 bucket. Grant decrypt access to the QuickSight role. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- D. Create an IAM role in the sales account and grant access to the S3 bucket. From the marketing account, assume the IAM role in the sales account to access the S3 bucket. Update the QuickSight role, to create a trust relationship with the new IAM role in the sales account.

Correct Answer: D*Community vote distribution*

D (63%)	C (28%)	8%
---------	---------	----

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: D

The correct answer is D. Create an IAM role in the sales account and grant access to the S3 bucket. From the marketing account, assume the IAM role in the sales account to access the S3 bucket. Update the QuickSight role to create a trust relationship with the new IAM role in the sales account.

This solution meets the requirements by allowing the marketing team to access the data in the S3 bucket in the sales account through assuming an IAM role, which eliminates the need to copy the data or share the KMS key, and also eliminates the need to modify the S3 bucket policy or create a KMS grant. This solution allows to use the same access to the bucket without duplicating data and re-encrypting it.

upvoted 27 times

 **masetromain** 2 years, 11 months ago

A. Create a new S3 bucket in the marketing account. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing account. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket is not correct because it would create unnecessary data duplication and increased storage costs.

B. Create an SCP to grant access to the S3 bucket to the marketing account. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sales account with the marketing account. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket is not correct because it does not provide a secure way to share the KMS key between accounts and also it would create unnecessary data duplication and increased storage costs.

upvoted 4 times

 **masetromain** 2 years, 11 months ago

C. Update the S3 bucket policy in the marketing account to grant access to the QuickSight role. Create a KMS grant for the encryption key that is used in the S3 bucket. Grant decrypt access to the QuickSight role. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket is not correct because the Sales team's S3 bucket is in a different account, so the Marketing team cannot update the policy on the Sales team's S3 bucket.

upvoted 2 times

 **Maria2023** Highly Voted 2 years, 6 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 11 times

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

Selected Answer: D

Cross-account IAM role in Sales Account
Create a role in the Sales account that allows access to the S3 bucket.

Add trust relationship to allow QuickSight service role in the Marketing account to assume it.

Grant the required S3 and KMS permissions via the assumed role.

QuickSight can assume the cross-account role to access encrypted data.

AWS-recommended pattern for cross-account access, minimal replication, no duplicated storage, and no need for S3 replication.
upvoted 1 times

 **kylix75** 11 months ago

Selected Answer: D

The correct answer is D.

Rationale:

- Lowest operational overhead using native IAM mechanisms
- Enables secure cross-account access through role assumption
- Maintains centralized access control
- No data duplication or additional storage costs
- Works seamlessly with existing KMS encryption

Other options' drawbacks:

- A: Duplicates data and costs
 - B: SCPs aren't for granular access control
 - C: Incorrect bucket policy location (bucket is in sales account, not marketing)
- upvoted 1 times

 **bhanus** 1 year ago

Selected Answer: C

Option C provides the most straightforward and efficient solution with the least operational overhead. It directly addresses the cross-account access need while maintaining security through appropriate S3 bucket and KMS key policies.

upvoted 3 times

 **nimbus_00** 1 year, 2 months ago

Selected Answer: C

Creating an IAM role in the sales account that grants access to the S3 bucket and allowing the marketing account (QuickSight) to assume that role.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

C. Update the S3 bucket policy in the marketing account to grant access to the QuickSight role. Create a KMS grant for the encryption key that is used in the S3 bucket. Grant decrypt access to the QuickSight role. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.

upvoted 1 times

 **Jason666888** 1 year, 4 months ago

Selected Answer: C

There must be a typo in C.

In the context of option D, if Amazon QuickSight needs to access data in an S3 bucket in a different AWS account, and the setup involves assuming multiple roles, this approach could be problematic. QuickSight would not be able to assume the role in the sales account while simultaneously using its own role in the marketing account.

upvoted 4 times

 **Jason666888** 1 year, 4 months ago

In C, "Update the S3 bucket policy in the marketing account" should be changed to "Update the S3 bucket policy in the sales account"
upvoted 3 times

 **helloworldabc** 1 year, 4 months ago

just D

upvoted 1 times

 **8693a49** 1 year, 4 months ago

Selected Answer: A

What is QuickSight role? It can't be D. I'm assuming there is no typo, so C is wrong too. B is wrong because you can't grant that permission with SCPs.

A would work provided that the replication permissions are set up correctly. It's not great because I don't think it's necessary to duplicate the data, but it's the only viable option we are given.

upvoted 1 times

 **Jason666888** 1 year, 4 months ago

Dude, do you have any idea of what Petabytes amount of data mean? No one would do that in real life if there's other options

upvoted 1 times

 **vip2** 1 year, 6 months ago

Selected Answer: C

C should be correct if change typo from market account to sales account for S3 bucket policy statement.

upvoted 3 times

 **quizzical_kiwi** 1 year, 6 months ago

Selected Answer: C

Agree with other answers on C. This question is clearly a typo, and "marketing" should be changed to "sales" in C. The resolution for this scenario is even stated in the AWS Knowledge base, and the solution is identical when replacing "marketing" with "sales":

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

upvoted 3 times

 **teo2157** 1 year, 8 months ago

Selected Answer: C

It should be C and there should be a misspelling in "Update the S3 bucket policy in the marketing account" when it's referring to sales account

upvoted 2 times

 **djeong95** 1 year, 9 months ago

I think this is a great question with poorly phrased answers. If I have to choose between C and D, it would be neither since they both do not provide complete answers. Let me explain:

For C, you are updating the S3 bucket policy for the marketing account, when you should be doing that for the sales account. So, C is wrong. However, if that were fixed to the sales account, everything would make sense, since the sales account would be providing the right policy, granting the correct KMS key permission, and the marketing account would be tweaking its permission in QuickSight.

For D, it is wrong simply because it says nothing about providing KMS key grant. Not only do you have to establish trust policy in the QuickSight role to access S3 bucket, you have to allow Decrypt to happen. You have to explicitly spell this out (read the permission part in the link below).

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

upvoted 3 times

 **djeong95** 1 year, 9 months ago

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

upvoted 1 times

 **VerRi** 1 year, 10 months ago

Selected Answer: D

Option C: Update the S3 bucket policy in the "marketing account"lol

upvoted 2 times

 **8608f25** 1 year, 10 months ago

Selected Answer: C

The answer is C. Update the S3 bucket policy in the sales account to grant access to the QuickSight role in the marketing account. Create a KMS grant for the encryption key that is used in the S3 bucket. Grant decrypt access to the QuickSight role. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.

Option C correctly identifies the need to update the S3 bucket policy to grant access specifically to the QuickSight IAM role in the marketing account, which directly addresses the requirement for cross-account access to S3 data. Additionally, creating a KMS grant for the encryption key to allow decrypt access by the QuickSight role aligns with best practices for secure, cross-account access to encrypted S3 data. This approach minimizes operational overhead by using existing roles and permissions without the need for replication or additional resource sharing mechanisms.

upvoted 2 times

 **AimarLeo** 1 year, 10 months ago

the question is badly formulated.. with all given options missing each a spec .. none of the answers are fully convincing

upvoted 2 times

 **tmlong18** 1 year, 11 months ago

Selected Answer: C

All answers are wrong:

- A. No KMS, not necessary replication
- B. No IAM
- C. No KMS

But the most likely answer is C.

"Update the S3 bucket policy in the marketing account"

The question was never asked marketing s3 team bucket and all the data store in sales team S3 bucket.

I think it's a typing error (marketing-> sales).

upvoted 4 times

Question #102

A company is planning to migrate its business-critical applications from an on-premises data center to AWS. The company has an on-premises installation of a Microsoft SQL Server Always On cluster. The company wants to migrate to an AWS managed database service. A solutions architect must design a heterogeneous database migration on AWS.

Which solution will meet these requirements?

- A. Migrate the SQL Server databases to Amazon RDS for MySQL by using backup and restore utilities.
- B. Use an AWS Snowball Edge Storage Optimized device to transfer data to Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.
- C. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MySQL. Then use AWS Database Migration Service (AWS DMS) to migrate the data from on-premises databases to Amazon RDS.
- D. Use AWS DataSync to migrate data over the network between on-premises storage and Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.

Correct Answer: C

Community vote distribution

C (100%)

 **xplusfb** Highly Voted 2 years, 4 months ago

Selected Answer: C

This question quietly smell weird to me but no problem answer is C

Exp : AWS Schema Conversion Tool (SCT) can automatically convert the database schema from Microsoft SQL Server to Amazon RDS for MySQL. This allows for a smooth transition of the database schema without any manual intervention. AWS DMS can then be used to migrate the data from the on-premises databases to the newly created Amazon RDS for MySQL instance. This service can perform a one-time migration of the data or can set up ongoing replication of data changes to keep the on-premises and AWS databases in sync.

upvoted 9 times

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

Selected Answer: C

Use AWS Schema Conversion Tool (SCT) + AWS Database Migration Service (DMS)

SCT: Converts database schema and code (tables, indexes, stored procedures) from SQL Server to MySQL.

DMS: Handles data migration, with options for full load and ongoing replication (minimal downtime).

This is the standard AWS-recommended approach for heterogeneous migrations.

Low downtime + automated tools = ideal for business-critical apps.

upvoted 1 times

 **nimbus_00** 1 year, 2 months ago

Selected Answer: C

Schema conversion required!

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: C

This process becomes easier with services like AWS DMS and AWS Schema Conversion Tool (AWS SCT), which help you migrate your commercial database to an open-source database on AWS with minimal downtime.

In heterogeneous database migrations, the source and target databases engines are different, as in Oracle to Amazon Aurora, or Oracle to PostgreSQL, MySQL, or MariaDB migrations. The schema structure, data types, and database code in the source and target databases can be quite different, so the schema and code must be transformed before the data migration starts. For this reason, heterogeneous migration is a two-step process:

Step 1. Convert the source schema and code to match that of the target database. You can use AWS SCT for this conversion.

Step 2. Migrate data from the source database to the target database. You can use AWS DMS for this process.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-oracle-database/heterogeneous-migration.html>

upvoted 3 times

 **career360guru** 2 years ago

Selected Answer: C

Option C

upvoted 1 times

 **SK_Tyagi** 2 years, 4 months ago

Selected Answer: C

My 2 cents, Heterogeneous database migration and SCT go with each other

upvoted 3 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C of course

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: C

keyword = AWS Schema Conversion Tool

upvoted 1 times

 **rbm2023** 2 years, 7 months ago

Selected Answer: C

The question is about heterogeneous database migration so in this case we need to convert the DB to a new schema. Therefore, answer is C

upvoted 2 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

Use the AWS Schema Conversion Tool

upvoted 1 times

 **God_Is_Love** 2 years, 9 months ago

Selected Answer: C

For heterogeneous DBs, SCT is apt.

upvoted 1 times

 **Appon** 2 years, 10 months ago

Selected Answer: C

<https://aws.amazon.com/blogs/database/migrating-a-sql-server-database-to-a-mysql-compatible-database-engine/>

upvoted 2 times

 **Musk** 2 years, 10 months ago

Selected Answer: C

heterogeneous -> from one DB engine to another

upvoted 2 times

 **MasterP007** 2 years, 10 months ago

Straightforward - C

upvoted 2 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: C

C is the answer

upvoted 3 times

 **masetromain** 2 years, 11 months ago

Selected Answer: C

The correct answer is C. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MySQL. Then use AWS Database Migration Service (AWS DMS) to migrate the data from on-premises databases to Amazon RDS.

AWS Schema Conversion Tool (SCT) can automatically convert the database schema from Microsoft SQL Server to Amazon RDS for MySQL. This allows for a smooth transition of the database schema without any manual intervention.

AWS DMS can then be used to migrate the data from the on-premises databases to the newly created Amazon RDS for MySQL instance. This service can perform a one-time migration of the data or can set up ongoing replication of data changes to keep the on-premises and AWS databases in sync.

upvoted 4 times

 **masetromain** 2 years, 11 months ago

Option A is not correct because while Amazon RDS for MySQL supports SQL Server databases, it is not a good fit for migrating business-critical applications. The data model and architecture are different and would require significant re-engineering.

Option B is not correct because AWS Snowball Edge Storage Optimized devices are used for transferring large amounts of data to and from AWS, but they do not support SQL Server.

Option D is not correct because AWS DataSync can only transfer files and folders, it does not support SQL Server databases.

upvoted 2 times

Question #103

Topic 1

A publishing company's design team updates the icons and other static assets that an ecommerce web application uses. The company serves the icons and assets from an Amazon S3 bucket that is hosted in the company's production account. The company also uses a development account that members of the design team can access.

After the design team tests the static assets in the development account, the design team needs to load the assets into the S3 bucket in the production account. A solutions architect must provide the design team with access to the production account without exposing other parts of the web application to the risk of unwanted changes.

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

- A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket.
- B. In the development account, create a new IAM policy that allows read and write access to the S3 bucket.
- C. In the production account, create a role Attach the new policy to the role. Define the development account as a trusted entity.
- D. In the development account, create a role. Attach the new policy to the role Define the production account as a trusted entity.
- E. In the development account, create a group that contains all the IAM users of the design team Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role In the production account.
- F. In the development account, create a group that contains all the IAM users of the design team Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the development account.

Correct Answer: ACE

Community vote distribution

ACE (95%)	5%
-----------	----

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: ACE

The correct answer is A, C, and E.

A: In the production account, creating a new IAM policy that allows read and write access to the S3 bucket is correct because it allows the design team to upload and update the static assets in the S3 bucket in the production account.

C: In the production account, creating a role and attaching the new policy to the role, and defining the development account as a trusted entity is correct because it allows the design team from the development account to assume the role and access the S3 bucket in the production account, while limiting their access to only the specific resources and actions defined in the policy.

upvoted 14 times

 **masetromain** 2 years, 11 months ago

E: In the development account, creating a group that contains all the IAM users of the design team and attaching a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account is correct because it allows the users in the group to assume the role created in the production account, which gives them access to the S3 bucket in the production account.

The other choices are not correct because:

B: In the development account, creating a new IAM policy that allows read and write access to the S3 bucket is not correct because the design team needs to access the S3 bucket in the production account, not the development account.

upvoted 4 times

 **masetromain** 2 years, 11 months ago

D: In the development account, creating a role, attaching the new policy to the role and defining the production account as a trusted entity is not correct because the design team needs to assume a role in the production account to access the S3 bucket, not create a role in the development account.

F: In the development account, creating a group that contains all the IAM users of the design team and attaching a different IAM policy to the group to allow the sts:AssumeRole action on the role in the development account is not correct because the design team needs to assume a role in the production account to access the S3 bucket, not the development account.

upvoted 2 times

 **zejou1** Highly Voted 2 years, 9 months 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 11 times

✉ **LuongTo** 1 year ago

C: "creating a role and attaching the new policy to the role" => it is very clear to use the policy to control read write. A question about the role created with C, where to use?

upvoted 1 times

✉ **princajen** Most Recent 4 months, 4 weeks ago

Selected Answer: ACE

The correct answer is A, C, and E:

A: Creates the necessary permissions to write to the S3 bucket.

C: Creates a role in the production account that can be assumed by the development account.

E: Gives the design team (in the development account) permission to assume the cross-account role.

This setup follows AWS best practices for secure cross-account access with least privilege and isolation.

upvoted 1 times

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

- A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket.
- 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.

upvoted 1 times

✉ **Dgix** 1 year, 9 months ago

Selected Answer: ACE

ACE. F is a trap.

upvoted 1 times

✉ **career360guru** 2 years ago

Selected Answer: ACE

A, C and E

upvoted 1 times

✉ **AMohanty** 2 years, 1 month ago

BCE

Need to provide Account in Dev S3 Read Write Access

We define the permissions of the user in the Account it was created in

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: ACE

ACE in this case

upvoted 1 times

✉ **MoussaNoussa** 2 years, 6 months ago

ACE is the correct choice of course

upvoted 1 times

✉ **leehjworking** 2 years, 7 months ago

Selected Answer: ACE

Vote for ACE

upvoted 2 times

✉ **mfsec** 2 years, 9 months ago

Selected Answer: ACE

ACE is the best choice

upvoted 3 times

✉ **God_Is_Love** 2 years, 9 months ago

Selected Answer: ACE

Make Dev account as trusted entity. create a role in prod account. attache IAM policy of prod account and let development account assume this role to access prod s3 bucket.

upvoted 2 times

✉ **Musk** 2 years, 10 months ago

Selected Answer: ACE

I think it's clear
upvoted 1 times

 **tatdatpham** 2 years, 10 months ago

Selected Answer: ACE

ACE is correct answer
upvoted 2 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: ACE

ACE should works
upvoted 2 times

 **zhangyu20000** 2 years, 11 months ago

ACE is my answer
upvoted 2 times

 **masetromain** 2 years, 11 months ago

Selected Answer: ADE

A, D, and E are the correct steps that would meet the requirements.

A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket. This will allow the design team to read and write to the S3 bucket that holds the assets in the production account.

D. In the development account, create a role. Attach the new policy to the role. Define the production account as a trusted entity. This will allow the design team to assume a role in the development account that has permissions to access the S3 bucket in the production account.

E. In the development account, create a group that contains all the IAM users of the design team. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account. This will allow the users in the design team group to assume the role created in step D and access the S3 bucket in the production account.

upvoted 2 times

 **masetromain** 2 years, 11 months ago

Option B is not required because the design team needs to access the S3 bucket in the production account, not in the development account.

Option C is not required because the design team needs to access the S3 bucket in the production account and this can be done by assuming a role in the development account.

Option F is not required because the design team needs to access the S3 bucket in the production account and this can be done by assuming a role in the development account that is trusted by the production account.

upvoted 1 times

Question #104

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 Zone. Add a scale-out rule that will run if the sum CPU utilization is over 85% for 5 minutes.

Correct Answer: C*Community vote distribution*

C (96%)	4%
---------	----

 **Untamables** Highly Voted 2 years, 11 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 27 times

 **ninomfr64** Highly Voted 1 year, 11 months ago

A = you don't need to create a new application (instead you could create a new environment in the existing application)

B = traffic-split is used to deploy a new version of the app, not to scale out

C = correct

D = rebuild does not allow to change environment configuration <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environment-management-rebuild.html>

upvoted 5 times

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

Selected Answer: C

Modify the existing environment's capacity to load-balanced...

This is the most efficient solution:

No need to create new applications or environments.

Just change from single-instance to load-balanced type.

Configure auto scaling rule to scale out if CPU > 85%.

Meets the requirement and minimizes operational overhead.

upvoted 1 times

 **nimbus_00** 1 year, 2 months 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.

upvoted 2 times

 **amministrazione** 1 year, 3 months 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.

upvoted 1 times

 **Maygam** 2 years ago

Selected Answer: C

You can change the existing environment from single instance to load balanced.

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>

upvoted 3 times

 **career360guru** 2 years ago

Selected Answer: C

Option C

upvoted 1 times

 **yuliaqwerty** 2 years ago

C here <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/GettingStarted.EditConfig.html>

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: C

you can change existing Beanstalk environment type from a single instance to load-balanced

upvoted 2 times

 **CuteRunRun** 2 years, 4 months ago

Selected Answer: C

I prefer C

upvoted 1 times

 **Spaco** 2 years, 5 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 years, 5 months ago

Selected Answer: C

its a C

upvoted 1 times

 **leehjworking** 2 years, 7 months ago

Anybody know why we should select all AZs?

upvoted 4 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

Modify the existing environment's capacity configuration to use a load-balanced environment type.

upvoted 1 times

 **zejou1** 2 years, 9 months 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** 2 years, 9 months ago

Selected Answer: C

A is wrong. no need to re create new EB env when the question is asking to mitigate probable performance issues based on current compute consumption of >=85%

upvoted 2 times

 **spd** 2 years, 10 months ago

Selected Answer: C

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>

upvoted 2 times

Question #105

A finance company is running its business-critical application on current-generation Linux EC2 instances. The application includes a self-managed MySQL database performing heavy I/O operations. The application is working fine to handle a moderate amount of traffic during the month. However, it slows down during the final three days of each month due to month-end reporting, even though the company is using Elastic Load Balancers and Auto Scaling within its infrastructure to meet the increased demand.

Which of the following actions would allow the database to handle the month-end load with the LEAST impact on performance?

- A. Pre-warming Elastic Load Balancers, using a bigger instance type, changing all Amazon EBS volumes to GP2 volumes.
- B. Performing a one-time migration of the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month.
- C. Using Amazon CloudWatch with AWS Lambda to change the type, size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric.
- D. Replacing all existing Amazon EBS volumes with new PIOPS volumes that have the maximum available storage size and I/O per second by taking snapshots before the end of the month and reverting back afterwards.

Correct Answer: B*Community vote distribution*

B (93%)	7%
---------	----

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: B

B. Performing a one-time migration of the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month.

This is the optimal solution as migrating the database to Amazon RDS will provide the ability to easily scale read replicas for handling increased read traffic during the end of the month. Additionally, RDS will manage the underlying infrastructure and provide automatic backups, software patching, and monitoring, which will reduce the operational overhead for the company.

Option A may help but it will not be sufficient to handle the heavy load, option C and D are not efficient solutions to han
upvoted 16 times

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

Selected Answer: B

Migrate to Amazon RDS + Add Read Replicas:
 This moves the workload to managed RDS, reducing operational burden.
 Adding read replicas offloads read/reporting queries from the primary.
 Can scale read replicas just for month-end (temporarily).
 Great match for reporting load (which is read-heavy).
 Minimal operational overhead — RDS handles patching, backups, etc.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: B

B, include read replicas
upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: B

Option B -> Reporting workload = higher read operation ==> Solution RDS read replica.
upvoted 1 times

 **hansean** 2 years, 2 months ago

Selected Answer: D

I go with D
upvoted 1 times

 **uC6rW1aB** 2 years, 3 months ago

Selected Answer: D

I vote D

To solve heavy IO issue, I think both option B and D both works. But the question demands for to "handle the month-end load with the LEAST impact on performance", Option B create the new read replicas during end of month seems too complicated, you'll need to separate read/write traffic from application at the end of the month.

upvoted 1 times

 **venvig** 2 years, 3 months 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** 2 years, 4 months 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 years, 5 months ago

Selected Answer: B

B of course

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months 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 years, 5 months ago

month end reporting is to submit the financial data, aka write the new data to DB

upvoted 2 times

 **mfsec** 2 years, 9 months ago

Selected Answer: B

Performing a one-time migration

upvoted 1 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: B

B is the best solution

upvoted 2 times

Question #106

Topic 1

A company runs a Java application that has complex dependencies on VMs that are in the company's data center. The application is stable, but the company wants to modernize the technology stack. The company wants to migrate the application to AWS and minimize the administrative overhead to maintain the servers.

Which solution will meet these requirements with the LEAST code changes?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Grant the ECS task execution role permission to access the ECR image repository. Configure Amazon ECS to use an Application Load Balancer (ALB). Use the ALB to interact with the application.
- B. Migrate the application code to a container that runs in AWS Lambda. Build an Amazon API Gateway REST API with Lambda integration. Use API Gateway to interact with the application.
- C. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) on EKS managed node groups by using AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Give the EKS nodes permission to access the ECR image repository. Use Amazon API Gateway to interact with the application.
- D. Migrate the application code to a container that runs in AWS Lambda. Configure Lambda to use an Application Load Balancer (ALB). Use the ALB to interact with the application.

Correct Answer: A

Community vote distribution

A (94%) 6%

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: A

The correct answer would be A, as migrating the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Container and storing container images in Amazon Elastic Container Registry (Amazon ECR) would minimize the code changes and administrative overhead required to maintain the servers. This option would allow the company to use the Application Load Balancer (ALB) to interact with the application and the ECS task execution role permission to access the ECR image repository.

Option B would require the application code to be migrated to a container that runs in AWS Lambda, which would require more code changes.

Option C would require migrating the application to Amazon Elastic Kubernetes Service (Amazon EKS) which would require more administrative overhead.

Option D would require configuring Lambda to use an Application Load Balancer (ALB), which is not a native feature of Lambda.
upvoted 20 times

 **Musk** 2 years, 10 months ago

B does not say anything about Lambda. Where have you read that?

upvoted 1 times

 **Musk** 2 years, 10 months ago

You are right, I mixed A with B

upvoted 1 times

 **rbm2023** 2 years, 7 months ago

There is another problem with Option B, it suggests using EKS with managed node groups and not Fargate, which breaks the requirement for reducing administrative overhead

upvoted 1 times

 **masetromain** 2 years, 11 months ago

This solution allows for the existing application code to be packaged into a container, which can then be deployed to ECS on Fargate. The use of AWS App2Container will help automate the containerization process, minimizing the need for code changes. Additionally, by using ECR to store container images, the application can continue to use the same images and dependencies that it currently relies on. The use of an Application Load Balancer (ALB) to interact with the application further simplifies the migration process by allowing the use of the existing application's endpoint.

upvoted 4 times

 **zejou1** Highly Voted 2 years, 9 months 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 9 times

princajen Most Recent 4 months, 4 weeks ago

Selected Answer: A

ECS on AWS Fargate + App2Container + ALB:

App2Container is made for this! It containerizes existing Java and .NET apps without needing code changes.

Fargate is serverless for containers → no EC2 server management.

Uses ALB for traffic — common and efficient for web apps.

Amazon ECR for storing images.

Just containerize and deploy → fits the scenario perfectly.

upvoted 1 times

princajen 4 months, 4 weeks ago

Selected Answer: A

ECS on AWS Fargate + App2Container + ALB:

App2Container is made for this! It containerizes existing Java and .NET apps without needing code changes.

Fargate is serverless for containers → no EC2 server management.

Uses ALB for traffic — common and efficient for web apps.

Amazon ECR for storing images.

Just containerize and deploy → fits the scenario perfectly.

upvoted 1 times

amministrazione 1 year, 3 months ago

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.

upvoted 1 times

gofavad926 1 year, 9 months ago

Selected Answer: A

A, ECS Fargate

upvoted 1 times

AimarLeo 1 year, 11 months ago

Selected Answer: A

If the keyword 'Java' has not been mentioned, Answer A would have been considered as A2C (App2Container) is valid only for Java and .Net web applications

upvoted 2 times

ninomfr64 1 year, 11 months ago

Selected Answer: A

A = correct

B = migrating app to container to be executed in a Lambda requires more code changes

C = EKS with managed node group requires more operations than ECS with Fargate

D = see B

upvoted 1 times

career360guru 2 years ago

Selected Answer: A

Option A. Option C is not valid because using API Gateway is not needed and may require more code changes.

upvoted 2 times

severlight 2 years, 1 month ago

Selected Answer: A

In the case of Fargate capacity provider, you should grant permissions to access ECR to task execution role, otherwise to EC2 instance roles which you run containers on

upvoted 1 times

CVDON 2 years, 2 months ago

Sorry is A

upvoted 1 times

CVDON 2 years, 2 months ago

C on EKS because of complex VM dependencies

upvoted 1 times

 **CVDON** 2 years, 2 months ago

D because of complex vm dependencies
upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

it's an A
upvoted 1 times

 **Maria2023** 2 years, 6 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** 2 years, 8 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** 2 years, 9 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

Question #107

A company has an asynchronous HTTP application that is hosted as an AWS Lambda function. A public Amazon API Gateway endpoint invokes the Lambda function. The Lambda function and the API Gateway endpoint reside in the us-east-1 Region. A solutions architect needs to redesign the application to support failover to another AWS Region.

Which solution will meet these requirements?

- A. Create an API Gateway endpoint in the us-west-2 Region to direct traffic to the Lambda function in us-east-1. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure API Gateway to direct traffic to the SQS queue instead of to the Lambda function. Configure the Lambda function to pull messages from the queue for processing.
- C. Deploy the Lambda function to the us-west-2 Region. Create an API Gateway endpoint in us-west-2 to direct traffic to the Lambda function in us-west-2. Configure AWS Global Accelerator and an Application Load Balancer to manage traffic across the two API Gateway endpoints.
- D. Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.

Correct Answer: D*Community vote distribution*

D (95%)	5%
---------	----

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: D

The correct answer is D. Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints. This solution meets the requirement of having a failover to another region by having a copy of the Lambda function and API Gateway endpoint in a different region, and using Route 53's failover routing policy to route traffic between the two regions.

Option A is not correct because it only creates an additional API Gateway endpoint in us-west-2 and relies on Route 53's failover routing policy to direct traffic to the correct endpoint. But it does not deploy the Lambda function to the new region and this makes the failover incomplete.

upvoted 24 times

 **masetromain** 2 years, 11 months ago

Option B is not correct because it uses a SQS queue as a buffer between the API Gateway and the Lambda function, but this does not provide failover to another region. In addition, it would also increase the latency of the system as the SQS will act as an additional layer.

Option C is not correct because it deploys the Lambda function to the us-west-2 Region and creates an API Gateway endpoint in the same region. But it uses AWS Global Accelerator and an Application Load Balancer to manage traffic across the two API Gateway endpoints. However, this is not a failover solution as both regions will be active and serving traffic at the same time.

upvoted 3 times

 **testingaws123** 2 years, 9 months ago

You always use ChatGPT to paste answers. Most of the time ChatGPT gives wrong answers do you know this?

upvoted 12 times

 **juanife** 10 months, 2 weeks ago

If the answer explanation of why it's one option and why the other ones are not ok truly represents the correct answer then I would not say anything. I think chat gpt is very useful if you (with knowledge on mind) are able to judge what this ai machine says and validate that.

upvoted 1 times

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

Selected Answer: D

Deploy Lambda + API Gateway to us-west-2; use Route 53 failover

This is the ideal solution.

Fully regional: deploy redundant infrastructure in us-west-2.

Use Route 53 failover routing policy to direct traffic:

If us-east-1 is healthy → traffic goes there.

If us-east-1 fails → failover to us-west-2.

Works with asynchronous workloads.

Simple and reliable.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: D

D, deploy everything in the second region and configure the failover routing policy

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: D

Option D

upvoted 1 times

 **venvig** 2 years, 3 months 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 years, 5 months ago

Selected Answer: D

clearly D

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: D

Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region

upvoted 1 times

 **zejou1** 2 years, 9 months 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** 2 years, 9 months 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** 2 years, 11 months ago

Selected Answer: D

The correct answer is D

upvoted 2 times

 **zhangyu20000** 2 years, 11 months ago

D is correct

A is not because the Lambda is in us-east-1 but api gateway is in us-west-2. cannot cross regions

upvoted 4 times

 **masetromain** 2 years, 11 months ago

Selected Answer: A

The correct answer is A.

In this solution, an API Gateway endpoint is created in the us-west-2 Region. This new endpoint is configured to direct traffic to the Lambda function in us-east-1. If a failure occurs in the us-east-1 Region, Amazon Route 53's failover routing policy automatically routes traffic to the us-west-2 Region. This ensures that traffic is directed to a healthy endpoint, providing failover support for the application.

B, C and D does not meet the requirement of having failover routing policy.

In B, SQS is not a failover mechanism, it is a messaging service and it does not provide failover routing.

In C, Global Accelerator and Application Load Balancer does not provide failover routing.

In D, While creating a second endpoint in the us-west-2 Region and using Amazon Route 53 to route traffic to it, it still does not provide failover routing.

upvoted 2 times

✉️ **CProgrammer** 2 years, 3 months ago

D CLEARLY States: Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints. You claimed it did not , and the moderator ALLOWED IT ?!? !?

upvoted 1 times

✉️ **CProgrammer** 2 years, 3 months ago

Gateway VPC endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC.

<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html>

==> IN CONTRAST

These are the ENDPOINTS for API Gateway:

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

Gateway endpoint DOES NOT DIRECT TRAFFIC PERIOD

upvoted 1 times

Question #108

Topic 1

A retail company has structured its AWS accounts to be part of an organization in AWS Organizations. The company has set up consolidated billing and has mapped its departments to the following OUs: Finance, Sales, Human Resources (HR), Marketing, and Operations. Each OU has multiple AWS accounts, one for each environment within a department. These environments are development, test, pre-production, and production.

The HR department is releasing a new system that will launch in 3 months. In preparation, the HR department has purchased several Reserved Instances (RIs) in its production AWS account. The HR department will install the new application on this account. The HR department wants to make sure that other departments cannot share the RI discounts.

Which solution will meet these requirements?

- A. In the AWS Billing and Cost Management console for the HR department's production account turn off RI sharing.
- B. Remove the HR department's production AWS account from the organization. Add the account to the consolidating billing configuration only.
- C. In the AWS Billing and Cost Management console, use the organization's management account to turn off RI Sharing for the HR department's production AWS account.
- D. Create an SCP in the organization to restrict access to the RIs. Apply the SCP to the OUs of the other departments.

Correct Answer: C

Community vote distribution

C (80%) 11% 9%

 **kiran15789**  2 years, 9 months ago

Selected Answer: C

Management account --> Billing Dashboard --> Billing preferences, this option is there to choose enable/disable RI discounts sharing
upvoted 9 times

 **princajen**  4 months, 4 weeks ago

Selected Answer: C

From the management account, turn off RI sharing for the HR production account.
This is the correct approach.

The management account can disable "shared RI discount allocation" for specific linked accounts.
This ensures only HR's production account uses its RIs — no cross-account discounting.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 2 times

 **Dgix** 1 year, 9 months ago

Selected Answer: C

It is indeed C.
upvoted 2 times

 **Dgix** 1 year, 9 months ago

Selected Answer: A

RI sharing is done for the whole Org. It's all or nothing, and it's done in the Billing and Cost Management console in the Org account.
upvoted 2 times

 **JOKERO** 1 year, 9 months ago

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

C

upvoted 1 times

 **helloworldabc** 1 year, 3 months ago

just C

upvoted 1 times

 **8608f25** 1 year, 10 months ago

Selected Answer: A

Option A is correct because AWS allows the management of RI sharing settings at the account level within the AWS Billing and Cost Management console. By turning off RI sharing in the HR department's production account, the RI benefits (such as the discounted rate) are applied only to instances within that account, preventing other accounts, even within the same organization, from accessing these discounts. This directly addresses the requirement.

Option C suggests using the organization's management account to turn off RI sharing for the HR department's production AWS account. While the management account controls many aspects of AWS Organizations, including consolidated billing, RI sharing preferences are managed at the individual account level within the Billing and Cost Management console, not directly through the management account for specific accounts.

upvoted 2 times

 **Chris_W_1234** 2 months, 2 weeks ago

Quote: The management account of an organization can deactivate Reserved Instance discount and Savings Plans discount sharing for any accounts in that organization, including the management account. This means that Reserved Instances and Savings Plans discounts aren't shared between any accounts that have deactivated sharing.

From <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

upvoted 1 times

 **horyoryo** 2 years ago

Selected Answer: C

option C

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: C

Option C

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

surely C

upvoted 3 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

C is the way to go

upvoted 1 times

 **sambb** 2 years, 9 months ago

Selected Answer: C

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

upvoted 3 times

 **God_Is_Love** 2 years, 9 months ago

Selected Answer: C

Management account --> Billing Dashboard --> Billing preferences, this option is there to choose enable/disable RI discounts sharing
<https://us-east-1.console.aws.amazon.com/billing/home#/preferences>

upvoted 3 times

 **testingaws123** 2 years, 10 months ago

Selected Answer: D

How can you restrict access from AWS billing console? Can you show me please??

Option D is the correct solution because an SCP (Service Control Policy) can be created in the AWS Organizations service to restrict access to specific resources or actions across the entire organization or specific OUs. In this case, an SCP can be created to restrict other departments from accessing the RIs purchased by the HR department's production account. This ensures that the discounts are not shared with other departments.

upvoted 3 times

 **God_Is_Love** 2 years, 9 months 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 5 times

 **chikorita** 2 years, 4 months ago

initially i thought the same....but the catch here is that RIs are purchased in HR Prod department

So, we have to work on disabling discount sharing wrt that account so that IT IS NOT SHARED W OTHERS and this actions can only be performed from Management account

upvoted 1 times

 **SK_Tyagi** 2 years, 4 months ago

Restricting the access to RI's is not the ask in the question, only "restricting the RI discounts" from HR to other departments is the ask, and that you could be done by Management Account (as identified by others in this forum). Hope that helps!

upvoted 2 times

 **jojom19980** 2 years, 10 months ago

Selected Answer: C

The correct answer is C

upvoted 1 times

 **masetromain** 2 years, 11 months ago

Selected Answer: C

The correct answer is C.

In this solution, the organization's management account can be used to turn off RI sharing for the HR department's production AWS account in the AWS Billing and Cost Management console. This will ensure that the other departments cannot share the RI discounts and the HR department can use the RIs for their new system without any interruption.

upvoted 3 times

 **masetromain** 2 years, 11 months ago

A, B and D does not meet the requirement of turning off RI sharing for the HR department's production AWS account.

In A, Turning off RI sharing in the HR department's production account will not prevent other departments from sharing the RI discounts.

In B, Removing the HR department's production AWS account from the organization may cause issues in consolidated billing and it does not prevent other departments from sharing the RI discounts.

In D, Creating an SCP in the organization to restrict access to the RIs is not necessary because the management account can directly turn off the RI sharing, it also does not prevent other departments from sharing the RI discounts.

upvoted 3 times

Question #109

Topic 1

A large company is running a popular web application. The application runs on several Amazon EC2 Linux instances in an Auto Scaling group in a private subnet. An Application Load Balancer is targeting the instances in the Auto Scaling group in the private subnet. AWS Systems Manager Session Manager is configured, and AWS Systems Manager Agent is running on all the EC2 instances.

The company recently released a new version of the application. Some EC2 instances are now being marked as unhealthy and are being terminated. As a result, the application is running at reduced capacity. A solutions architect tries to determine the root cause by analyzing Amazon CloudWatch logs that are collected from the application, but the logs are inconclusive.

How should the solutions architect gain access to an EC2 instance to troubleshoot the issue?

- A. Suspend the Auto Scaling group's HealthCheck scaling process. Use Session Manager to log in to an instance that is marked as unhealthy.
- B. Enable EC2 instance termination protection. Use Session Manager to log in to an instance that is marked as unhealthy.
- C. Set the termination policy to OldestInstance on the Auto Scaling group. Use Session Manager to log in to an instance that is marked as unhealthy.
- D. Suspend the Auto Scaling group's Terminate process. Use Session Manager to log in to an instance that is marked as unhealthy.

Correct Answer: D*Community vote distribution*

D (93%) 7%

 **zozza2023**  2 years, 11 months ago

Selected Answer: D

The correct answer is D.

upvoted 10 times

 **God_Is_Love**  2 years, 9 months 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 9 times

 **princajen**  4 months, 4 weeks ago

Selected Answer: D

Suspend the Auto Scaling group's Terminate process. Use Session Manager to log in...

This is the correct answer.

ASG has multiple processes — including:

Launch
Terminate
HealthCheck
ReplaceUnhealthy

By suspending the Terminate process, the ASG won't terminate unhealthy instances.

You can then use Session Manager to log in and troubleshoot before it's terminated.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

D. Suspend the Auto Scaling group's Terminate process. Use Session Manager to log in to an instance that is marked as unhealthy.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: D

D, stop the autoscaling process

upvoted 1 times

 **AWSLord32** 1 year, 11 months ago

Why not B? Can the ASG override the EC2 termination protection?

upvoted 3 times

 **career360guru** 2 years ago

Selected Answer: D

Option D

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: D

you can stop auto-scaling processes, here you need to stop termination, you need health checks to know which instance to check
upvoted 2 times

 **venvig** 2 years, 3 months 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 4 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: D

d of course

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: D

keyword == Auto Scaling group's Terminate process.

upvoted 1 times

 **Alando** 2 years, 3 months ago

Have you cleared the exam?

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: D

Suspend the Auto Scaling group's Terminate process.

upvoted 2 times

 **zejou1** 2 years, 9 months ago

Selected Answer: D

Amazon EC2 Auto Scaling stops marking instances unhealthy as a result of EC2 and Elastic Load Balancing health checks. Your custom health checks continue to function properly. After you suspend HealthCheck, if you need to, you can manually set the health state of instances in your group and have ReplaceUnhealthy replace them.

Suspending the Terminate process doesn't prevent the successful termination of instances using the force delete option with the delete-auto-scaling-group command.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html>

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

We want the health checks to continue failing, just stop terminating to identify root cause

upvoted 4 times

 **testingaws123** 2 years, 10 months 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** 2 years, 9 months ago

That does not solve, it removes the healthcheck process, but also removes the ones that are being marked as unhealthy. The issue now is that one it is tagged as unhealthy they are being terminated. So, any that are already marked get terminated and you just removed the health checks to find remaining. you can't troubleshoot what you don't know.

upvoted 5 times

 **masetromain** 2 years, 11 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/51249-exam-aws-certified-solutions-architect-professional-topic-1/>

The correct answer is D.

In this solution, the architect can suspend the Auto Scaling group's Terminate process, which will prevent the instances marked as unhealthy from being terminated. This will allow the architect to log in to the instance using Session Manager and troubleshoot the issue without losing access to the instance.

upvoted 7 times

 **masetromain** 2 years, 11 months ago

Option A is incorrect because suspending the HealthCheck scaling process will not prevent instances from being terminated.

Option B is incorrect because enabling EC2 instance termination protection will not prevent instances from being terminated by Auto Scaling group.

Option C is incorrect because setting the termination policy to OldestInstance on the Auto Scaling group will not prevent instances marked as unhealthy from being terminated.

upvoted 4 times

Question #110

A company wants to deploy an AWS WAF solution to manage AWS WAF rules across multiple AWS accounts. The accounts are managed under different OUs in AWS Organizations.

Administrators must be able to add or remove accounts or OUs from managed AWS WAF rule sets as needed. Administrators also must have the ability to automatically update and remediate noncompliant AWS WAF rules in all accounts.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Use AWS Firewall Manager to manage AWS WAF rules across accounts in the organization. Use an AWS Systems Manager Parameter Store parameter to store account numbers and OUs to manage. Update the parameter as needed to add or remove accounts or OUs. Use an Amazon EventBridge rule to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account.
- B. Deploy an organization-wide AWS Config rule that requires all resources in the selected OUs to associate the AWS WAF rules. Deploy automated remediation actions by using AWS Lambda to fix noncompliant resources. Deploy AWS WAF rules by using an AWS CloudFormation stack set to target the same OUs where the AWS Config rule is applied.
- C. Create AWS WAF rules in the management account of the organization. Use AWS Lambda environment variables to store account numbers and OUs to manage. Update environment variables as needed to add or remove accounts or OUs. Create cross-account IAM roles in member accounts. Assume the roles by using AWS Security Token Service (AWS STS) in the Lambda function to create and update AWS WAF rules in the member accounts.
- D. Use AWS Control Tower to manage AWS WAF rules across accounts in the organization. Use AWS Key Management Service (AWS KMS) to store account numbers and OUs to manage. Update AWS KMS as needed to add or remove accounts or OUs. Create IAM users in member accounts. Allow AWS Control Tower in the management account to use the access key and secret access key to create and update AWS WAF rules in the member accounts.

Correct Answer: A*Community vote distribution*

A (94%)

6%

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: A

The correct answer is A.

In this solution, AWS Firewall Manager is used to manage AWS WAF rules across accounts in the organization. An AWS Systems Manager Parameter Store parameter is used to store account numbers and OUs to manage. This parameter can be updated as needed to add or remove accounts or OUs. An Amazon EventBridge rule is used to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account. This solution allows for easy management of AWS WAF rules across multiple accounts with minimal operational overhead.

upvoted 20 times

 **masetromain** 2 years, 11 months ago

Option B does not meet the requirement of being able to add or remove accounts or OUs from managed AWS WAF rule sets as needed.

Option C is not the best approach as it requires manual configuration of the cross-account IAM roles and assume-role calls in the Lambda function, increasing the operational overhead.

Option D does not meet the requirement of providing a centralized management console to manage the WAF rules across multiple accounts.

upvoted 3 times

 **Aquaman** 9 months, 2 weeks ago

B doesn't allow you to target just accounts. The question is asking for a solution that can target accounts and OUs

upvoted 1 times

 **Untamables** Highly Voted 2 years, 11 months ago

Selected Answer: A

<https://aws.amazon.com/solutions/implementations/automations-for-aws-firewall-manager/>

upvoted 6 times

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

Selected Answer: A

Use AWS Firewall Manager + Parameter Store + EventBridge + Lambda:

Uses Firewall Manager, which is the right tool.

The use of Parameter Store to store account/OUs is flexible.

EventBridge + Lambda to auto-update policies = automates OU/account changes.

Least overhead compared to scripting or manual stacks.

upvoted 1 times

 **d0ug7979** 1 year, 3 months ago

Selected Answer: B

Correct answer is B. I would have said A like everyone else, but correct answer was provided in Udemy practice exam.

Thanks to Organization structure, Config rules apply automatically to newly added accounts (fulfills requirements: least amount of operational overhead (as opposed to A - manually maintaining accounts and OU list).

As often, AWS exam answers are partially off-track, a real-life deployment would be a clever combination of both A & B answers, using FW manager, Config and Cloudformation.

<https://aws.amazon.com/blogs/security/use-aws-firewall-manager-to-deploy-protection-at-scale-in-aws-organizations/>

upvoted 3 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: A

Option A

upvoted 1 times

 **venvig** 2 years, 3 months 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 5 times

 **CuteRunRun** 2 years, 4 months 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 years, 5 months ago

Selected Answer: A

A is a good option

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: A

keyword == AWS Firewall Manager

upvoted 3 times

 **tromyunpak** 2 years, 6 months ago

the correct answer is A <https://docs.aws.amazon.com/solutions/latest/automations-for-aws-firewall-manager/architecture-overview.html>
upvoted 2 times

 **rbm2023** 2 years, 7 months ago

Selected Answer: A

This is a complex question. But I voted A because the Firewall manager seems to be the correct way to centralize the rules across accounts.

Below are some interesting references I could find

<https://catalog.us-east-1.prod.workshops.aws/workshops/4cbaea3b-ceba-48e3-bd56-eca138f7a66c/en-US>

<https://aws.amazon.com/blogs/security/use-aws-firewall-manager-vpc-security-groups-to-protect-applications-hosted-on-ec2-instances/>

<https://aws.amazon.com/blogs/security/automatically-updating-aws-waf-rule-in-real-time-using-amazon-eventbridge/>

upvoted 3 times

 **mfsec** 2 years, 9 months ago

Selected Answer: A

Use AWS Firewall Manager to manage AWS WAF rules

upvoted 2 times

 **God_Is_Love** 2 years, 9 months ago

Selected Answer: A

Not D, KMS to store account numbers ?

upvoted 1 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: A

The correct answer is A.

upvoted 2 times

Question #111

A solutions architect is auditing the security setup of an AWS Lambda function for a company. The Lambda function retrieves the latest changes from an Amazon Aurora database. The Lambda function and the database run in the same VPC. Lambda environment variables are providing the database credentials to the Lambda function.

The Lambda function aggregates data and makes the data available in an Amazon S3 bucket that is configured for server-side encryption with AWS KMS managed encryption keys (SSE-KMS). The data must not travel across the Internet. If any database credentials become compromised, the company needs a solution that minimizes the impact of the compromise.

What should the solutions architect recommend to meet these requirements?

- A. Enable IAM database authentication on the Aurora DB cluster. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authentication. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- B. Enable IAM database authentication on the Aurora DB cluster. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authentication. Enforce HTTPS on the connection to Amazon S3 during data transfers.
- C. Save the database credentials in AWS Systems Manager Parameter Store. Set up password rotation on the credentials in Parameter Store. Change the IAM role for the Lambda function to allow the function to access Parameter Store. Modify the Lambda function to retrieve the credentials from Parameter Store. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- D. Save the database credentials in AWS Secrets Manager. Set up password rotation on the credentials in Secrets Manager. Change the IAM role for the Lambda function to allow the function to access Secrets Manager. Modify the Lambda function to retrieve the credentials from Secrets Manager. Enforce HTTPS on the connection to Amazon S3 during data transfers.

Correct Answer: A*Community vote distribution*

A (82%)

D (18%)

 **zozza2023**  2 years, 11 months ago

Selected Answer: A

a little bit confused between A and D but as said by others members D doesn't address the question of "data must not travel across the Internet"==> A is the answer

upvoted 20 times

 **MikelH93**  2 years, 8 months 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 8 times

 **princajen**  4 months, 3 weeks ago

Selected Answer: A

The best answer is Option A. It uses IAM database authentication, which eliminates the need for storing or rotating static credentials by using short-lived IAM tokens. This significantly reduces the impact of credential compromise. It also includes a VPC gateway endpoint for S3, ensuring that data transfers stay within AWS and do not traverse the public internet. This setup provides both strong security and low operational overhead, making it the best choice overall.

upvoted 2 times

 **Paul123456789** 9 months ago

Selected Answer: D

Option A does not address the requirement for rotating database credentials.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **MAZIADI** 1 year, 4 months ago

Selected Answer: A

A is better than D because it removes the complexity of managing the secret to connect to the DB and replaces it with the IAM DB authentication. In addition, S3 endpoint GW is better to prevent traffic going through the internet.

upvoted 1 times

 **AWSPro1234** 1 year, 9 months ago

Selected Answer: A

Key is data must not travel accros the internet mean use VPC gateway

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A, "data must no travel across the internet". This setup ensures internal network use only, meeting the security and networking requirements efficiently

upvoted 1 times

 **a54b16f** 1 year, 10 months ago

Selected Answer: A

The data must not travel across the Internet.

upvoted 2 times

 **8608f25** 1 year, 10 months ago

Selected Answer: D

Option D offers a comprehensive solution by leveraging AWS Secrets Manager for storing and automatically rotating database credentials, which directly addresses the concern of minimizing the impact if credentials become compromised. Changing the Lambda function to retrieve credentials from Secrets Manager enhances security by not storing credentials within environment variables. Enforcing HTTPS for S3 data transfers ensures the data in transit is encrypted. While deploying a gateway VPC endpoint for S3 (as mentioned in other options) is a best practice to keep traffic within the AWS network, enforcing HTTPS also contributes to securing data transfers without explicitly stating the need to avoid Internet travel. Secrets Manager inherently provides secure access to secrets without needing to travel across the Internet when accessed from AWS services within the same region.

Option A does not address the requirement for securing and rotating database credentials stored as Lambda environment variables.

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: A

Answer is A as S3 VPC is endpoint is needed to avoid data going over internet.

upvoted 1 times

 **task_7** 2 years, 3 months ago

Selected Answer: D

AWS Secrets Manager is meant for this job, why go with any other option

upvoted 2 times

 **task_7** 2 years, 3 months ago

My bad its A

D is not addressing this point

The data must not travel across the Internet

upvoted 6 times

 **CuteRunRun** 2 years, 4 months ago

I prefer A

upvoted 2 times

 **Jonalb** 2 years, 5 months ago

Selected Answer: A

A

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

upvoted 3 times

 **Jonalb** 2 years, 5 months ago

Selected Answer: D

https://docs.aws.amazon.com/pt_br/secretsmanager/latest/userguide/vpc-endpoint-overview.html

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

A for sure

upvoted 1 times

 **rbm2023** 2 years, 7 months ago

Selected Answer: A

I was about to chose D however just enforcing the HTTP will not avoid the data to travel across internet. You will need the option where the gateway VPC endpoint is deployed for access the S3. The answer is A.

A will also solve the issue related to authenticate the lambda to aurora without needing to store passwords, refer to -

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

upvoted 1 times

Question #112

A large mobile gaming company has successfully migrated all of its on-premises infrastructure to the AWS Cloud. A solutions architect is reviewing the environment to ensure that it was built according to the design and that it is running in alignment with the Well-Architected Framework.

While reviewing previous monthly costs in Cost Explorer, the solutions architect notices that the creation and subsequent termination of several large instance types account for a high proportion of the costs. The solutions architect finds out that the company's developers are launching new Amazon EC2 instances as part of their testing and that the developers are not using the appropriate instance types.

The solutions architect must implement a control mechanism to limit the instance types that only the developers can launch.

Which solution will meet these requirements?

- A. Create a desired-instance-type managed rule in AWS Config. Configure the rule with the instance types that are allowed. Attach the rule to an event to run each time a new EC2 instance is launched.
- B. In the EC2 console, create a launch template that specifies the instance types that are allowed. Assign the launch template to the developers' IAM accounts.
- C. Create a new IAM policy. Specify the instance types that are allowed. Attach the policy to an IAM group that contains the IAM accounts for the developers
- D. Use EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image.

Correct Answer: C
Community vote distribution

C (100%)

 masetromain Highly Voted 2 years, 11 months ago

Selected Answer: C

The correct answer is C.

In this solution, a new IAM policy is created that specifies the allowed instance types. This policy is then attached to an IAM group that contains the IAM accounts for the developers. This will ensure that the developers can only launch instances of the specified types, thus limiting the costs associated with the creation and termination of large instances.

upvoted 15 times

 masetromain 2 years, 11 months ago

A. Creating a desired-instance-type managed rule in AWS Config is not a sufficient solution, as it only identifies when an instance is launched with an unauthorized type, it does not prevent it.

B. Creating a launch template that specifies the instance types that are allowed is not a sufficient solution, because it limits the instances types that can be launched in the EC2 console, but it does not prevent the launch of instances through the AWS SDK, AWS CLI, or other AWS services.

D. Using EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image is not a direct solution to the problem of limiting the instance types that only the developers can launch. It can be useful for creating standardize images for the developers, but it does not provide the necessary control mechanism to limit the instance types.

upvoted 12 times

 gagol14 Highly Voted 1 year, 11 months ago

Selected Answer: C

```
{
  "Sid": "limitedSize",
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "ForAnyValue:StringNotLike": {
      "ec2:InstanceType": [
        "*.nano",
        "*.small",
        "*.micro",
        "*.medium"
      ]
    }
  }
}
```

```
}
```

```
}
```

upvoted 7 times

 **princajen** Most Recent  4 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Using IAM policies, you can control which EC2 instance types specific users (like developers) are allowed to launch. This is the only option that proactively prevents launching unapproved instance types. AWS Config (A) only detects after the fact, Launch Templates (B) are not enforceable, and Image Builder (D) doesn't control instance size. IAM policies offer a scalable and enforceable solution that aligns with the Well-Architected Framework's Cost Optimization pillar.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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

upvoted 1 times

 **cox1960** 1 year, 11 months ago

"an IAM group that contains the IAM accounts" ???

upvoted 1 times

 **igor12ghsj577** 1 year, 11 months ago

yes, in IAM group you have user IAM accounts.

upvoted 1 times

 **sse69** 1 year, 6 months ago

You have IAM users...Not IAM "accounts". Bad wording here...

upvoted 2 times

 **career360guru** 2 years ago

Selected Answer: C

Option C

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

Its a C

upvoted 1 times

 **Maria2023** 2 years, 6 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 2 times

 **Parimal1983** 2 years, 6 months ago

C is the correct solution remained. Typo mistake in the comments.

upvoted 1 times

 **easystoo** 2 years, 6 months ago

C-C-C-C-CC-C-C-CC-C-C-C-CC-

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

IAM policy..

upvoted 1 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: C

answer is C

upvoted 3 times

Question #113

A company is developing and hosting several projects in the AWS Cloud. The projects are developed across multiple AWS accounts under the same organization in AWS Organizations. The company requires the cost for cloud infrastructure to be allocated to the owning project. The team responsible for all of the AWS accounts has discovered that several Amazon EC2 instances are lacking the Project tag used for cost allocation.

Which actions should a solutions architect take to resolve the problem and prevent it from happening in the future? (Choose three.)

- A. Create an AWS Config rule in each account to find resources with missing tags.
- B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing.
- C. Use Amazon Inspector in the organization to find resources with missing tags.
- D. Create an IAM policy in each account with a deny action for ec2:RunInstances if the Project tag is missing.
- E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag.
- F. Use AWS Security Hub to aggregate a list of EC2 instances with the missing Project tag.

Correct Answer: ABE

Community vote distribution

ABE (81%)

Other

✉️ **God_Is_Love** Highly Voted 2 years, 9 months 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 7 times

✉️ **God_Is_Love** 2 years, 9 months 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 4 times

✉️ **OCHT** Highly Voted 2 years, 8 months 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 5 times

✉️ **OCHT** 2 years, 8 months 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 7 times

✉️ **AWSLord32** 1 year, 11 months ago

So what is the point of having A if you have E at an Org level?

upvoted 2 times

✉️ **fartosh** 1 year, 7 months ago

AWS Config aggregator does not run any rules on its own. Instead, it collects the data from the "source accounts" where AWS Config is enabled.

A to get the list of EC2 instances in each account.

E to aggregate the lists from all accounts in one place.

B to disallow creating non-compliant EC2 instances.

See <https://docs.aws.amazon.com/config/latest/developerguide/aggregate-data.html>.

upvoted 3 times

✉️ **OCHT** 2 years, 8 months ago

B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing.

By creating a Service Control Policy (SCP) in the organization, you can enforce a deny action for EC2 instances that do not have the required Project tag. This can prevent users from launching instances that are not tagged correctly and ensure that new instances are tagged properly for cost allocation. Here is the AWS Organizations documentation for creating SCPS: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

upvoted 5 times

 **amministrazione** Most Recent 1 year, 3 months ago

- 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.
 - E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag.
- upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: ABE

ABE, SCP + Config + Config Aggregator

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: BE

B and E handle the requirements in a centralised manner, giving least operational overhead, without anything needing to be added. The question is plainly wrongly stated. If three options have to be selected, then A is the least absurd one.

upvoted 3 times

 **8608f25** 1 year, 10 months ago

Selected Answer: ABE

- A. Create an AWS Config rule in each account to find resources with missing tags. AWS Config can evaluate the configuration of your AWS resources and identify resources that do not comply with specified requirements, such as missing specific tags. This helps in identifying existing resources with the issue.
- B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing. Service Control Policies (SCPs) can enforce permissions across all accounts in an organization. By creating an SCP that denies launching EC2 instances without the required Project tag, you can prevent the problem from occurring in the future at the organization level.
- E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag. An AWS Config aggregator can aggregate compliance data from multiple accounts and regions. This allows for centralized visibility of instances lacking the required tags, making it easier to address and resolve the issue across the entire organization.

upvoted 2 times

 **AWSLord32** 1 year, 11 months ago

Selected Answer: BDE

A is not needed if you have D. Correct answer is BDE.

upvoted 1 times

 **AWSLord32** 1 year, 11 months ago

I meant E, not D

upvoted 1 times

 **8608f25** 1 year, 10 months ago

It is not D. Create an IAM policy in each account with a deny action for ec2:RunInstances if the Project tag is missing.

IAM policies do not directly support conditional denies based on tag presence during the resource creation process in the same way SCPs do. This enforcement is better handled at the organization level with SCPs.

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: ABE

Option A, B and E

upvoted 1 times

 **Sandeep_B** 2 years, 2 months ago

Selected Answer: ABE

Inspector checks for Vulnerabilities but not the tags.

upvoted 3 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: ABE

its ABE

upvoted 2 times

 **youngmanaws** 2 years, 8 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 3 times

 **mfsec** 2 years, 9 months ago

Selected Answer: ABE

ABE is the better choice

upvoted 1 times

 **Damijo** 2 years, 9 months ago

what's the value of A and E together- it's either or ? the outcome is the same - thoughts?

upvoted 4 times

 **AWSLord32** 1 year, 11 months ago

Fully agree, BDE

upvoted 1 times

 **AWSLord32** 1 year, 11 months ago

Did some research..

Aggregators provide a read-only view into the source accounts and regions that the aggregator is authorized to view. Aggregators do not provide mutating access into the source account or region. For example, this means that you cannot deploy rules through an aggregator or pull snapshot files from the source account or region through an aggregator.
<https://docs.aws.amazon.com/config/latest/developerguide/config-concepts.html#multi-account-multi-region-data-aggregation>

So ABE seems correct

upvoted 2 times

 **jaysparky** 2 years, 10 months ago

ABE makes sense

upvoted 1 times

 **spd** 2 years, 10 months 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** 2 years, 10 months ago

Selected Answer: AE

BE makes sense

upvoted 1 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: ABE

the best way to deploy config rules accross accounts= SCP

upvoted 2 times

Question #114

A company has an on-premises monitoring solution using a PostgreSQL database for persistence of events. The database is unable to scale due to heavy ingestion and it frequently runs out of storage.

The company wants to create a hybrid solution and has already set up a VPN connection between its network and AWS. The solution should include the following attributes:

- Managed AWS services to minimize operational complexity.
- A buffer that automatically scales to match the throughput of data and requires no ongoing administration.
- A visualization tool to create dashboards to observe events in near-real time.
- Support for semi-structured JSON data and dynamic schemas.

Which combination of components will enable the company to create a monitoring solution that will satisfy these requirements? (Choose two.)

- A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events.
- B. Create an Amazon Kinesis data stream to buffer events. Create an AWS Lambda function to process and transform events.
- C. Configure an Amazon Aurora PostgreSQL DB cluster to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.
- D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards.
- E. Configure an Amazon Neptune DB instance to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.

Correct Answer: AD
Community vote distribution

AD (81%)

Other

 **God_Is_Love** Highly Voted  2 years, 9 months 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 14 times

 **OCHT** Highly Voted  2 years, 8 months 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 13 times

 **princajen** Most Recent  4 months, 3 weeks ago

Selected Answer: AD

So What Should You Pick: A or B?

Pick A (Firehose) if:

You care more about minimizing admin overhead.

"Near real-time" (60+ seconds delay) is acceptable.

You want simpler architecture (Firehose → OpenSearch).

Pick B (Streams) if:

You need true real-time ingestion.

You're okay with slightly more complexity/admin.

You want more control over how/when data is processed.

Let's Recheck the Clue:

"A buffer that automatically scales to match the throughput of data and requires no ongoing administration"

This screams Kinesis Firehose (A) — it's fully managed, auto-scales, and requires no manual configuration like shards.

upvoted 1 times

✉ **Paul123456789** 9 months ago

Selected Answer: BD

AWS Lambda is a source for Amazon Kinesis Data Firehose not a destination

<https://docs.aws.amazon.com/firehose/latest/dev/create-name.html>

<https://docs.aws.amazon.com/firehose/latest/dev/create-destination.html>

also, Firehose encountered timeout errors when calling AWS Lambda. The maximum supported function timeout is 5 minutes

<https://docs.aws.amazon.com/firehose/latest/dev/data-transformation.html>

correct answer B and D

upvoted 2 times

✉ **albert_kuo** 9 months, 4 weeks ago

Selected Answer: BD

Option B (Kinesis Data Streams + Lambda) + Option D (Amazon ES + Kibana):

Buffer: Kinesis Data Streams automatically scales and buffers events.

Processing: Lambda transforms JSON events and sends them to Amazon ES.

Storage: Amazon ES stores semi-structured JSON with dynamic schemas.

Visualization: Kibana provides near-real-time dashboards.

Managed: All services (Kinesis, Lambda, ES, Kibana) are fully managed.

Workflow: Events flow from on-premises via VPN to Kinesis → Lambda → ES → Kibana.

Result: Meets all requirements seamlessly.

upvoted 2 times

✉ **GabrielShiao** 11 months, 2 weeks ago

Selected Answer: BD

While most voted AD, I vote BD. I picked B instead of A because you can not use lambda to access the kinesis firehose directly.

upvoted 2 times

✉ **albert_kuo** 9 months, 4 weeks ago

Agreed

upvoted 1 times

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

A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events.

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.

upvoted 1 times

✉ **Smart** 1 year, 7 months ago

Selected Answer: AD

"A buffer that automatically scales to match the throughput of data and requires no ongoing administration."

I think buffer, here, means a solution that will reliably hold information for further successful processing. I don't think it means to buffer and batch process the events so I don't agree with other people's comments in regards to buffer.

That said, my concern is with "automatically scales to match the throughput of data". Firehose does it automatically. Kinesis can also do automatically if on-demand mode is chosen.

Also, "Support for semi-structured JSON data and dynamic schemas." Dynamic Schemas? Firehose or Data stream don't do that. Firehose does do dynamic partitioning and JSON deserializing. I guess that's what the question meant?

upvoted 1 times

✉ **TonytheTiger** 1 year, 8 months ago

Selected Answer: AD

Option A NOT Option B - Amazon Data Firehose buffers incoming streaming data in memory to a certain size (buffering size) and for a certain period of time (buffering interval) before delivering it to the specified destinations.

<https://docs.aws.amazon.com/firehose/latest/dev/buffering-hints.html>

upvoted 1 times

✉ **Dgix** 1 year, 9 months ago

Selected Answer: AD

On second thought: A because B requires manual shard configuration.

upvoted 1 times

✉ **Dgix** 1 year, 9 months ago

Selected Answer: BE

Also, Streams is more real-time.

upvoted 1 times

✉ **AWSum1** 1 year, 2 months ago

It says "Near Real Time" not "Real Time" so Firehouse is the better option between the 2

upvoted 1 times

✉ **Dgix** 1 year, 9 months ago

Selected Answer: BD

B rather than A because B integrates the lambda functionality for transformation of the data, which must be done as an added step in A, thereby increasing operational overhead.

upvoted 2 times

 **8608f25** 1 year, 10 months ago

Selected Answer: AD

A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events. Amazon Kinesis Data Firehose provides a fully managed service for effortlessly loading streaming data into AWS services such as Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk. It scales automatically to match the throughput of data and requires no ongoing administration. AWS Lambda can be used in conjunction with Kinesis Data Firehose to process and transform the data before it's loaded into the destination, supporting dynamic schemas and semi-structured JSON data. Additionally, Amazon Kinesis Data Firehose has built-in buffering capabilities and can be used to observe events in near-real time, making it a more appropriate choice for the given scenario.

upvoted 2 times

 **8608f25** 1 year, 10 months ago

D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards. Amazon Elasticsearch Service (Amazon ES) is a managed service that makes it easy to deploy, secure, operate, and scale Elasticsearch to search, analyze, and visualize data in real-time. Kibana is an open-source visualization tool designed to work with Elasticsearch, providing powerful and easy-to-use features to create dashboards that can visualize data in near-real-time.

upvoted 1 times

 **AimarLeo** 1 year, 11 months ago

ElasticSearch is the ex name of new OpenSearch

upvoted 2 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: BD

I choose Data Stream (KDS) over Data Firehose (KDF) in this scenario:

- KDS allows to you store events up to 1 year, allowing to achieve buffering with no constraints on size and with a very large time limit. KDS support on-demand capacity mode
- KDF transport mechanism is based on buffering, but here buffering is limited on size (max 128MiB) and time (up to 900 sec)

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: AD

A and D

upvoted 1 times

 **AMohanty** 2 years, 3 months ago

BD

Question states near-Real time

Thats the differentiating factor between Kinesis data stream and Firehose

I would go for B and D

upvoted 2 times

 **chikorita** 2 years, 3 months ago

but about "• Managed AWS services to minimize operational complexity."

i believe Kinesis Firehose is managed solution whereas DataStream required operational overhead

upvoted 2 times

Question #115

A team collects and routes behavioral data for an entire company. The company runs a Multi-AZ VPC environment with public subnets, private subnets, and an internet gateway. Each public subnet also contains a NAT gateway. Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads run in private subnets.

A solutions architect must review the infrastructure. The solution architect needs to reduce costs and maintain the function of the applications. The solutions architect uses Cost Explorer and notices that the cost in the EC2-Other category is consistently high. A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category.

What should the solutions architect do to meet these requirements?

- A. Enable VPC Flow Logs. Use Amazon Athena to analyze the logs for traffic that can be removed. Ensure that security groups are blocking traffic that is responsible for high costs.
- B. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that applications have the correct IAM permissions to use the interface VPC endpoint.
- C. Enable VPC Flow Logs and Amazon Detective. Review Detective findings for traffic that is not related to Kinesis Data Streams. Configure security groups to block that traffic.
- D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that the VPC endpoint policy allows traffic from the applications.

Correct Answer: D

Community vote distribution

D (80%)

B (20%)

 **God_Is_Love** Highly Voted  2 years, 9 months 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 14 times

 **Maria2023** Highly Voted  2 years, 6 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 10 times

 **4a86914** Most Recent  3 months ago

Selected Answer: D

While you need IAM permission to use a service, you don't need IAM permissions to use an interface VPC endpoint itself. Hence, B is incorrect.

Note that D is merely suggesting "Ensure that the VPC endpoint policy allows traffic from the applications.". It isn't saying VPC endpoint policy must be created. In brief, D is the correct answer.

upvoted 1 times

 **a9fb7b2** 3 months, 1 week ago

Selected Answer: B

answer is B

D mentions endpoint policy, but it's optional; by default the endpoint allows access, whereas IAM permissions are always required for the apps.

upvoted 1 times

 **Nad1122** 4 months, 2 weeks ago

Selected Answer: B

It is B. D is incorrect because default VPC endpoint policy allows all access.

upvoted 1 times

 **thanab** 4 months, 3 weeks ago

Selected Answer: B

i think B. I feel it
upvoted 1 times

 **princajen** 4 months, 3 weeks ago

Selected Answer: B

VPC endpoint policies control which principals can use the endpoint, but they don't grant permission to use the AWS service itself. The default policy allows all access, so in most cases you don't need to modify it. However, applications still require IAM permissions to perform actions like reading or writing to Kinesis. Therefore, for exam and real-world purposes, IAM access is the critical piece, and Option B is the best answer.

Think of it like this:

You built a private tunnel (VPC endpoint) from your office to AWS.
The tunnel gate (endpoint policy) is open by default.
But when your employee arrives at the AWS service door, the IAM guard still checks their ID badge (permissions).

If they don't have the right badge (IAM permission), they're still denied — even if the tunnel is open.

upvoted 1 times

 **kylx75** 11 months ago

Selected Answer: B

The correct answer is B.

Rationale:

Interface VPC endpoints for Kinesis eliminate NAT gateway traffic costs
Applications in private subnets can access Kinesis through the VPC endpoint
IAM permissions are the proper security control
Maintains functionality while reducing costs

Other options issues:

A/C: Flow logs analysis won't reduce NAT costs
D: Similar to B but focuses on endpoint policy instead of IAM permissions
upvoted 2 times

 **Heman31in** 1 year ago

Selected Answer: D

Why Option D is a Better Fit Here

Cost Reduction Goal: The scenario is primarily about reducing NAT gateway costs by using a VPC endpoint. A properly configured VPC endpoint policy ensures applications can connect to Kinesis through the private endpoint without hitting NAT gateways.
IAM Permissions Likely Already Exist: If the applications are already interacting with Kinesis, their IAM permissions should already be in place. The focus, therefore, shifts to configuring the new VPC endpoint properly.
Endpoint Policy Completeness: VPC endpoint policies act as a resource-based policy at the network level, which is critical for ensuring that applications can route their traffic correctly through the VPC endpoint.

upvoted 1 times

 **youonebe** 1 year, 1 month ago

Answer is B.

Option D is incorrect.

While similar to B, focuses on endpoint policy instead of IAM permissions
VPC endpoint policies alone are insufficient
IAM permissions are crucial for application access
upvoted 1 times

 **Syre** 1 year, 3 months ago

Selected Answer: B

Access Permissions are still required for most AWS services, including Kinesis Data Streams, even when accessed via a VPC endpoint. The endpoint allows traffic to the service, but your application or users still need IAM permissions to interact with the service. Without proper IAM permissions, even if the routing is set up correctly, the service will not authorize actions like reading from or writing to a Kinesis stream.

upvoted 2 times

 **amministrazione** 1 year, 3 months ago

D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that the VPC endpoint policy allows traffic from the applications.

upvoted 1 times

 **red_panda** 1 year, 8 months ago

Selected Answer: D

D without any doubt.
upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: D

D, VPC endpoint
upvoted 2 times

✉  **gofavad926** 1 year, 9 months ago

Selected Answer: D

D, VPC endpoint

upvoted 1 times

✉  **career360guru** 2 years ago

Selected Answer: D

Option D

upvoted 1 times

✉  **rif** 2 years, 2 months ago

Answer is D.

An endpoint policy is a resource-based policy that you attach to a VPC endpoint to control which AWS principals can use the endpoint to access an AWS service.

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

upvoted 1 times

Question #116

A retail company has an on-premises data center in Europe. The company also has a multi-Region AWS presence that includes the eu-west-1 and us-east-1 Regions. The company wants to be able to route network traffic from its on-premises infrastructure into VPCs in either of those Regions. The company also needs to support traffic that is routed directly between VPCs in those Regions. No single points of failure can exist on the network.

The company already has created two 1 Gbps AWS Direct Connect connections from its on-premises data center. Each connection goes into a separate Direct Connect location in Europe for high availability. These two locations are named DX-A and DX-B, respectively. Each Region has a single AWS Transit Gateway that is configured to route all inter-VPC traffic within that Region.

Which solution will meet these requirements?

- A. Create a private VIF from the DX-A connection into a Direct Connect gateway. Create a private VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with the Direct Connect gateway. Peer the transit gateways with each other to support cross-Region routing.
- B. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Associate the eu-west-1 transit gateway with this Direct Connect gateway. Create a transit VIF from the DX-B connection into a separate Direct Connect gateway. Associate the us-east-1 transit gateway with this separate Direct Connect gateway. Peer the Direct Connect gateways with each other to support high availability and cross-Region routing.
- C. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway. Configure the Direct Connect gateway to route traffic between the transit gateways.
- D. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway. Peer the transit gateways with each other to support cross-Region routing.

Correct Answer: D*Community vote distribution*

D (91%)	7%
---------	----

 **God_Is_Love**  2 years, 9 months 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 16 times

 **God_Is_Love** 2 years, 9 months ago

Whichever option has this text is correct - "Peer the transit gateways with each other to support cross-Region routing"

upvoted 5 times

 **strike3test** 6 months, 1 week ago

Option D is incorrect because it suggests peering Transit Gateways to support cross-Region routing. While Transit Gateway peering is possible, it is not required when using a Direct Connect gateway, which can route traffic between associated Transit Gateways directly, reducing operational complexity

upvoted 1 times

 **princajen**  4 months, 3 weeks ago

Selected Answer: D

Use Transit VIFs from each Direct Connect link to connect to a single Direct Connect Gateway. Associate both Transit Gateways (in eu-west-1 and us-east-1) with the DXGW to allow on-premises traffic to reach both Regions. Then, peer the Transit Gateways to enable inter-region VPC traffic. This setup uses managed services, supports high availability (via two DXs), and enables full cross-region and hybrid connectivity.

upvoted 1 times

 **Syre** 1 year, 3 months ago

Selected Answer: C

While transit gateway peering can enable cross-Region VPC communication, it is not necessary when you are using a Direct Connect gateway. A Direct Connect gateway already provides the capability to route traffic across multiple Regions without needing to peer the transit gateways directly.

upvoted 2 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **teo2157** 1 year, 8 months ago

It can be both A or D based on AWS documentation: <https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/hybrid-network-connections.html>

upvoted 2 times

 **Dgix** 1 year, 9 months ago

Selected Answer: D

Don't let "No single points of failure can exist on the network" mislead you into thinking that you need two DCGWs. DCGWs are not part of the region they connect to. Therefore, no SPOF translates to a double DC connection to a single DCGW. Hence, D.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: D

D, this approach ensures high availability and robust network connectivity across the specified AWS regions and the on-premises data center.

upvoted 1 times

 **_Jassybanga_** 1 year, 10 months ago

Answer D - As per from AWS

<https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-aws-transit-gateway-multi-regions-more-than-3.html>

upvoted 3 times

 **career360guru** 2 years ago

Selected Answer: D

Choice is between C and D. Better the two D is the right option.

upvoted 1 times

 **subupro** 2 years ago

D is correct ref architecture <https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-aws-transit-gateway-multi-regions-and-aws-public-peering.html>

upvoted 4 times

 **mnsait** 1 year, 1 month ago

This is the best answer I found for this question. Thank you @subupro for the reference. It explains exactly what is needed to understand here.

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: D

Answer D. Peer the transit gateways for cross-region routing.

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: D

to connect to transit gateways through the dx gateway you should use transit VIF

upvoted 1 times

 **frfavoreto** 2 years, 3 months ago

I agree 'D' is a good answer to the problem, but isn't the DXGW a single point of failure?

Question says "No single points of failure can exist on the network."

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: D

it's D

upvoted 1 times

 **happystrawberry** 2 years, 7 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** 2 years, 7 months ago

Actually, D is a proper answer.
upvoted 1 times

✉️  **rbm2023** 2 years, 7 months 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** 2 years, 7 months 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** 2 years, 8 months 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

Question #117

A company is running an application in the AWS Cloud. The company's security team must approve the creation of all new IAM users. When a new IAM user is created, all access for the user must be removed automatically. The security team must then receive a notification to approve the user. The company has a multi-Region AWS CloudTrail trail in the AWS account.

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

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule. Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.
- B. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Invoke a container that runs in Amazon Elastic Container Service (Amazon ECS) with AWS Fargate technology to remove access.
- D. Invoke an AWS Step Functions state machine to remove access.
- E. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.
- F. Use Amazon Pinpoint to notify the security team.

Correct Answer: ADE

Community vote distribution

ADE (74%)	12%	9%
-----------	-----	----

 **God_Is_Love** Highly Voted 2 years, 9 months 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 14 times

 **Jay_2pt0_1** 2 years, 7 months ago

I agree with this.
upvoted 1 times

 **hobokabobo** 2 years, 9 months ago

this explanation makes sense to me.
upvoted 1 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: ADE

When a new IAM user is created, CloudTrail logs the CreateUser event. EventBridge matches the event and triggers a Step Functions state machine, which removes access by calling IAM actions like detaching policies or disabling the login profile. The state machine then uses SNS to notify the security team. This architecture is fully serverless, scalable, and provides auditability, fulfilling all requirements from detection to access mitigation and alerting.

upvoted 1 times

 **sergza888** 6 months, 1 week ago

Selected Answer: ACE

I Just do not see any reasoning to use step functions. There is no orchestration involved here. you just need lambda or Fargate to remove the access. D does not say anything about lambda step at all i think it is just distractor
upvoted 1 times

 **amministrazione** 1 year, 3 months ago

- 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.
- D. Invoke an AWS Step Functions state machine to remove access.
- E. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.

upvoted 1 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: ACE

Option ADE: Most people agree with option AE. There can be situations where human intervention is required before the workflow can progress. For example, approving a substantial credit increase may require human approval

<https://docs.aws.amazon.com/step-functions/latest/dg/use-cases-security-automation.html>

upvoted 1 times

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

just ADE

upvoted 1 times

✉️ **24Gel** 1 year, 9 months ago

Why not BCE? or ACE?

How to use Step Function to remove permission?

upvoted 1 times

✉️ **dankositze** 1 year, 10 months ago

Poorly constructed answer choices, but ADE is the least worst option.

upvoted 2 times

✉️ **zanhsieh** 1 year, 10 months ago

Selected Answer: ADE

I picked ADE. EventBridge, Lambda / Step Function, and SNS are required.

BDE: No. CloudTrail can't trigger Step Function directly.

ABE: No. This solution can't remove the user access automatically.

Choosing B alone without A can't directly trigger Lambda / Step functions to remove the user access. C can't compare with D. F is not relevant.

upvoted 1 times

✉️ **AWSLord32** 1 year, 11 months ago

Selected Answer: BDE

Eventbridge is not needed. Clouptrail can send notifications to SNS directly

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/configure-sns-notifications-for-cloudtrail.html>

upvoted 3 times

✉️ **AWSLord32** 1 year, 11 months ago

Also, if you select ADE how would the event ever trigger SNS to send the notification?

upvoted 2 times

✉️ **fartosh** 1 year, 7 months ago

What do you mean? SNS topic is one of the (many) allowed targets for EventBridge.

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-targets.html>

Regarding "Eventbridge is not needed" - it's only true for notifications because CloudTrail integrates with SNS. CloudTrail alone cannot trigger any automation tools like Lambda or Step Function. That's why EventBridge is better in this case. You can add both targets to the same rule.

upvoted 1 times

✉️ **altonh** 11 months, 2 weeks ago

"You can be notified when CloudTrail publishes new log files to your Amazon S3 bucket. You manage notifications using Amazon Simple Notification Service (Amazon SNS)."

That's the only notification you are getting. It's not good enough. You need the actual API call made, which is the user creation API.

upvoted 1 times

✉️ **bjexamprep** 1 year, 11 months ago

Selected Answer: ACE

Step function is a process/workflow orchestrator. Usually process/workflow orchestrator doesn't do actual task, cause the objective of a orchestrator is to maintain the stage of a process/workflow. Instead, the orchestrator call a service to complete the task and update the stage.

So the task of removing access should be done by a Lambda function. Since lambda function is not an option, the only applicable option is C, while ECS introduces too much administration overhead, and is a very bad choice for this task.

upvoted 1 times

✉️ **career360guru** 2 years ago

Selected Answer: ADE

A, D and E

upvoted 1 times

✉️ **NikkyDicky** 2 years, 5 months ago

Selected Answer: ADE

ADE. have to assume the step function calls lambda or some such to actually perform action

upvoted 1 times

✉️ **Maria2023** 2 years, 7 months 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 2 times

✉️ **AWSLord32** 1 year, 11 months ago

Here you go <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/configure-sns-notifications-for-cloudtrail.html>

upvoted 1 times

✉️ **OCHT** 2 years, 8 months ago

Selected Answer: ABE

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule. Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.

B. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.

E. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.

upvoted 2 times

✉️ **OCHT** 2 years, 8 months 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** 2 years, 9 months ago

Selected Answer: ADE

ADE is right

upvoted 1 times

✉️ **Musk** 2 years, 10 months ago

Selected Answer: ACE

I like ACE better. I am not sure Step Functions would work.

upvoted 1 times

✉️ **moota** 2 years, 10 months 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** 2 years, 11 months ago

ADE are correct

upvoted 1 times

Question #118

Topic 1

A company wants to migrate to AWS. The company wants to use a multi-account structure with centrally managed access to all accounts and applications. The company also wants to keep the traffic on a private network. Multi-factor authentication (MFA) is required at login, and specific roles are assigned to user groups.

The company must create separate accounts for development, staging, production, and shared network. The production account and the shared network account must have connectivity to all accounts. The development account and the staging account must have access only to each other.

Which combination of steps should a solutions architect take to meet these requirements? (Choose three.)

- A. Deploy a landing zone environment by using AWS Control Tower. Enroll accounts and invite existing accounts into the resulting organization in AWS Organizations.
- B. Enable AWS Security Hub in all accounts to manage cross-account access. Collect findings through AWS CloudTrail to force MFA login.
- C. Create transit gateways and transit gateway VPC attachments in each account. Configure appropriate route tables.
- D. Set up and enable AWS IAM Identity Center (AWS Single Sign-On). Create appropriate permission sets with required MFA for existing accounts.
- E. Enable AWS Control Tower in all accounts to manage routing between accounts. Collect findings through AWS CloudTrail to force MFA login.
- F. Create IAM users and groups. Configure MFA for all users. Set up Amazon Cognito user pools and Identity pools to manage access to accounts and between accounts.

Correct Answer: ACD*Community vote distribution*

ACD (100%)

 **masetromain**  2 years, 11 months ago

Selected Answer: ACD

The correct answer would be options A, C and D, because they address the requirements outlined in the question.

- A. Deploying a landing zone environment using AWS Control Tower and enrolling accounts in an organization in AWS Organizations allows for a centralized management of access to all accounts and applications.
- C. Creating transit gateways and transit gateway VPC attachments in each account and configuring appropriate route tables allows for private network traffic, and ensures that the production account and shared network account have connectivity to all accounts, while the development and staging accounts have access only to each other.
- D. Setting up and enabling AWS IAM Identity Center (AWS Single Sign-On) and creating appropriate permission sets with required MFA for existing accounts allows for multi-factor authentication at login and specific roles to be assigned to user groups.

upvoted 17 times

 **masetromain** 2 years, 11 months ago

The other options are not correct because:

- B. Enabling AWS Security Hub in all accounts to manage cross-account access and collecting findings through AWS CloudTrail to force MFA login is not enough to meet the requirement of creating separate accounts for development, staging, production, and shared network. It can be used in addition to the other steps, but not as a standalone solution.
- E. Enabling AWS Control Tower in all accounts to manage routing between accounts and collecting findings through AWS CloudTrail to force MFA login is not enough to meet the requirement of creating separate accounts for development, staging, production, and shared network. It can be used in addition to the other steps, but not as a standalone solution.

upvoted 4 times

 **masetromain** 2 years, 11 months ago

F. Creating IAM users and groups and configuring MFA for all users and setting up Amazon Cognito user pools and Identity pools to manage access to accounts and between accounts does not address the requirement of creating separate accounts for development, staging, production, and shared network. Additionally, it does not address the requirement of keeping the traffic on a private network.

upvoted 3 times

 **princajen**  4 months, 3 weeks ago

Selected Answer: ACD

A makes sense because AWS Control Tower with Organizations sets up a governed multi-account structure and lets you manage accounts like dev, staging, prod, and shared networking.

C is needed for private connectivity. Transit Gateway + route tables gives you control over which accounts can talk to each other (e.g., dev → staging only, while prod and shared network can talk to all).

D is for centralized access. IAM Identity Center (SSO) allows MFA, group-based role assignments, and access control across all accounts.

B, E, and F don't fit:

B/E mention CloudTrail and Security Hub but those don't enforce MFA.

F mixes IAM users with Cognito, which is for app auth — not ideal for managing access across AWS accounts.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

- A. Deploy a landing zone environment by using AWS Control Tower. Enroll accounts and invite existing accounts into the resulting organization in AWS Organizations.
- 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.

upvoted 1 times

 **ajeeshb** 1 year, 9 months ago

Selected Answer: ACD
A, C and D are right answers. Option C is though not clear. Transit gateway needs to be created in shared network account and tgw vpc attachment in all accounts. But option C says "create tgw and tgw vpc attachment in all accounts", which is a bit confusing

upvoted 2 times

 **8693a49** 1 year, 4 months ago

Yes, you probably only need one TGW in the shared account

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: ACD

A, C and D

upvoted 1 times

 **shaam80** 2 years ago

Selected Answer: ACD

Answer - ACD

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: ACD

ACD easy

upvoted 1 times

 **Maria2023** 2 years, 6 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 2 times

 **OCHT** 2 years, 8 months 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 4 times

 **mfsec** 2 years, 9 months ago

Selected Answer: ACD

ACD are the best choice

upvoted 1 times

 **spd** 2 years, 10 months ago

Selected Answer: ACD

By Elimination Rule

upvoted 3 times

 **zhangyu20000** 2 years, 11 months ago

ACD are correct.

upvoted 3 times

Question #119

Topic 1

A company runs its application in the eu-west-1 Region and has one account for each of its environments: development, testing, and production. All the environments are running 24 hours a day, 7 days a week by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases. The databases are between 500 GB and 800 GB in size.

The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day, 7 days a week. The company wants to reduce costs. All resources are tagged with an environment tag with either development, testing, or production as the key.

What should a solutions architect do to reduce costs with the LEAST operational effort?

- A. Create an Amazon EventBridge rule that runs once every day. Configure the rule to invoke one AWS Lambda function that starts or stops instances based on me tag, day, and time.
- B. Create an Amazon EventBridge rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that stops instances based on the tag. Create a second EventBridge rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that starts instances based on the tag.
- C. Create an Amazon EventBridge rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that terminates instances based on the lag. Create a second EventBridge rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that restores the instances from their last backup based on the tag.
- D. Create an Amazon EventBridge rule that runs every hour. Configure the rule to invoke one AWS Lambda function that terminates or restores instances from their last backup based on the tag, day, and time.

Correct Answer: B*Community vote distribution*

B (100%)

masetromain Highly Voted 2 years, 11 months ago**Selected Answer: B**

The correct answer is B. Creating an Amazon EventBridge rule that runs every business day in the evening to stop instances and another rule that runs every business day in the morning to start instances based on the tag will reduce costs with the least operational effort.

This approach allows for instances to be stopped during non-business hours when they are not in use, reducing the costs associated with running them. It also allows for instances to be started again in the morning when the development and testing teams need to use them.

Option A would require the instances to be stopped and started once a day, which could result in instances being stopped while they are in use or not being stopped when they are not in use.

Option C would terminate instances during non-business hours and restore them again in the morning, which could lead to data loss or longer start up times.

Option D would terminate or restore instances every hour, which could lead to unnecessary costs as well as data loss or longer start up times.

upvoted 11 times

Musk Highly Voted 2 years, 10 months ago**Selected Answer: B**

this is easy. I wish I'll have several of this in the exam.

upvoted 9 times

princjen Most Recent 4 months, 3 weeks ago**Selected Answer: B**

B is the better option because it separates the stop and start logic into two EventBridge rules and two simple Lambda functions. This avoids having complex time-based logic inside a single Lambda (like you'd need in A). Even though A uses fewer components, it increases operational overhead by making the Lambda function more complicated to manage and test.

With B, each function only does one thing (stop or start) based on tags, and it aligns better with AWS best practices for scheduled automation. Lower code complexity = less maintenance in the long run.

upvoted 1 times

nimbus_00 1 year, 2 months ago**Selected Answer: B**

Stopping instances rather than terminating them ensures that the environment's state can be quickly restored the next day without needing to manage backups or restorations, making it operationally efficient.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **AWSLord32** 1 year, 11 months ago

Selected Answer: B

Voted B, but C seems to be more cost effective. Any idea to why it wouldn't work?

upvoted 1 times

 **pangchn** 1 year, 10 months ago

C will terminate the instance which may potentially lose work on the disk

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: B

Option B

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B for sure

upvoted 1 times

 **Maria2023** 2 years, 6 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** 2 years, 7 months ago

Can anyone explain why B has less operational effort than A?

upvoted 1 times

 **chikorita** 2 years, 6 months ago

cuze 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** 2 years, 8 months 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** 2 years, 9 months ago

Selected Answer: B

B is the easy choice

upvoted 2 times

 **zhangyu20000** 2 years, 11 months ago

B is correct. Stop the instance that preserves all data.

C is incorrect because it terminates instances that will lose data

upvoted 5 times

 **rbm2023** 2 years, 7 months ago

with the addition to the fact that to recreate those DBs from scratch would take a long time.

upvoted 2 times

Question #120

A company is building a software-as-a-service (SaaS) solution on AWS. The company has deployed an Amazon API Gateway REST API with AWS Lambda integration in multiple AWS Regions and in the same production account.

The company offers tiered pricing that gives customers the ability to pay for the capacity to make a certain number of API calls per second. The premium tier offers up to 3,000 calls per second, and customers are identified by a unique API key. Several premium tier customers in various Regions report that they receive error responses of 429 Too Many Requests from multiple API methods during peak usage hours. Logs indicate that the Lambda function is never invoked.

What could be the cause of the error messages for these customers?

- A. The Lambda function reached its concurrency limit.
- B. The Lambda function its Region limit for concurrency.
- C. The company reached its API Gateway account limit for calls per second.
- D. The company reached its API Gateway default per-method limit for calls per second.

Correct Answer: C*Community vote distribution*

C (86%) 11%

 **sambb** Highly Voted 2 years, 9 months 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 14 times

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: C

The correct answer is C. The company reached its API Gateway account limit for calls per second. This is because Amazon API Gateway has a default account-level limit of 10,000 requests per second (RPS) and a default per-method limit of 5,000 RPS. If the company's premium tier customers are making more than 10,000 requests per second in total across all API methods and regions, they would be receiving the error message of 429 Too Many Requests. This indicates that the API Gateway account is reaching its capacity limit, and the Lambda function is not being invoked because API Gateway is blocking the requests before they reach the Lambda function.

The other choices are not correct because the Lambda function's concurrency limit and region limit for concurrency would not affect the API Gateway's request rate limit, and the API Gateway's default per-method limit is 5,000 RPS which is less than the premium tier's 3,000 calls per second.

upvoted 7 times

 **Chris_W_1234** 2 months, 2 weeks ago

Where did you get the info about 5000 RPS limit for methods? ChatGPT? Stages and methods have the same 10k limit as at account level.

Also, the 10 RPS limit does not apply at account level across ALL regions, it is per region.

upvoted 1 times

 **masetromain** 2 years, 11 months ago

Option A is incorrect because the error message is not related to the Lambda function reaching its concurrency limit.

Option B is incorrect because the error message is not related to the Lambda function reaching its region limit for concurrency.

Option D is incorrect because the error message is not related to the company reaching its API Gateway default per-method limit for calls per second, but it's related to the account level limit.

upvoted 4 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: C

Even though method-level throttling (Option D) could explain 429s, the key detail here is that 429 errors are happening across multiple API methods and Regions. This points to the API Gateway account-level limit on requests per second, which is shared across all deployed methods and stages in a Region. If total API traffic from premium-tier customers exceeds this account-level RPS limit, API Gateway returns 429s without invoking the Lambda — exactly what the question describes.

upvoted 1 times

 **Paul123456789** 9 months ago

Selected Answer: D

"they receive error responses of 429 Too Many Requests from multiple API methods"

Error are not coming from all API calls but from multiple API methods

D looks correct

upvoted 1 times

 **BennyMao** 9 months, 3 weeks ago

Selected Answer: D

API Gateway enforces a default per-method limit of 1,000 RPS (requests per second).

Since premium customers require up to 3,000 RPS, they would exceed this limit, leading to 429 errors.

upvoted 1 times

 **E90** 11 months ago

Selected Answer: D

Going with D because:

1) 429 "Too Many requests" error is shown

"Check the rate or burst limit for per-client or per-method throttling limits that you set for the API stage for your usage plan. When the rate or burst limit is exceeded, the CloudWatch event logs an exceeded throttle limit."

<https://repost.aws/knowledge-center/api-gateway-429-limit>

2) The premium tier offer only allows up to 3000 calls per second, while API Gateway has a limit of 10k requests per second, per account, per region - this is far below the allocated limit

3) Question also points to "multiple premium tier users in various regions" i.e. this issue is happening for different AWS accounts in different regions - which suggests that it is not related to the account limit

upvoted 1 times

 **Chris_W_1234** 2 months, 2 weeks ago

The scenario didn't mention anything about stage- or method-level rate limiting, except for the customer quota of 3000 RPS.

If multiple premium tier customers in the same region reach their 3000 RPS limit, they'll quickly reach the 10000 RPS account/region limit. The same seems to occur in multiple regions. My answer is C.

upvoted 1 times

 **sintesi_suffisso0** 11 months ago

Actually the account is only one

upvoted 2 times

 **Heman31in** 1 year ago

Selected Answer: D

The most likely cause of the 429 Too Many Requests error messages, despite the Lambda function not being invoked, is D. The company reached its API Gateway default per-method limit for calls per second.

Here's a breakdown of why:

API Gateway Limits: API Gateway imposes rate limits on API methods to prevent abuse and ensure fair resource allocation. These limits can be configured at the account level or the individual method level.

Default Limits: If not explicitly configured, API Gateway applies default limits to methods. These default limits may be insufficient for high-traffic scenarios, especially during peak usage hours.

Lambda Function Invocations: The Lambda function is not invoked because the request is being throttled at the API Gateway level before it reaches the Lambda function.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

C. The company reached its API Gateway account limit for calls per second.

upvoted 1 times

 **8693a49** 1 year, 4 months ago

Selected Answer: B

I'm going to argue the problem is that the source of the errors is Lambda reaching its regional concurrency limit.

By default, Lambda has a regional limit of 1000 concurrent invocations. The premium tier allows 3000 requests/s. Depending on the number of premium customers and the average duration of a call it may be that the concurrency limit is reached or not. We don't know for sure, but it is certainly plausible. If Lambda hits the concurrency limit, it also returns 429. So how do we know where the error is coming from?

The key is in what exactly fails: "multiple API methods during peak usage hours". Notice it is not ALL API calls. If the gateway was rate limiting then we would see blocks of random requests being denied until the rate bucket empties to allow new ones. But if the Lambda concurrency is hit then it means no new execution environments of Lambda are created, but the ones that exist keep processing. So the behaviour is that some functions will continue to operate, while others will start throttling with 429. This behaviour better matches with "multiple API methods" failing.

upvoted 1 times

 **helloworldabc** 1 year, 3 months ago

just C

upvoted 1 times

 **fangdOn** 1 year, 7 months ago

C correct. This is Gateway API response
upvoted 1 times

 **JohnLuo** 1 year, 8 months ago

Selected Answer: C

C is correct.
upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: C

429 is API Gateway API throttle default limit.
upvoted 3 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C of course
upvoted 1 times

 **dev112233xx** 2 years, 8 months ago

Selected Answer: C

C
429 error indicates that API calls per second was exceeded ... it's not a Lambda issue
upvoted 3 times

 **mfsec** 2 years, 9 months ago

Selected Answer: C

Company reached its limit
upvoted 1 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: C

C is the answer
upvoted 1 times

 **zhangyu20000** 2 years, 11 months ago

C is correct answer
upvoted 1 times

Question #121

Topic 1

A financial company is planning to migrate its web application from on premises to AWS. The company uses a third-party security tool to monitor the inbound traffic to the application. The company has used the security tool for the last 15 years, and the tool has no cloud solutions available from its vendor. The company's security team is concerned about how to integrate the security tool with AWS technology.

The company plans to deploy the application migration to AWS on Amazon EC2 instances. The EC2 instances will run in an Auto Scaling group in a dedicated VPC. The company needs to use the security tool to inspect all packets that come in and out of the VPC. This inspection must occur in real time and must not affect the application's performance. A solutions architect must design a target architecture on AWS that is highly available within an AWS Region.

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

- A. Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC
- B. Deploy the web application behind a Network Load Balancer
- C. Deploy an Application Load Balancer in front of the security tool instances
- D. Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool
- E. Provision a transit gateway to facilitate communication between VPCs.

Correct Answer: AD

Community vote distribution

AD (53%)	DE (45%)
----------	----------

 **rbm2023** Highly Voted 2 years, 7 months 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 26 times

 **OCHT** Highly Voted 2 years, 8 months 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 24 times

 **deegadaze1** 2 years, 7 months ago

Correct for GLB--> https://www.youtube.com/watch?v=-j2smz_VCH4

upvoted 2 times

 **43c89f4** 1 year, 8 months ago

DE is correct, the question clearly mention which combination

- GWLB and provision transit gateway is solution

upvoted 4 times

 **Chris_W_1234** 2 months, 2 weeks ago

I wouldn't exactly say the question *clearly* mentions this... but I interpret "dedicated VPC for the application" as, the security tools shall *not* run in the same VPC. Ergo, multiple VPCs are in play, and the TGW makes a lot of sense then.

I vote DE.

upvoted 1 times

 **Chris_W_1234** Most Recent 2 months, 2 weeks ago

Selected Answer: DE

The question mentions "dedicated VPC" for the application, i.e. the security tools will *not* run in the same VPS. Therefore, the use of TGW makes a lot of sense.

upvoted 1 times

 **princajen** 4 months, 3 weeks ago

Selected Answer: DE

The correct answer is DE. The key is that the application is deployed in a dedicated VPC, which implies the security tool is in a separate inspection VPC. To inspect traffic without impacting performance, you use Gateway Load Balancer (D). Since the security and application VPCs are separate, you need a Transit Gateway (E) to route traffic between them. This pattern aligns with AWS's best practice for centralizing security in a scalable, high-availability setup.

Option A falls short because it implies deploying the security tool in the same VPC, which doesn't align with the "dedicated" wording in the question — and breaks isolation.

upvoted 1 times

 **Kaps443** 6 months, 3 weeks ago

Selected Answer: AD

A. Deploy the security tool on EC2 instances

Since the tool is legacy and has no cloud-native support, it must run on EC2 instances.

An Auto Scaling group helps maintain availability and resilience.

Placing the tool in the same VPC allows for easy traffic routing via a Gateway Load Balancer.

D. Provision a Gateway Load Balancer (GWLB) per AZ

Gateway Load Balancer is designed specifically for this use case: deploying virtual appliances (like firewalls, IDS/IPS, and packet inspection tools).

It redirects VPC traffic to your EC2-based security tool instances for inline, transparent inspection, without affecting the app performance.

upvoted 3 times

 **jimee11** 7 months, 3 weeks ago

Selected Answer: AD

Requirements clearly call out the 'web application' vs. 'security tool'. The web application is not going to be deployed behind an NLB. This rules out B. Requirements say you need scalability. Deploy the security tool behind an ALB with auto-scaling (A). Gateway LB is best for deep packet inspections (D).

upvoted 2 times

 **kylix75** 11 months ago

Selected Answer: BD

Correct answers: B and D

Rationale:

B (Network Load Balancer):

- Operates at layer 4
- Minimal latency impact
- Supports transparent network inspection

D (Gateway Load Balancer):

- Purpose-built for third-party security appliances
- Enables inline traffic inspection
- High availability with per-AZ deployment

Other options' issues:

A: Doesn't address traffic routing

C: ALB operates at layer 7, adding unnecessary overhead

E: Transit gateway unnecessary for single VPC setup

upvoted 1 times

 **ahhatem** 1 year ago

Selected Answer: DE

The question explicitly states that it would be deployed in a dedicated VPC. This disqualifies A.

On another hand, dedicated security appliances are usually deployed in a centralized networking setup with central ingress/egress. Check this whitepaper:

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-gwlb-with-tg-for-cns.html>

upvoted 1 times

 **Edd_18** 1 year, 1 month ago

Selected Answer: DE

<https://www.fortinet.com/blog/business-and-technology/highly-scalable-fortigate-next-generation-firewall-security-on-aws-gateway-load-balancer-service>

upvoted 2 times

 **FZA24** 1 year, 2 months ago

Selected Answer: AD

In AD, it mention that will be deployed in the existing VPC. however, in DE, it does not mention that the security tool is deployed in another VPC. It only mention transit gateway between VPCs.

upvoted 3 times

 **AWSum1** 1 year, 2 months ago

Selected Answer: AD

it says it needs to inspect traffic coming in and out of THE VPC not multiple VPC's. This statement disqualifies E

upvoted 4 times

 **amministrazione** 1 year, 3 months ago

- A. Deploy the security tool on EC2 instances m a new Auto Scaling group in the existing VPC
- D. Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool

upvoted 1 times

 **ry1999** 1 year, 3 months ago

Selected Answer: AD

D and E make the most sense if your architecture involves multiple VPCs where traffic needs to be centrally managed and inspected. This combination addresses both the direct need for packet inspection and the broader network management requirements.

A and E could be considered if the application and security tool deployment are straightforward and confined to a single or connected VPCs. However, managing traffic flow effectively to the security tools might require additional configuration that can complicate the setup.

Since there is only once VPC, AD

upvoted 3 times

 **Jason666888** 1 year, 4 months ago

Selected Answer: AD

It has to be AD.

I've taken the Udemy Course from stephane maarek and his course described this kind of scenario

upvoted 5 times

 **seochan** 1 year, 4 months ago

Selected Answer: AD

DE cannot be the answer. The combination doesn't describe how to deploy the security tools on the cloud.

upvoted 2 times

 **michele_scar** 1 year, 6 months ago

Selected Answer: DE

DE is the answer. Transit -> GWLB -> Inspection tool

upvoted 1 times

 **helloworldabc** 1 year, 3 months ago

just AD

upvoted 1 times

 **ce825d4** 1 year, 6 months ago

Selected Answer: AD

AD is correct as the requirement is to use the Security tool to inspect traffic coming in and out of the VPC. So, you need to deploy the security tool on EC2 instances and provision a Gateway loadbalancer to load balance the traffic. With a GLB, you can deploy, manage, and scale virtual appliances, such as intrusion detection and prevention, firewalls, and deep packet inspection systems. It creates a single entry and exit point for all appliance traffic and scales your virtual appliances with demand. You can also exchange traffic across virtual private cloud (VPC) boundaries.

upvoted 2 times

Question #122

A company has purchased appliances from different vendors. The appliances all have IoT sensors. The sensors send status information in the vendors' proprietary formats to a legacy application that parses the information into JSON. The parsing is simple, but each vendor has a unique format. Once daily, the application parses all the JSON records and stores the records in a relational database for analysis.

The company needs to design a new data analysis solution that can deliver faster and optimize costs.

Which solution will meet these requirements?

- A. Connect the IoT sensors to AWS IoT Core. Set a rule to invoke an AWS Lambda function to parse the information and save a .csv file to Amazon S3. Use AWS Glue to catalog the files. Use Amazon Athena and Amazon QuickSight for analysis.
- B. Migrate the application server to AWS Fargate, which will receive the information from IoT sensors and parse the information into a relational format. Save the parsed information to Amazon Redshift for analysis.
- C. Create an AWS Transfer for SFTP server. Update the IoT sensor code to send the information as a .csv file through SFTP to the server. Use AWS Glue to catalog the files. Use Amazon Athena for analysis.
- D. Use AWS Snowball Edge to collect data from the IoT sensors directly to perform local analysis. Periodically collect the data into Amazon Redshift to perform global analysis.

Correct Answer: A

Community vote distribution

A (83%)

B (17%)

 **God_Is_Love** Highly Voted 2 years, 9 months 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 12 times

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: A

A. Connect the IoT sensors to AWS IoT Core. Set a rule to invoke an AWS Lambda function to parse the information and save a .csv file to Amazon S3. Use AWS Glue to catalog the files. Use Amazon Athena and Amazon QuickSight for analysis.

This solution meets the requirement of faster analysis and cost optimization by using AWS IoT Core to collect data from the IoT sensors in real-time and then using AWS Glue and Amazon Athena for efficient data analysis.

Option B and D do not optimize the cost of data analysis as they involve use of expensive services like AWS Fargate and Snowball Edge respectively. Option C does not make use of real-time data collection and may not be optimal for faster analysis.

upvoted 5 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: A

Answer is A — this is the most efficient and scalable solution.

Why?

AWS IoT Core connects IoT sensors securely and in real-time.

An IoT Rule sends data to a Lambda function to parse vendor-specific formats.

Parsed data is saved in S3, cataloged by Glue, queried with Athena, and visualized in QuickSight.

It's serverless, real-time, and cost-effective, unlike the batch-processing legacy system.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: A

A, IoT Core

upvoted 1 times

✉ career360guru 2 years ago

Selected Answer: A

Option A is best(fastest) and most cost effective.

upvoted 1 times

✉ GaryQian 2 years ago

Selected Answer: A

Everytime the exam shows IOT sensor, think of IOT Core and aws glue

upvoted 1 times

✉ KCjoe 2 years, 2 months ago

Selected Answer: B

How can A satisfy this requirement? "relational database for analysis"

The only option is B with relational database for analysis.

upvoted 4 times

✉ heatblur 2 years, 1 month ago

"The company needs to design a new data analysis solution that can deliver faster and optimize costs."

upvoted 2 times

✉ helloworldabc 1 year, 3 months ago

just A

upvoted 1 times

✉ uC6rW1aB 2 years, 3 months ago

Selected Answer: A

Option A: AWS IoT Core + Lambda

Speed: Near real-time data collection and analysis.

Flexibility: Ability to adapt to different data formats from multiple vendors.

Option C: AWS Transfer for SFTP

Speed: There may be network delays and waiting for all data to be sent.

Development needs: The sensor code needs to be updated, which increases the development workload.

All things considered, option A is better than option C in terms of speed and flexibility, and is especially suitable for real-time or near-real-time requirements.

upvoted 1 times

✉ NikkyDicky 2 years, 5 months ago

Selected Answer: A

A for sure

upvoted 1 times

✉ Maria2023 2 years, 7 months 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 2 years, 8 months 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 2 years, 9 months ago

Selected Answer: A

Connect the IoT sensors to AWS IoT Core.

upvoted 2 times

✉ spd 2 years, 10 months ago

Selected Answer: A

A by Elimination rule

upvoted 4 times

✉ Musk 2 years, 10 months ago

Selected Answer: B

I m not convinced about A. It kind of requires changes in the sensors to be compatible with AWS IoT Core.

upvoted 4 times

✉ Sarutobi 2 years, 8 months 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** 2 years, 11 months ago

Selected Answer: A

i'll go for A

upvoted 4 times

 **zhangyu20000** 2 years, 11 months ago

A is correct.

B: it is appliance, impossible to install on Fargate

C: device not use FTP protocol

D: snowball is not real time

upvoted 4 times

 **Musk** 2 years, 10 months ago

In B, we don't try to port appliances to Fargate, but only the app that parses the information from the appliances into JSON. I am doubting about A. Unless you would reprogram the sensors they would not know how to connect to AWS IoT Core.

upvoted 1 times

Question #123

Topic 1

A company is migrating some of its applications to AWS. The company wants to migrate and modernize the applications quickly after it finalizes networking and security strategies. The company has set up an AWS Direct Connect connection in a central network account.

The company expects to have hundreds of AWS accounts and VPCs in the near future. The corporate network must be able to access the resources on AWS seamlessly and also must be able to communicate with all the VPCs. The company also wants to route its cloud resources to the internet through its on-premises data center.

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

- A. Create a Direct Connect gateway in the central account. In each of the accounts, create an association proposal by using the Direct Connect gateway and the account ID for every virtual private gateway.
- B. Create a Direct Connect gateway and a transit gateway in the central network account. Attach the transit gateway to the Direct Connect gateway by using a transit VIF.
- C. Provision an internet gateway. Attach the internet gateway to subnets. Allow internet traffic through the gateway.
- D. Share the transit gateway with other accounts. Attach VPCs to the transit gateway.
- E. Provision VPC peering as necessary.
- F. Provision only private subnets. Open the necessary route on the transit gateway and customer gateway to allow outbound internet traffic from AWS to flow through NAT services that run in the data center.

Correct Answer: BDF

Community vote distribution

BDF (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: BDF

B and D and F are correct.

B: Creating a Direct Connect gateway and a transit gateway in the central network account will allow the company to connect its on-premises data center to the resources in AWS.

D: Sharing the transit gateway with other accounts will allow the company to communicate with all the VPCs in multiple accounts.

F: Provisioning only private subnets and opening necessary routes on the transit gateway and customer gateway will allow the company to route its cloud resources to the internet through its on-premises data center.

A is incorrect because it would be redundant to use both a Direct Connect gateway and a transit gateway.

C is incorrect because it is not necessary to provision an internet gateway, since the company wants to route traffic through their on-premises data center.

E is incorrect because VPC peering may not be necessary if the company is using a transit gateway to connect all the VPCs.

upvoted 13 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: BDF

The correct answers are B, D, and F.

B sets up scalable on-prem to AWS connectivity using a Direct Connect Gateway and a Transit Gateway.

D allows you to share the TGW across accounts and attach VPCs easily.

F ensures outbound internet traffic goes through the on-premises NAT, as required.

Avoid options like A (too manual), C (introduces IGW), or E (non-transitive, doesn't scale).

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

D. Share the transit gateway with other accounts. Attach VPCs to the transit gateway.

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.

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: BDF

BDF is most scalable solution.

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: BDF

Answer BDF
DGW and TGW
Share TGW and configure VPC attachments to TGW
Open necessary routes for traffic routing via NAT gw on the on-prem dc
upvoted 1 times

 **SK_Tyagi** 2 years, 4 months ago

Selected Answer: BDF

Very logical
upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: BDF

BDF for sure
upvoted 1 times

 **Maria2023** 2 years, 6 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 3 times

 **SkyZeroZx** 2 years, 7 months ago

Selected Answer: BDF

BDF is the right ans
upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: BDF

BDF is the right combo
upvoted 1 times

 **God_Is_Love** 2 years, 9 months 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** 2 years, 11 months ago

Selected Answer: BDF

B D and F
upvoted 4 times

 **zozza2023** 2 years, 11 months ago

I agree with BD&F
upvoted 3 times

 **zhangyu20000** 2 years, 11 months ago

BDF are correct
upvoted 2 times

Question #124

A company has hundreds of AWS accounts. The company recently implemented a centralized internal process for purchasing new Reserved Instances and modifying existing Reserved Instances. This process requires all business units that want to purchase or modify Reserved Instances to submit requests to a dedicated team for procurement. Previously, business units directly purchased or modified Reserved Instances in their own respective AWS accounts autonomously.

A solutions architect needs to enforce the new process in the most secure way possible.

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

- A. Ensure that all AWS accounts are part of an organization in AWS Organizations with all features enabled.
- B. Use AWS Config to report on the attachment of an IAM policy that denies access to the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- C. In each AWS account, create an IAM policy that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- D. Create an SCP that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action. Attach the SCP to each OU of the organization.
- E. Ensure that all AWS accounts are part of an organization in AWS Organizations that uses the consolidated billing feature.

Correct Answer: AD

Community vote distribution

AD (100%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: AD

A and D are the correct answer.

A: By ensuring all AWS accounts are part of an organization in AWS Organizations, it allows for centralized management and control of the accounts. This can help enforce the new purchasing process by giving a dedicated team the ability to manage and enforce policies across all accounts.

D: By creating an SCP (Service Control Policy) that denies access to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions, it enforces the new centralized purchasing process. Attaching the SCP to each OU (organizational unit) within the organization ensures that all business units are adhering to the new process.

B and C are not the correct answer, because AWS Config and IAM policies are used for monitoring and managing access to resources in an account, respectively. They don't enforce the new process for purchasing reserved instances.

E is not the correct answer as this is not related to the new process for purchasing reserved instances.

upvoted 9 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: AD

Correct answers are A and D.

A ensures all accounts are in an org with SCP support.

D applies a Service Control Policy to prevent business units from purchasing or modifying Reserved Instances, enforcing the centralized process securely.

IAM policies (C) are not scalable, and Config (B) is for monitoring, not enforcement.

E doesn't help unless all features are enabled.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

A. Ensure that all AWS accounts are part of an organization in AWS Organizations with all features enabled.

D. Create an SCP that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action. Attach the SCP to each OU of the organization.

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: AD

A and D

upvoted 1 times

 **atirado** 2 years ago

A+D achieve the goal of denying access to purchase and to modify Reserved Instances to all OUs. The dedicated team can still perform these actions if they are part of the management account.

C, E don't actually do anything, as in, actually control anything at all. B will trigger on the wrong thing to be alarmed about, if triggering an alarm was the goal.

upvoted 1 times

 **dkcloudguru** 2 years, 3 months ago

A and D : is the best way

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: AD

AD. A so can use SCP

upvoted 1 times

 **Maria2023** 2 years, 7 months ago

Selected Answer: AD

I was not confident about enabling all features because I was messing "features" and "services". Yes - you need to enable all features, otherwise you cannot control the accounts in your organization. The rest is common sense

upvoted 3 times

 **mfsec** 2 years, 9 months ago

Selected Answer: AD

AD easy

upvoted 3 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: AD

A and D

upvoted 4 times

 **zhangyu20000** 2 years, 11 months ago

AD are correct

upvoted 2 times

Question #125

Topic 1

A company is running a critical application that uses an Amazon RDS for MySQL database to store data. The RDS DB instance is deployed in Multi-AZ mode.

A recent RDS database failover test caused a 40-second outage to the application. A solutions architect needs to design a solution to reduce the outage time to less than 20 seconds.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Use Amazon ElastiCache for Memcached in front of the database
- B. Use Amazon ElastiCache for Redis in front of the database
- C. Use RDS Proxy in front of the database.
- D. Migrate the database to Amazon Aurora MySQL.
- E. Create an Amazon Aurora Replica.
- F. Create an RDS for MySQL read replica

Correct Answer: CDE

Community vote distribution

CDE (91%) 9%

 **RaghavendraPrakash** Highly Voted 2 years, 7 months 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 13 times

 **dev112233xx** Highly Voted 2 years, 8 months 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 11 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: CDE

To reduce RDS failover time to under 20 seconds, combining Amazon Aurora MySQL with Aurora Replicas and RDS Proxy is the most effective solution.

Aurora (D) supports faster, automatic failover than RDS MySQL.

Aurora Replicas (E) act as pre-provisioned failover targets, minimizing downtime.

RDS Proxy (C) handles persistent DB connections, auto-retries, and insulates the application from the failover event.

This trio reduces both failover execution time and application recovery time, ensuring high availability with minimal interruption.

upvoted 1 times

 **zak543** 11 months ago

Selected Answer: CDE

for multiple chose answer, if i select 2of3 right, in this case the whole quest will be wrong or what?

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

C. Use RDS Proxy in front of the database.

D. Migrate the database to Amazon Aurora MySQL.

E. Create an Amazon Aurora Replica.

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: CDE

A and B don't contribute to reducing response time in failover scenarios.

D is required for faster failover.

E is required to support D.

F doesn't reduce failover time.

C, finally, is the remaining option. It doesn't hurt, and can contribute to faster failover, though it is not the most important factor here - the switch to Aurora with an Aurora read replica is.

upvoted 2 times

 **bjexamprep** 1 year, 9 months ago

Anyone can share why choosing E? I know we have to choose 3. isn't it weird? Aurora already has replicas natively. Why creating another one?

upvoted 2 times

 **career360guru** 2 years ago

Selected Answer: CDE

Option C, D and E

upvoted 1 times

 **atirado** 2 years ago

Selected Answer: CDE

C+D+E provides the 'fastest' failover with the options available:

- Aurora MySQL is Multi-AZ by design: During failover it will promote a Replica to primary or create a Primary instance
- Creating a Replica provides the option to have something to failover to
- Using an RDS Proxy further reduces failover time and provides 'transparent' failovers as well (It manages DNS changes)

The argument against Caching (options A or B) is that it doesn't accelerate failing over to a different instance. Cache misses and write operations will produce exceptions because there is no instance to query. Moreover, there is no information in the question to choose between either caching option, i.e. Both options can be created starting from an Aurora DB Cluster settings - <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/creating-elasticache-cluster-with-RDS-settings.html>

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: CDE

CDE, agree with other comments

upvoted 2 times

 **Sarutobi** 2 years, 8 months ago

Selected Answer: CDE

The trick seems to be that the RDS proxy handles DNS updates quickly. While if you don't use it, you are at the mercy of the host to update its DNS cache.

upvoted 3 times

 **mfsec** 2 years, 9 months ago

Selected Answer: CDE

CDE is the best choice

upvoted 1 times

 **DWsk** 2 years, 9 months 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** 2 years, 8 months ago

I agree with your logic.

upvoted 1 times

 **God_Is_Love** 2 years, 9 months 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** 2 years, 11 months ago

Selected Answer: CDE

C D and E

upvoted 2 times

 **nyxs_19** 2 years, 10 months 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 2 times

 **AjayD123** 2 years, 11 months ago

Selected Answer: CDE

RDS read replica auto failover takes approx 35 seconds hence, BCF does not satisfy under 20 seconds failover requirement.

<https://aws.amazon.com/rds/features/multi-az/#:~:text=Amazon%20RDS%20Multi%2DAZ%20with%20two%20readable%20standbys,-Automatically%20fail%20over&text=Automatically%20failover%20in%20typically%20under, and%20with%20no%20manual%20intervention.>

upvoted 5 times

✉ **zozza2023** 2 years, 11 months ago

thanks for the information about RDS read replica

upvoted 2 times

✉ **masetromain** 2 years, 11 months ago

Selected Answer: CDE

The correct answer is D, E and C:

Migrate the database to Amazon Aurora MySQL.

- Create an Amazon Aurora Replica.
- Use RDS Proxy in front of the database.
- These options are correct because they address the requirement of reducing the failover time to less than 20 seconds.

Migrating to Amazon Aurora MySQL and creating an Aurora replica can reduce the failover time to less than 20 seconds. Aurora has a built-in, fault-tolerant storage system that can automatically detect and repair failures. Additionally, Aurora has a feature called "Aurora Global Database" which allows you to create read-only replicas across multiple AWS regions which can further help to reduce the failover time.

Creating an Aurora replica can also help to reduce the failover time as it can take over as the primary DB instance in case of a failure.

Using RDS proxy can also help to reduce the failover time as it can route the queries to the healthy DB instance, it also helps to balance the load across multiple DB instances.

upvoted 4 times

✉ **masetromain** 2 years, 11 months ago

Option A and B, Use Amazon ElastiCache for Memcached and Redis in front of the database, are not correct as ElastiCache is a caching service, it doesn't provide a high availability solution for the underlying database.

Option F, Create an RDS for MySQL read replica, is not correct as a read replica can only be used to offload read traffic from the primary instance, it doesn't provide a high availability solution for the underlying database.

upvoted 1 times

Question #126

Topic 1

An AWS partner company is building a service in AWS Organizations using its organization named org1. This service requires the partner company to have access to AWS resources in a customer account, which is in a separate organization named org2. The company must establish least privilege security access using an API or command line tool to the customer account.

What is the MOST secure way to allow org1 to access resources in org2?

- A. The customer should provide the partner company with their AWS account access keys to log in and perform the required tasks.
- B. The customer should create an IAM user and assign the required permissions to the IAM user. The customer should then provide the credentials to the partner company to log in and perform the required tasks.
- C. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN) when requesting access to perform the required tasks.
- D. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN), including the external ID in the IAM role's trust policy, when requesting access to perform the required tasks.

Correct Answer: D

Community vote distribution

D (100%)

 **dev112233xx** Highly Voted  2 years, 8 months ago

Selected Answer: D

D

Well.. "external ID" is the keyword that you should look for in such scenario.

upvoted 6 times

 **princajen** Most Recent  4 months, 3 weeks ago

Selected Answer: D

The most secure way for a partner company in a different AWS Organization to access a customer's resources is for the customer to create an IAM role with least-privilege permissions and include an external ID in the trust policy. The partner company can then assume the role using the ARN and external ID via the AWS STS API.

This approach prevents confused deputy attacks and aligns with AWS best practices for cross-account access between third-party services and customer accounts.

upvoted 1 times

 **d401c0d** 11 months ago

Selected Answer: D

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.

A - that is just hilarious and should not be the case.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: D

Option D is most secure.

upvoted 1 times

 **atirado** 2 years ago

Selected Answer: D

Sharing credentials will always be a bad idea. In comparison to C and D, options A and B are insecure.

The reason D is the most secure option compared to C is because it addresses the confused deputy problem -
<https://docs.aws.amazon.com/IAM/latest/UserGuide/confused-deputy.html>

upvoted 3 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: D
it's D, but private link would be a better choice
upvoted 3 times

 **mfsec** 2 years, 9 months ago

Selected Answer: D
With the external ID.
upvoted 2 times

 **God_Is_Love** 2 years, 9 months ago

Selected Answer: D
{
"Version": "2012-10-17",
"Statement": {
"Effect": "Allow",
"Principal": {
"AWS": "Example Corp's AWS Account ID"
},
"Action": "sts:AssumeRole",
"Condition": {
"StringEquals": {
"sts:ExternalId": "1122334455-The ID that only Third party and customer knows"
}
}
}
}
}
}
upvoted 3 times

 **Musk** 2 years, 10 months ago

Selected Answer: D
Easy. The external ID is for sure the winner.
upvoted 1 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: D
D seems the correct answer
upvoted 2 times

 **Untamables** 2 years, 11 months ago

Selected Answer: D
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html
upvoted 2 times

 **masetromain** 2 years, 11 months ago

Selected Answer: D
The correct answer is D. This is the most secure way to allow org1 to access resources in org2 because it allows for least privilege security access. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN) and include the external ID in the IAM role's trust policy when requesting access to perform the required tasks. This ensures that the partner company can only access the resources that it needs and only from the specific customer account.

Option A and B both involve providing the partner company with credentials, which can be easily compromised and could lead to a security breach. Option C also provides the partner company with an IAM role, but it doesn't have any restrictions on when and where the partner company can access the resources in customer account, it could be a security risk.

upvoted 3 times

 **zhangyu20000** 2 years, 11 months ago

D is correct
upvoted 1 times

Question #127

A delivery company needs to migrate its third-party route planning application to AWS. The third party supplies a supported Docker image from a public registry. The image can run in as many containers as required to generate the route map.

The company has divided the delivery area into sections with supply hubs so that delivery drivers travel the shortest distance possible from the hubs to the customers. To reduce the time necessary to generate route maps, each section uses its own set of Docker containers with a custom configuration that processes orders only in the section's area.

The company needs the ability to allocate resources cost-effectively based on the number of running containers.

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

- A. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on Amazon EC2. Use the Amazon EKS CLI to launch the planning application in pods by using the --tags option to assign a custom tag to the pod.
- B. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on AWS Fargate. Use the Amazon EKS CLI to launch the planning application. Use the AWS CLI tag-resource API call to assign a custom tag to the pod.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster on Amazon EC2. Use the AWS CLI with run-tasks set to true to launch the planning application by using the --tags option to assign a custom tag to the task.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster on AWS Fargate. Use the AWS CLI run-task command and set enableECSManagedTags to true to launch the planning application. Use the --tags option to assign a custom tag to the task.

Correct Answer: D

Community vote distribution

D (83%)

B (17%)

 **dev112233xx**  2 years, 8 months 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 16 times

 **Jay_2pt0_1** 2 years, 1 month ago

Stepped through that same thought process

upvoted 1 times

 **God_Is_Love**  2 years, 9 months 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 6 times

 **princajen**  4 months, 3 weeks ago

Selected Answer: D

ECS on Fargate is the best fit here because the company wants cost-effective scaling based on the number of containers and least operational overhead. Fargate removes the need to manage EC2 infrastructure, and ECS is easier to work with than EKS unless you're running a complex Kubernetes-based microservices platform.

Also, tagging is natively supported in ECS Fargate tasks using the --tags option along with --enable-ecs-managed-tags, which is perfect for cost allocation per delivery section. In contrast, tagging pods directly in EKS via CLI is not straightforward, and managing Kubernetes adds unnecessary complexity for this use case.

upvoted 1 times

 **0dc6cac** 6 months, 2 weeks ago

Selected Answer: D

it's D, people who pick B have never worked with EKS in a prod environment :-/

upvoted 1 times

 **altonh** 11 months, 2 weeks ago

Selected Answer: D

For option B, how do you tag a POD using AWS CLI?

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: D

A and B = between EKS and ECS if K8s is not required I go for ECS

C = between EC2 and Fargate if nothing points you clearly to Ec2 i would go for Fargate (less overhead, could cost less)

D = correct

upvoted 3 times

 **ele** 1 year, 11 months ago

Selected Answer: B

D is a trap, even if it's tempting, but '--tags' is not a valid option for tagging ecs tasks/services.

B is the right answer.

upvoted 1 times

 **cox1960** 1 year, 11 months ago

--tags is valid

<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ecs/run-task.html>

upvoted 1 times

 **cox1960** 1 year, 11 months ago

but --enable-ecs-managed-tags is the right option instead of "enableECSManagedTags` to `true`"

upvoted 1 times

 **helloworldabc** 1 year, 3 months ago

just D

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: D

D is best option with least operational overhead.

upvoted 3 times

 **atirado** 2 years ago

Selected Answer: D

Options A and C are more operationally complex than B and D because you will need to manage the EC2 instances and underpin the EKS cluster and the ECS service definition. And as if to make the selection easier, B and D explicitly mention using AWS Fargate in a way that works.

Selecting between Options B and D boils down the interpretation of "each section uses its own set of Docker containers with a custom configuration that processes orders only in the section's area". The only indication in the question that kind of helps is "The third party supplies a supported Docker image from a public registry": The custom configuration is just for processing orders in the section's area rather something in the docker image itself.

upvoted 2 times

 **n_d1** 2 years, 3 months 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 3 times

 **Ganshank** 2 years, 4 months ago

Real-world answer - B.

Certification answer - D.

upvoted 5 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: D

going with D

upvoted 2 times

 **rbm2023** 2 years, 7 months 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 4 times

 **iamunstopable** 2 years, 8 months ago

B is correct

Anytime you need Docker containers with a custom configuration use EKS

upvoted 2 times

 **Jay_2pt0_1** 2 years, 8 months 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 3 times

 **mfsec** 2 years, 9 months ago

Selected Answer: D

D is easier

upvoted 2 times

Question #128

A software company hosts an application on AWS with resources in multiple AWS accounts and Regions. The application runs on a group of Amazon EC2 instances in an application VPC located in the us-east-1 Region with an IPv4 CIDR block of 10.10.0.0/16. In a different AWS account, a shared services VPC is located in the us-east-2 Region with an IPv4 CIDR block of 10.10.10.0/24. When a cloud engineer uses AWS CloudFormation to attempt to peer the application VPC with the shared services VPC, an error message indicates a peering failure.

Which factors could cause this error? (Choose two.)

- A. The IPv4 CIDR ranges of the two VPCs overlap
- B. The VPCs are not in the same Region
- C. One or both accounts do not have access to an Internet gateway
- D. One of the VPCs was not shared through AWS Resource Access Manager
- E. The IAM role in the peer accepter account does not have the correct permissions

Correct Answer: AE*Community vote distribution*

AE (81%)

Other

 **Appon** Highly Voted 2 years, 10 months ago

Selected Answer: AE

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudformation-vpc-peering-error/>
upvoted 10 times

 **zhangyu20000** Highly Voted 2 years, 11 months ago

AE is correct
D is not correct because you cannot share VPC via RAM, subnet can
upvoted 5 times

 **djeong95** 1 year, 9 months ago

In this link, you can find VPC sharing being described as "In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organization". You can share subnets using AWS RAM. I think it is safe to conclude you can share VPCs using RAM.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-sharing.html#vpc-share-prerequisites>
upvoted 1 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: AE

VPC peering will fail if the CIDR ranges of the two VPCs overlap, even partially — as in this case, where 10.10.10.0/24 is within 10.10.0.0/16. Also, for cross-account peering via CloudFormation, the accepter account needs the correct IAM permissions to accept the peering request, or the operation will be denied. Region differences are supported, and VPCs do not need to be shared via RAM for peering to work.

upvoted 2 times

 **Syre** 1 year, 2 months ago

Selected Answer: AB

E is wrong
upvoted 3 times

 **amministrazione** 1 year, 3 months ago

A. The IPv4 CIDR ranges of the two VPCs overlap
E. The IAM role in the peer accepter account does not have the correct permissions
upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: AE

Option A and E
upvoted 1 times

 **m1xa** 2 years, 1 month ago

Selected Answer: AE

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
<https://repost.aws/knowledge-center/cloudformation-vpc-peering-error>
upvoted 1 times

⊕  **SK_Tyagi** 2 years, 4 months ago

Selected Answer: AE

This is correct, per Appon's link

upvoted 1 times

⊕  **NikkyDicky** 2 years, 5 months ago

Selected Answer: AE

AE for sure

upvoted 1 times

⊕  **ThaiNT** 2 years, 7 months ago

Selected Answer: BE

VPCs are not in the same Region.

upvoted 3 times

⊕  **ThaiNT** 2 years, 7 months ago

My bad, option B is incorrect.

upvoted 2 times

⊕  **mfsec** 2 years, 9 months ago

Selected Answer: AE

AE is the best choice

upvoted 2 times

⊕  **God_Is_Love** 2 years, 9 months 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 4 times

⊕  **zozza2023** 2 years, 11 months ago

Selected Answer: AE

A and E

upvoted 1 times

⊕  **masetromain** 2 years, 11 months ago

Selected Answer: AE

A is correct because the IPv4 CIDR ranges of the two VPCs overlap. The two VPCs have an IP range of 10.10.0.0/16 and 10.10.10.0/24, which means that they share the same 10.10.0.0 network. This causes a conflict in routing and will prevent the VPCs from being able to communicate with each other.

E is correct because the IAM role in the peer accepter account does not have the correct permissions. The role must have permissions to create, modify, and delete VPC peering connections in order for the peering to be established.

B, C, and D are not correct. The VPCs are in the same region, both accounts have access to an internet gateway and both VPCs are not shared through AWS Resource Access Manager.

upvoted 3 times

⊕  **clownfishman** 2 years, 6 months ago

us-east-1 is in virginia, us-east-2 is in ohio - they are separate regions

upvoted 5 times

⊕  **Arnaud92** 2 years, 3 months ago

stop asking to ChatGPT

upvoted 7 times

⊕  **m1xa** 2 years, 1 month ago

It doesn't matter if both accounts are in the same region or not.

>>> The VPCs can be in different Regions (also known as an inter-Region VPC peering connection).

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

upvoted 1 times

Question #129

Topic 1

An external audit of a company's serverless application reveals IAM policies that grant too many permissions. These policies are attached to the company's AWS Lambda execution roles. Hundreds of the company's Lambda functions have broad access permissions such as full access to Amazon S3 buckets and Amazon DynamoDB tables. The company wants each function to have only the minimum permissions that the function needs to complete its task.

A solutions architect must determine which permissions each Lambda function needs.

What should the solutions architect do to meet this requirement with the LEAST amount of effort?

- A. Set up Amazon CodeGuru to profile the Lambda functions and search for AWS API calls. Create an inventory of the required API calls and resources for each Lambda function. Create new IAM access policies for each Lambda function. Review the new policies to ensure that they meet the company's business requirements.
- B. Turn on AWS CloudTrail logging for the AWS account. Use AWS Identity and Access Management Access Analyzer to generate IAM access policies based on the activity recorded in the CloudTrail log. Review the generated policies to ensure that they meet the company's business requirements.
- C. Turn on AWS CloudTrail logging for the AWS account. Create a script to parse the CloudTrail log, search for AWS API calls by Lambda execution role, and create a summary report. Review the report. Create IAM access policies that provide more restrictive permissions for each Lambda function.
- D. Turn on AWS CloudTrail logging for the AWS account. Export the CloudTrail logs to Amazon S3. Use Amazon EMR to process the CloudTrail logs in Amazon S3 and produce a report of API calls and resources used by each execution role. Create a new IAM access policy for each role. Export the generated roles to an S3 bucket. Review the generated policies to ensure that they meet the company's business requirements.

Correct Answer: B

Community vote distribution

B (100%)

 **God_Is_Love** Highly Voted  2 years, 9 months 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 14 times

 **God_Is_Love** 2 years, 9 months 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 7 times

 **princajen** Most Recent  4 months, 3 weeks ago

Selected Answer: B

The best approach is to use IAM Access Analyzer with CloudTrail logging enabled. IAM Access Analyzer can automatically generate IAM policies based on actual API activity recorded in CloudTrail. This provides least-privilege IAM policies with minimal effort and is specifically designed for this use case. Other options require manual scripting or overcomplicated processing like EMR, making them less efficient.

upvoted 1 times

 **amministrazione** 1 year, 3 months ago

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.

upvoted 1 times

 **cox1960** 1 year, 11 months ago

poor since B only works when functions are actually triggered and all the branches of the code are covered.

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: B

Option B is obvious choice

upvoted 1 times

 **atirado** 2 years ago

Selected Answer: B

When approaching questions related to access permissions, it will always help to determine who is accessing what, in this case, it is Lambda functions accessing AWS services (S3 buckets and DynamoDB table).

The choice between A,B and C,D is then based on knowing that Code Guru and Access Analyzer used an automated process to detect issues in code and to compare actual access versus permissions - least effort than C & D.

That last bit is where the kicker is. The question refers to IAM execution roles with too-broad AWS IAM permissions to access AWS services and resources: You are looking for the option that tightens IAM policies rather than in AWS Lambda Function code.

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B - basic access analyzer use case

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: B

keyword == Access Management Access Analyzer to generate IAM

upvoted 1 times

 **Alabi** 2 years, 6 months ago

Selected Answer: B

B definitely

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: B

B - Identity and Access Management Access Analyzer

upvoted 1 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: B

Identity and Access Management Access Analyzer

upvoted 1 times

 **masetromain** 2 years, 11 months ago

Selected Answer: B

The correct answer is B. Turn on AWS CloudTrail logging for the AWS account, and use AWS Identity and Access Management Access Analyzer to generate IAM access policies based on the activity recorded in the CloudTrail log. Review the generated policies to ensure that they meet the company's business requirements.

This is the least amount of effort as it makes use of AWS services that can automatically analyze the CloudTrail logs, generate the IAM policies, and provide a report for the review process.

Option A and D both involve additional steps such as running scripts or using Amazon EMR, which would take more effort to set up and maintain.

Option C is similar to option A and D but doesn't use any AWS services to help with the process.

upvoted 3 times

 **zhangyu20000** 2 years, 11 months ago

B is correct

upvoted 1 times

Question #130

Topic 1

A solutions architect must analyze a company's Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to determine whether the company is using resources efficiently. The company is running several large, high-memory EC2 instances to host database clusters that are deployed in active/passive configurations. The utilization of these EC2 instances varies by the applications that use the databases, and the company has not identified a pattern.

The solutions architect must analyze the environment and take action based on the findings.

Which solution meets these requirements MOST cost-effectively?

- A. Create a dashboard by using AWS Systems Manager OpsCenter. Configure visualizations for Amazon CloudWatch metrics that are associated with the EC2 instances and their EBS volumes. Review the dashboard periodically, and identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- B. Turn on Amazon CloudWatch detailed monitoring for the EC2 instances and their EBS volumes. Create and review a dashboard that is based on the metrics. Identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- C. Install the Amazon CloudWatch agent on each of the EC2 instances. Turn on AWS Compute Optimizer, and let it run for at least 12 hours. Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed.
- D. Sign up for the AWS Enterprise Support plan. Turn on AWS Trusted Advisor. Wait 12 hours. Review the recommendations from Trusted Advisor, and rightsize the EC2 instances as directed.

Correct Answer: C

Community vote distribution

C (97%)

✉️  **God_Is_Love**  2 years, 9 months 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 17 times

✉️  **God_Is_Love** 2 years, 9 months ago

fyi Pricing looks cheap too - <https://aws.amazon.com/compute-optimizer/pricing/>

upvoted 2 times

✉️  **God_Is_Love** 2 years, 9 months 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 4 times

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

Selected Answer: C

The best solution is to install the CloudWatch agent and enable AWS Compute Optimizer, which uses machine learning to analyze EC2 and EBS usage patterns and provides automated rightsizing recommendations. This is more cost-effective and less manual than building dashboards or purchasing Enterprise Support for Trusted Advisor. It allows you to optimize resource allocation even without a clear usage pattern.

upvoted 1 times

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

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.

upvoted 1 times

✉️  **saggy4** 1 year, 10 months ago

Selected Answer: C

A - Not possible
D - Costliest Option possible
now between B and C

The question mentions high-memory EC2 instances.
You cannot get memory metrics without the Cloudwatch agent installed hence C.

upvoted 2 times

career360guru 2 years ago

Selected Answer: C
Option C is most cost effective choice.
upvoted 1 times

wmp7039 2 years ago

C is incorrect : When you first opt in Compute Optimizer, it may take up to 24 hours to fully analyze the AWS resources in your account.
<https://aws.amazon.com/compute-optimizer/faqs/>
upvoted 1 times

carpa_jo 1 year, 12 months ago

You are correct that in the FAQ you've linked it says 24 hours, but in other places of the AWS documentation it says 12 hours, like here:
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-getting-recommendations.html#viewing-recommendations>
or here: <https://docs.aws.amazon.com/awssupport/latest/user/compute-optimizer-with-trusted-advisor.html>
Seems like even AWS doesn't know :D So I would still go with C.

upvoted 1 times

atirado 2 years ago

Selected Answer: C
Option A is not in the running because it will require incurring further expense to address the cost issue.

Option D is expensive - the Enterprise Support plan charges a minimum flat fee minimum or a % of your AWS bill. This could be a large amount for the company's hundreds of instances.

Option B is expensive - Detailed monitoring scales based on the number of metrics and the number of resources. The company has hundreds of instances so this option could potentially be more expensive than D.

Option C - Compute Optimizer will provide improvement suggestions based on 14 prior days usage data from the moment it was enabled. Moreover, the default service option is free. Nothing is said about the custom metrics being used for the CloudWatch agent but it could be the most expensive of all options if mis-used. So either cost 0 or incredibly large if used carelessly.

upvoted 1 times

NikkyDicky 2 years, 5 months ago

Selected Answer: C
C. need CW agent for RAM util
upvoted 1 times

Fredonly 2 years, 8 months ago

Selected Answer: C
C- Compute Optimizer is the easiest solution
upvoted 1 times

mfsec 2 years, 9 months ago

Selected Answer: C
C - cost optimizer
upvoted 1 times

mfsec 2 years, 9 months ago

*Compute
upvoted 1 times

spd 2 years, 9 months ago

Selected Answer: C
C is correct - Optimizer
upvoted 2 times

kiran15789 2 years, 10 months ago

Selected Answer: A
Option C may be a good solution to rightsizing the EC2 instances but may incur additional cost for installing the Amazon CloudWatch agent on each of the EC2 instances.

The MOST cost-effective solution to analyze the company's Amazon EC2 instances and Amazon EBS volumes is to create a dashboard using AWS Systems Manager OpsCenter. The OpsCenter dashboard can be configured to visualize the Amazon CloudWatch metrics associated with the EC2 instances and their EBS volumes. By reviewing the dashboard periodically, usage patterns can be identified, and EC2 instances can be right-sized based on the peaks in the metrics.

upvoted 1 times

God_Is_Love 2 years, 9 months ago

Bro, install cost is 0. Simple linux command > sudo yum install amazon-cloudwatch-agent
upvoted 2 times

 **masetromain** 2 years, 11 months ago

Selected Answer: C

The correct answer is C. Installing the Amazon CloudWatch agent on each of the EC2 instances and turning on AWS Compute Optimizer allows the solutions architect to analyze the environment and make recommendations on the sizing of the EC2 instances in a cost-effective way. AWS Compute Optimizer analyzes the utilization of the instances and recommends the optimal instance types for the workloads. This solution is more cost-effective than creating a dashboard and reviewing it periodically, or signing up for the AWS Enterprise Support plan and waiting for Trusted Advisor recommendations.

upvoted 3 times

 **zhangyu20000** 2 years, 11 months ago

C is correct, with computer optimizer
upvoted 1 times

Question #131

A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company uses AWS Control Tower for governance and uses AWS Transit Gateway for VPC connectivity across accounts.

In an AWS application account, the company's application team has deployed a web application that uses AWS Lambda and Amazon RDS. The company's database administrators have a separate DBA account and use the account to centrally manage all the databases across the organization. The database administrators use an Amazon EC2 instance that is deployed in the DBA account to access an RDS database that is deployed in the application account.

The application team has stored the database credentials as secrets in AWS Secrets Manager in the application account. The application team is manually sharing the secrets with the database administrators. The secrets are encrypted by the default AWS managed key for Secrets Manager in the application account. A solutions architect needs to implement a solution that gives the database administrators access to the database and eliminates the need to manually share the secrets.

Which solution will meet these requirements?

- A. Use AWS Resource Access Manager (AWS RAM) to share the secrets from the application account with the DBA account. In the DBA account, create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the shared secrets. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- B. In the application account, create an IAM role that is named DBA-Secret. Grant the role the required permissions to access the secrets. In the DBA account, create an IAM role that is named DBA-Admin. Grant the DBA-Admin role the required permissions to assume the DBA-Secret role in the application account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets
- C. In the DBA account create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the secrets and the default AWS managed key in the application account. In the application account, attach resource-based policies to the key to allow access from the DBA account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- D. In the DBA account, create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the secrets in the application account. Attach an SCP to the application account to allow access to the secrets from the DBA account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.

Correct Answer: B*Community vote distribution*

B (82%)

Other

 **bititan** Highly Voted 2 years, 4 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 16 times

 **Sarutobi** Highly Voted 2 years, 2 months 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 7 times

 **ninomfr64** 1 year, 5 months ago

Grant the DBA-Admin role the required permissions to assume the DBA-Secret role in the application account. This sounds like a trust policy to me
 upvoted 1 times

 **4a86914** Most Recent 3 months ago

Selected Answer: B

A: Wrong, RAM does not support KMS for resource sharing.
 C: You can't edit AWS managed key.
 D: SCP is used to deny permissions. It can't allow/grant permissions.
 upvoted 1 times

 **princajen** 4 months, 3 weeks ago

Selected Answer: C

Although AWS supports cross-account access to Secrets Manager secrets using AssumeRole (Option B), it only works if the secret is encrypted with a customer-managed KMS key (CMK). The question specifies that the secret is encrypted with the default AWS-managed key, which cannot be shared across accounts. As confirmed by AWS's own documentation (<https://aws.amazon.com/blogs/database/design-patterns-to-access-cross-account-secrets-stored-in-aws-secrets-manager/>), this requires switching to a CMK and granting cross-account kms:Decrypt access. Therefore, the correct answer is Option C, not B.

upvoted 1 times

 **Chris_W_1234** 2 months, 1 week ago

It's exactly the other way around: When using a resource-based policy, you can't use the default AWS-managed key, ergo C is not possible. But the identity-based policy from B *works* with either type of key. Ergo, answer is B.

upvoted 1 times

 **ninomfr64** 1 year, 5 months ago

Selected Answer: B

A = Secret is not a RAM sharable resource. But who can recall this full list? Thus my reasoning is, I would expect more details for sharing via RAM like enable AWS Org sharing, assign permission (actions allowed on the shared resource) and select the external principal.
 B = correct see <https://aws.amazon.com/blogs/database/design-patterns-to-access-cross-account-secrets-stored-in-aws-secrets-manager/>
 C = cannot cross-account access AWS managed KMS key as you do not have control on key policy
 D = SCP can only remove permissions. Even tough an SCP doesn't prevent you from accessing a secret, you still need to have IAM user permission and/or resource based policy in place to actually access

upvoted 4 times

 **horyoryo** 1 year, 6 months ago

option b

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: B

Option B

upvoted 1 times

 **bjexamprep** 1 year, 6 months ago

Selected Answer: B

Even B is the best answer among all the options, actually B is not correct. Without permission to access the KMS key, B cannot decrypt the secret.

upvoted 2 times

 **bjexamprep** 1 year, 3 months ago

I was wrong. It is using AWS managed default encryption key, so it doesn't need the permission to access KMS key. The flaw of B is trust relationship policy.

upvoted 1 times

 **severlight** 1 year, 7 months ago

Selected Answer: B

the Secrets Manager keys cannot be shared with RAM, key policy(resource policy) for the default KMS key managed by AWS cannot be changed, role is identity and can be granted access to assume other role

upvoted 1 times

 **rif** 1 year, 8 months ago

Answer is B.

Option A is wrong. AWS RAM can not share AWS Secrets Manager (see shareable resources in <https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>)

upvoted 3 times

 **uC6rW1aB** 1 year, 9 months ago

Selected Answer: A

Both Option A and Option B give repository administrators access to the repository and eliminate the need to manually share secrets. Option A is a relatively simple process of sharing secrets with AWS RAM and setting up an IAM role within the DBA account.

Option B requires creating an IAM role in two different AWS accounts and setting cross-account permissions, which is a more complicated process.

So, while both A and B accomplish the goal, option A is simpler and more straightforward.

upvoted 1 times

 **chikorita** 1 year, 9 months ago

who said we can share secrets using RAM??

i just checked under RAM and allowed sharable AWS services

AWS Secrets Manager is NOT one of those

Answer is B

upvoted 4 times

 **venvig** 1 year, 10 months 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** 1 year, 11 months ago

Selected Answer: B

its a b

upvoted 1 times

 **Jackhemo** 2 years 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** 2 years, 1 month 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 (OU)s 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** 2 years ago

I couldn't find any option to share Secret Manager resources via RAM, did anyone try it?

upvoted 4 times

 **dev112233xx** 2 years, 2 months 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** 2 years, 3 months ago

Selected Answer: B

B is the best choice

upvoted 2 times

Question #132

A company manages multiple AWS accounts by using AWS Organizations. Under the root OU, the company has two OUs: Research and DataOps.

Because of regulatory requirements, all resources that the company deploys in the organization must reside in the ap-northeast-1 Region. Additionally, EC2 instances that the company deploys in the DataOps OU must use a predefined list of instance types.

A solutions architect must implement a solution that applies these restrictions. The solution must maximize operational efficiency and must minimize ongoing maintenance.

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

- A. Create an IAM role in one account under the DataOps OU. Use the ec2:InstanceType condition key in an inline policy on the role to restrict access to specific instance type.
- B. Create an IAM user in all accounts under the root OU. Use the aws:RequestedRegion condition key in an inline policy on each user to restrict access to all AWS Regions except ap-northeast-1.
- C. Create an SCP. Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU.
- D. Create an SCP. Use the ec2:Region condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU, the DataOps OU, and the Research OU.
- E. Create an SCP. Use the ec2:InstanceType condition key to restrict access to specific instance types. Apply the SCP to the DataOps OU.

Correct Answer: CE

Community vote distribution

CE (100%)

 **OCHT** Highly Voted 2 years, 2 months 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 6 times

 **OCHT** 2 years, 2 months 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 4 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: CE

To enforce organization-wide region restrictions and instance type controls efficiently, use SCPs. Option C uses aws:RequestedRegion in an SCP attached to the root OU, which restricts all accounts to deploy only in ap-northeast-1. Option E uses ec2:InstanceType in an SCP attached to the DataOps OU, restricting EC2 launches to approved instance types only in that OU. IAM roles or inline policies would require per-account maintenance and don't scale — so SCPs are the correct governance solution here.

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: CE

Option C & E

upvoted 1 times

 **venvig** 1 year, 10 months ago

Selected Answer: CE

Very straightforward

upvoted 2 times

 **dtha1002** 1 year, 11 months ago

Selected Answer: CE

C for all resources region
and E for DataOps OU launch instance type

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: CE

its CE

upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: CE

SCP's are the most efficient here
upvoted 1 times

 **tatdatpham** 2 years, 4 months ago

Selected Answer: CE

With AWS Org, consider SCP first.
In this scenario, Only C,D,E are mention about SCP, but D apply for all, not only the DataOps OU
upvoted 4 times

 **masetromain** 2 years, 5 months ago

Selected Answer: CE

The correct options are C and E.

Option C: Create an SCP. Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU.

This option is correct because it allows the company to restrict access to all AWS regions except for ap-northeast-1. This ensures that all resources deployed in the organization must reside in the ap-northeast-1 region. By applying the SCP to the root OU, it ensures that all accounts and OUs under the root will be affected.

Option E: Create an SCP. Use the ec2:InstanceType condition key to restrict access to specific instance types. Apply the SCP to the DataOps OU.

This option is correct because it allows the company to restrict access to specific instance types, which is required for the DataOps OU. By applying the SCP to the DataOps OU, it ensures that only resources deployed in the DataOps OU will be affected by the restriction.

upvoted 4 times

 **masetromain** 2 years, 5 months ago

Option A is incorrect because it only restricts access to specific instance types, but it does not restrict access to a specific region.

Option B is incorrect because it is applied to IAM users rather than OUs, which would not effectively apply the restriction to all resources in the organization.

Option D is incorrect because it uses the ec2:Region condition key which would not allow to restrict the instances types only in the DataOps OU.

By creating an SCP that uses the aws:RequestedRegion condition key and restricting access to all regions except ap-northeast-1 and applying it to the root OU, this ensures that all resources deployed in the organization will reside in the ap-northeast-1 Region.

By creating an SCP that uses the ec2:InstanceType condition key and restricts access to specific instance types and applying it to the DataOps OU, this ensures that all EC2 instances deployed in the DataOps OU will use the predefined list of instance types.

upvoted 1 times

 **zhangyu20000** 2 years, 5 months ago

CE is correct

upvoted 1 times

Question #133

A company runs a serverless application in a single AWS Region. The application accesses external URLs and extracts metadata from those sites. The company uses an Amazon Simple Notification Service (Amazon SNS) topic to publish URLs to an Amazon Simple Queue Service (Amazon SQS) queue. An AWS Lambda function uses the queue as an event source and processes the URLs from the queue. Results are saved to an Amazon S3 bucket.

The company wants to process each URL in other Regions to compare possible differences in site localization. URLs must be published from the existing Region. Results must be written to the existing S3 bucket in the current Region.

Which combination of changes will produce multi-Region deployment that meets these requirements? (Choose two.)

- A. Deploy the SQS queue with the Lambda function to other Regions.
- B. Subscribe the SNS topic in each Region to the SQS queue.
- C. Subscribe the SQS queue in each Region to the SNS topic.
- D. Configure the SQS queue to publish URLs to SNS topics in each Region.
- E. Deploy the SNS topic and the Lambda function to other Regions.

Correct Answer: AC

Community vote distribution

AC (100%)

 **SK_Tyagi** Highly Voted 1 year, 10 months ago

Selected Answer: AC

SNS being the publisher, SQS is subscribing
upvoted 6 times

 **rif** Highly Voted 1 year, 8 months ago

AC.
Amazon SNS supports cross-region deliveries.
<https://docs.aws.amazon.com/sns/latest/dg/sns-cross-region-delivery.html>
upvoted 5 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: AC

To support multi-Region processing while keeping a centralized publisher, you deploy SQS queues and Lambda functions in each target Region (Option A). Then, you subscribe each regional SQS queue to the existing SNS topic in the origin Region (Option C). This pattern enables cross-Region fan-out for localized processing, while publishing remains centralized and results are saved to the original S3 bucket.
upvoted 1 times

 **SeemaDataReader** 1 year, 5 months ago

Selected Answer: AC

SNS in Region A, SQS + Lambda in Region A & B, S3 Bucket in Region A
upvoted 2 times

 **career360guru** 1 year, 6 months ago

Selected Answer: AC

A and C
upvoted 1 times

 **Passeexam4sure_com** 1 year, 8 months ago

Selected Answer: AC

Deploy the SQS queue with the Lambda function to other Regions.
Subscribe the SQS queue in each Region to the SNS topic.
upvoted 3 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: AC

It's an AC
upvoted 2 times

 **Maria2023** 2 years 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 3 times

 **awsleffe** 1 year, 2 months ago
SNS is the publisher and must stay in same region
upvoted 1 times

 **Parsons** 2 years, 2 months ago

Selected Answer: AC

A, C is correct.
It looks like Fan out pattern.
upvoted 3 times

 **Kampton** 2 years, 2 months ago

Why would need to deploy SQS with Lambda? Makes no sense! It's BE.
upvoted 1 times

 **Diego1414** 2 years, 1 month ago
It's SNS that publishes not SQS
upvoted 2 times

 **Asagumo** 2 years, 2 months ago

What does it mean in Option A that Lambda deploys SQS?
upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: AC
AC - SQS
upvoted 2 times

 **Zek** 2 years, 3 months ago

support A,C. <https://www.examtopics.com/discussions/amazon/view/74009-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 1 times

 **MasterP007** 2 years, 4 months ago

A & C - Deploy & Subscribe SQS.
upvoted 1 times

 **zozza2023** 2 years, 5 months ago

Selected Answer: AC
A and C
upvoted 3 times

 **masetromain** 2 years, 5 months ago

Selected Answer: AC
Option A is correct because deploying the SQS queue with the Lambda function to other regions will allow the application to process URLs in those regions and compare differences in site localization.

Option C is correct because subscribing the SQS queue in each region to the SNS topic in the existing region will allow the application to publish URLs to the existing SNS topic and have those URLs processed in other regions.

Option B is incorrect because subscribing the SNS topic in each region to the SQS queue in the existing region would not allow URLs to be processed in other regions.

Option D is incorrect because configuring the SQS queue to publish URLs to SNS topics in each region would not ensure that the URLs are processed in those regions.

Option E is incorrect because deploying the SNS topic and Lambda function to other regions without the SQS queue would not allow the application to process URLs in those regions.

upvoted 4 times

 **zhangyu20000** 2 years, 5 months ago

AC is correct
upvoted 1 times

Question #134

A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instances. The application is a Linux binary, and the source code cannot be modified. The application is single-threaded, uses 2 GB of RAM, and is highly CPU intensive. The application is scheduled to run every 4 hours and runs for up to 20 minutes. A solutions architect wants to revise the architecture for the solution.

Which strategy should the solutions architect use?

- A. Use AWS Lambda to run the application. Use Amazon CloudWatch Logs to invoke the Lambda function every 4 hours.
- B. Use AWS Batch to run the application. Use an AWS Step Functions state machine to invoke the AWS Batch job every 4 hours.
- C. Use AWS Fargate to run the application. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours.
- D. Use Amazon EC2 Spot Instances to run the application. Use AWS CodeDeploy to deploy and run the application every 4 hours.

Correct Answer: C*Community vote distribution*

C (74%)	B (19%)	7%
---------	---------	----

 **zhangyu20000** Highly Voted 2 years, 5 months ago

C is correct. only eventbridge can run scheduled task
upvoted 16 times

 **Maria2023** Highly Voted 2 years 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 6 times

 **eesa** Most Recent 8 months, 1 week ago

Selected Answer: C

AWS Fargate is ideal for running containerized workloads without managing underlying EC2 instances. Even though the application is a binary and its source code cannot be modified, it can be easily packaged into a Docker container without changing the binary itself.

Since the application runs periodically (every 4 hours) and for a short duration (up to 20 minutes), Fargate provides a cost-effective, serverless execution environment.

Amazon EventBridge (CloudWatch Events) can be scheduled to invoke Fargate tasks precisely at defined intervals.

upvoted 2 times

 **Longc** 9 months, 3 weeks ago

Selected Answer: C

Option C clearly includes EventBridge for scheduling, aligning with the requirement to run tasks every 4 hours. While AWS Batch is technically better for CPU-intensive workloads, the lack of explicit EventBridge integration in Option B makes C the correct answer under AWS's service design principles.

upvoted 1 times

 **albert_kuo** 9 months, 4 weeks ago

Selected Answer: B

B. Use AWS Batch to run the application. Use an AWS Step Functions state machine to invoke the AWS Batch job every 4 hours.
upvoted 2 times

 **9d7a975** 10 months, 2 weeks ago

Selected Answer: B

B: Usa uma máquina de estado do AWS Step Functions para invocar o trabalho do AWS Batch a cada 4 horas.
Por que não é a letra C : Embora possa executar containers, é mais adequado para aplicações de longa duração
upvoted 3 times

 **TonytheTiger** 1 year, 2 months ago

Option C : <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/run-event-driven-and-scheduled-workloads-at-scale-with-aws-fargate.html>
upvoted 1 times

 **ninomfr64** 1 year, 5 months ago

A = CW Log cannot invoke lambda every 4 hours
B = Step Function cannot invoke batch job every 4 hour (unless you use an EventBridhe scheduled event)
C = correct (but I do not like when Fargate is mentioned as a standalone service, as it is a serverless compute option for some some

services)

D = CodeDeploy cannot run an application every 4 hours

upvoted 3 times

 **cox1960** 1 year, 5 months ago

none. "highly CPU intensive" means no Fargate. scheduling means eventbridge.

upvoted 2 times

 **holymancolin** 1 year, 5 months ago

<https://aws.amazon.com/about-aws/whats-new/2018/10/aws-lambda-supports-functions-that-can-run-up-to-15-minutes/>
Lambda's max running time is 15 mins, cannot support up to 20mins application.

upvoted 1 times

 **haha001** 1 year, 6 months ago

<https://aws.amazon.com/tutorials/scheduling-a-serverless-workflow-step-functions-amazon-eventbridge-scheduler/>
Step Function cannot schedule a job. Step Function needs EventBridge as the scheduler.

upvoted 2 times

 **career360guru** 1 year, 6 months ago

Selected Answer: C

B is not possible as Step Function can not be used to run scheduled a job every 4 hour

upvoted 1 times

 **task_7** 1 year, 9 months ago

Selected Answer: D

containers are well-suited for applications that are built in microservices architecture, where each service is a self-contained unit that performs a specific task. These types of applications are typically designed to be scalable and easy to deploy, making them a good fit for containerization.

I feel D is the best option

upvoted 2 times

 **teo2157** 1 year, 4 months ago

you can't guarantee with spot instances that they're available every 4 hours, C is the answer

upvoted 3 times

 **uC6rW1aB** 1 year, 9 months ago

Selected Answer: C

I think Both B , C is missing some key point

Option B does not explain how to AWS Step Functions to trigger an AWS Batch job regularly, in this case 4 hours per run.

Option C does not explain how to use EventBridge to call the Fargate task, which is not native support, it might involve Lambda to achieve.

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

C. schedule -> eventbridge

upvoted 1 times

 **rbm2023** 2 years, 1 month 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 EventBridge.

Use a base image that matches your application's runtime environment

FROM ubuntu:latest

Copy the Linux binary into the container

COPY myapp /usr/local/bin/myapp

Set the entry point to execute the binary

ENTRYPOINT ["/usr/local/bin/myapp"]

upvoted 3 times

 **mfsec** 2 years, 3 months ago

Selected Answer: C

C - Fargate is the best choice here

upvoted 1 times

Question #135

A company is creating a sequel for a popular online game. A large number of users from all over the world will play the game within the first week after launch. Currently, the game consists of the following components deployed in a single AWS Region:

- Amazon S3 bucket that stores game assets
- Amazon DynamoDB table that stores player scores

A solutions architect needs to design a multi-Region solution that will reduce latency, improve reliability, and require the least effort to implement.

What should the solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Cross-Region Replication. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.
- B. Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Same-Region Replication. Create a new DynamoDB table in a new Region. Configure asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC).
- C. Create another S3 bucket in a new Region, and configure S3 Cross-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region. Configure DynamoDB global tables by enabling Amazon DynamoDB Streams, and add a replica table in a new Region.
- D. Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.

Correct Answer: C

Community vote distribution

C (87%)

13%

 **zozza2023**  2 years, 11 months ago

Selected Answer: C

DynamoDB global tables + S3 replication+Cloudfront
upvoted 14 times

 **masetromain**  2 years, 11 months ago

Option C is the correct answer because it meets the requirements of reducing latency, improving reliability and requiring minimal effort to implement.

By creating another S3 bucket in a new Region, and configuring S3 Cross-Region Replication between the buckets, the game assets will be replicated to the new Region, reducing latency for users accessing the assets from that region. Additionally, by creating an Amazon CloudFront distribution and configuring origin failover with two origins accessing the S3 buckets in each Region, it ensures that the game assets will be served to users even if one of the regions becomes unavailable.

Configuring DynamoDB global tables by enabling Amazon DynamoDB Streams, and adding a replica table in a new Region, will also improve reliability by allowing the player scores to be replicated and updated in multiple regions, ensuring that the scores are available even in the event of a regional failure.

upvoted 8 times

 **masetromain** 2 years, 11 months ago

Option A is not correct because using the new table as a replica target for DynamoDB global tables will not improve reliability. The same applies for Option D, which only uses S3 Same-Region Replication, which will not reduce latency for users in other regions.

Option B is not correct because configuring asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC) is not the best solution for this use case. It would require additional configuration and management effort.

upvoted 3 times

 **jimee11**  7 months, 3 weeks ago

Selected Answer: C

CloudFront supports two origins, and Streaming is required to enable Global tables.
upvoted 1 times

 **Daniel76** 1 year, 2 months ago

Selected Answer: C

Just to add for DynamoDB, indeed you will need to create replica in the new region when creating global table, making it accessible in the new region nearer to the user.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/V2globaltables.tutorial.html>

upvoted 1 times

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

Selected Answer: C

Option C is correct.

Just to clarify: AWS uses DynamoDB Streams to replicate DynamoDB Global Tables. Using the Console, it is enabled automatically. Using the CLI, you must enable it explicitly by using StreamEnabled=true.

upvoted 1 times

✉ **ninomfr64** 1 year, 11 months ago

Selected Answer: C

A = "Configure S3 Cross-Region Replication" but doesn't create a new bucket in another region.

B = "Configure S3 Same-Region Replication" without creating a second bucket and this should be cross-region. AWS DMS with CDC is not a good fit here, global table is the right option here

C = correct

D = we need the new bucket in a different region

upvoted 1 times

✉ **career360guru** 2 years ago

Selected Answer: C

Option C

upvoted 2 times

✉ **shaam80** 2 years ago

Selected Answer: C

Answer C.

Regarding DynamoDB Streams -

Global tables use DynamoDB Streams to replicate data across different Regions. When you create a replica for a global table, a stream is created by default. Any changes to a replica are replicated to all the other replicas within the same global table within a second using DynamoDB Streams.

upvoted 2 times

✉ **blackgamer** 2 years, 1 month ago

The answer is A. C added unnecessary complexities such as Amazon DynamoDB Streams and Origin Failover.

upvoted 1 times

✉ **ninomfr64** 1 year, 11 months ago

Option A doesn't mention creating a new bucket in a different region

upvoted 1 times

✉ **Jay_2pt0_1** 2 years, 1 month ago

I initially thought it was C, but I was torn between A and C. You may be right.

upvoted 1 times

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

just C

upvoted 1 times

✉ **uC6rW1aB** 2 years, 3 months ago

Selected Answer: A

other option are incorrect.

B: Configure S3 Same-Region Replication.---> It's not meet multi-region requirement.

C: Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region. ---> It's not support for this kinda failover

D: Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets. ---> It's not meet multi-region requirement.

upvoted 2 times

✉ **ninomfr64** 1 year, 11 months ago

C is correct, Origin Group allows failover see

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

upvoted 2 times

✉ **dkcloudguru** 2 years, 3 months ago

option c is the easiest way to do

upvoted 1 times

✉ **ProMax** 2 years, 3 months 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 2 times

 **SK_Tyagi** 2 years, 4 months ago

Selected Answer: C

Option C has another differentiator - DynamoDBStreams that will assist in Reliability

upvoted 2 times

 **ggrodsckiy** 2 years, 5 months 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** 2 years, 3 months 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 years, 5 months ago

Selected Answer: C

weird question wording, but C fit more

upvoted 1 times

 **mfsec** 2 years, 9 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

 **zhangyu20000** 2 years, 11 months ago

C is correct. S3 cross replicate, CloudFront, Dynamodb global database and origin failover

upvoted 2 times

Question #136

Topic 1

A company has an on-premises website application that provides real estate information for potential renters and buyers. The website uses a Java backend and a NoSQL MongoDB database to store subscriber data.

The company needs to migrate the entire application to AWS with a similar structure. The application must be deployed for high availability, and the company cannot make changes to the application.

Which solution will meet these requirements?

- A. Use an Amazon Aurora DB cluster as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.
- B. Use MongoDB on Amazon EC2 instances as the database for the subscriber data. Deploy EC2 instances in an Auto Scaling group in a single Availability Zone for the Java backend application.
- C. Configure Amazon DocumentDB (with MongoDB compatibility) with appropriately sized instances in multiple Availability Zones as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.
- D. Configure Amazon DocumentDB (with MongoDB compatibility) in on-demand capacity mode in multiple Availability Zones as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.

Correct Answer: C

Community vote distribution

C (87%)	13%
---------	-----

 uC6rW1aB Highly Voted 2 years, 3 months ago

Selected Answer: C

C correct
DocumentDB only have on-demand instance but not on-demand capacity mode, the mode is for DynamoDB
upvoted 13 times

 ninomfr64 Highly Voted 1 year, 11 months ago

Selected Answer: C

A = Aurora supports MySQL and PostgreSQL, not MongoDB. App changes are not allowed
B = This could work but DocumentDB provides managed MongoDB instance that is preferable
C = correct
D = there isn't on-demand capacity mode, in 2022 launched MondoDB Elastic Cluster that eliminates the need to choose, manage or upgrade instances and allows to scale up to 4PiB storage whereas instance based scales up to 128TiB.

I thing this question is pre elastic cluster as this is ambiguous between C and D
upvoted 6 times

 lunt Most Recent 2 weeks ago

Selected Answer: C

A. DB engine not same - nope.
B. Fails HA.
D. DocumentDB has no on-demand capacity "mode". It does have serverless, this is a misdirect. DocumentDB as of DEC2025 does have on-demand "instances" "pricing" model - key work instances + pricing > its not a "mode" but a billing feature. There is no "mode" setting to you set. AWS best practice migration = right sized unless specific scaling is required.
C = Yes.
upvoted 1 times

 princajen 4 months, 3 weeks ago

Selected Answer: C

Option C is correct because it uses Amazon DocumentDB, which is compatible with MongoDB and supports multi-AZ high availability. This allows the application to be migrated without any code changes. The Java backend is hosted on EC2 with Auto Scaling across multiple AZs, providing HA at the compute layer. It meets all requirements and minimizes operational overhead.
upvoted 1 times

 jimee11 7 months, 3 weeks ago

Selected Answer: C

C: DocumentDB has an on-demand instance type but NO on-demand capacity mode. Note the difference between the two:

On-demand instance type is specific to EC2 pricing for hourly or per-second compute capacity. On-demand capacity mode is specific for DynamoDB and Kinesis for pay-per-request pricing and no up-front capacity planning.

upvoted 1 times

 **cnethe** 1 year, 5 months ago

D is the correct answer <https://aws.amazon.com/documentdb/pricing/>
on-demand instance is supported by DocumentDB

upvoted 1 times

 **helloworldabc** 1 year, 3 months ago

just C

upvoted 2 times

 **gofavad926** 1 year, 9 months ago

Selected Answer: C

C, documented. No exists the on-demand capacity mode

upvoted 1 times

 **AimarLeo** 1 year, 11 months ago

'Appropriately sized instances' Means on-demand ? that is quite vague..

upvoted 4 times

 **jpa8300** 1 year, 11 months ago

Selected Answer: D

DocumentDB does indeed support on-demand capacity mode (Contrary to what other users say here)

<https://aws.amazon.com/blogs/database/running-spiky-workloads-and-optimizing-costs-by-more-than-90-using-amazon-dynamodb-on-demand-capacity-mode/>

On-Demand is ideally to a use case where you have unpredictable or variable database workloads, like this case, it is not said anywhere the expected workload, so it is better to start with On-demand , and later when you know the workload you can change it.

upvoted 2 times

 **buriz** 1 year, 11 months ago

what you have linked here is a dynamodb article not a documentDB one, documentDB does not support on-demand capacity mode -
<https://aws.amazon.com/documentdb/faqs/>

"You can scale the compute resources allocated to your instance in the AWS Management Console by selecting the desired instance and clicking the "modify" button. Memory and CPU resources are modified by changing your instance class."

upvoted 2 times

 **ninomfr64** 1 year, 11 months ago

There is no on-demand capacity for DocumentDB, however Elastic Cluster option is provided "Elastic Clusters enables you to elastically scale your document database to handle millions of writes and reads, with petabytes of storage capacity" see
<https://aws.amazon.com/documentdb/faqs/#:~:text=to%20learn%20more.-,Elastic%20Clusters,-What%20is%20Amazon>

upvoted 1 times

 **chicagobeef** 1 year, 11 months ago

This is DynamoDB, not DocumentDB. The choices only mention DocumentDB.

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: C

There is no on-demand capacity mode for DocumentDB, though there is on-demand vCPU based pricing available.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

There is no on-demand capacity for DocumentDB, however Elastic Cluster option is provided "Elastic Clusters enables you to elastically scale your document database to handle millions of writes and reads, with petabytes of storage capacity" see
<https://aws.amazon.com/documentdb/faqs/#:~:text=to%20learn%20more.-,Elastic%20Clusters,-What%20is%20Amazon>

upvoted 1 times

 **2aa2222** 1 year, 4 months ago

DocumentDB does support on-demand capacity:

<https://aws.amazon.com/documentdb/pricing/#:~:text=On-demand%20instances%20let%20you%20pay%20per%20second%2C%20and%20having%20to%20guess%20the%20correct%20capacity>

upvoted 1 times

 **ProMax** 2 years, 3 months ago

Selected Answer: C

Amazon DocumentDB does NOT have on-demand capacity mode, so its option C.

upvoted 3 times

 **ninomfr64** 1 year, 11 months ago

There is no on-demand capacity for DocumentDB, however Elastic Cluster option is provided "Elastic Clusters enables you to elastically scale your document database to handle millions of writes and reads, with petabytes of storage capacity" see
<https://aws.amazon.com/documentdb/faqs/#:~:text=to%20learn%20more.-,Elastic%20Clusters,-What%20is%20Amazon>

upvoted 1 times

✉ **SK_Tyagi** 2 years, 4 months ago

Selected Answer: D

I was leaning towards Option C but "Appropriately sized instances" is vague since the question does not state the size of Mongo DB. On-demand instances serve the purpose here, they are offered by DocumentDB, see the link
<https://aws.amazon.com/documentdb/pricing/>

upvoted 2 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

its a c

upvoted 2 times

✉ **easystoo** 2 years, 6 months ago

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

On-demand capacity mode as suggested in D may not provide the same level of high availability as multi-Availability Zone deployments. So it's c-c-c-c-c-c-c for me.

upvoted 2 times

✉ **SkyZeroZx** 2 years, 6 months ago

Selected Answer: C

See best practices for amazon documentdb - instance sizing in docs.

Additionally there is no on-demand capacity mode.

upvoted 2 times

✉ **F_Eldin** 2 years, 7 months 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** 2 years, 7 months ago

The correct link <https://www.apptytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/743016963590682>

upvoted 2 times

✉ **[Removed]** 2 years, 1 month ago

The content mentioned in your link and the original comment are both mentioning things related to DynamoDB. Your link is even worse which is describing DynamoDB but say it is for DocumentDB. Please study hard

upvoted 1 times

✉ **leehjworking** 2 years, 7 months ago

Selected Answer: C

See best practices for amazon documentdb - instance sizing in docs.

upvoted 1 times

Question #137

A digital marketing company has multiple AWS accounts that belong to various teams. The creative team uses an Amazon S3 bucket in its AWS account to securely store images and media files that are used as content for the company's marketing campaigns. The creative team wants to share the S3 bucket with the strategy team so that the strategy team can view the objects.

A solutions architect has created an IAM role that is named `strategy_reviewer` in the Strategy account. The solutions architect also has set up a custom AWS Key Management Service (AWS KMS) key in the Creative account and has associated the key with the S3 bucket. However, when users from the Strategy account assume the IAM role and try to access objects in the S3 bucket, they receive an Access Denied error.

The solutions architect must ensure that users in the Strategy account can access the S3 bucket. The solution must provide these users with only the minimum permissions that they need.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the bucket policy to the account ID of the Strategy account.
- B. Update the `strategy_reviewer` IAM role to grant full permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key.
- C. Update the custom KMS key policy in the Creative account to grant decrypt permissions to the `strategy_reviewer` IAM role.
- D. Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the bucket policy to an anonymous user.
- E. Update the custom KMS key policy in the Creative account to grant encrypt permissions to the `strategy_reviewer` IAM role.
- F. Update the `strategy_reviewer` IAM role to grant read permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key.

Correct Answer: ACF

Community vote distribution

ACF (100%)

 **God_Is_Love** Highly Voted  2 years, 3 months 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 13 times

 **God_Is_Love** 2 years, 3 months ago

first the source bucket needs to give grant access thru bucket policy and KMS key policy (A,C options)
 Secondly, Strategy IAM role needs to give access to read from S3 bucket and also KMS key (Option F)
 upvoted 3 times

 **leehjworking** Highly Voted  2 years, 1 month ago

Selected Answer: ACF

B full permission ? X
 D anonymous? X
 E encryption not needed for strategy team
 upvoted 6 times

 **princajen** Most Recent  4 months, 3 weeks ago

Selected Answer: ACF

To enable secure cross-account S3 access with KMS, the following are required:

The S3 bucket policy must allow the assumed role (A)
 The IAM role must include `s3:GetObject` and `kms:Decrypt` permissions (F)
 The KMS key policy must explicitly grant decrypt access to the assumed role (C)
 upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: ACF

A, C and F
 upvoted 1 times

SK_Tyagi 1 year, 10 months ago
Selected Answer: ACF
By rule of elimination
BDE are wrong. God_Is_Love is spot on
upvoted 1 times

NikkyDicky 1 year, 11 months ago
Selected Answer: ACF
its ACF
upvoted 2 times

OCHT 2 years, 2 months 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 2 years, 3 months ago
Selected Answer: ACF
ACF is the best choice
upvoted 2 times

taer 2 years, 3 months 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 2 years, 5 months ago
Selected Answer: ACF
A C AND F
upvoted 3 times

Untamables 2 years, 5 months ago
Selected Answer: ACF
<https://repost.aws/knowledge-center/cross-account-access-denied-error-s3>
upvoted 3 times

masetromain 2 years, 5 months ago
Selected Answer: ACF
A, C, and F are the correct options.
upvoted 4 times

masetromain 2 years, 5 months ago
A, C, and F are the correct options.

Option A creates a bucket policy that includes read permissions for the S3 bucket and sets the principal of the bucket policy to the account ID of the Strategy account. This ensures that users in the Strategy account have the necessary permissions to access the S3 bucket.

Option C updates the custom KMS key policy in the Creative account to grant decrypt permissions to the strategy_reviewer IAM role. This ensures that the users in the Strategy account have the necessary permissions to decrypt the objects stored in the S3 bucket.

Option F updates the strategy_reviewer IAM role to grant read permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key. This ensures that the users in the Strategy account have the necessary permissions to read the objects in the S3 bucket and to decrypt them using the custom KMS key.

The other options are not correct because they either grant unnecessary permissions (B, D) or grant permissions in the wrong way (E).
upvoted 3 times

zhangyu20000 2 years, 5 months ago
ACF is correct
upvoted 2 times

Question #138

A life sciences company is using a combination of open source tools to manage data analysis workflows and Docker containers running on servers in its on-premises data center to process genomics data. Sequencing data is generated and stored on a local storage area network (SAN), and then the data is processed. The research and development teams are running into capacity issues and have decided to re-architect their genomics analysis platform on AWS to scale based on workload demands and reduce the turnaround time from weeks to days.

The company has a high-speed AWS Direct Connect connection. Sequencers will generate around 200 GB of data for each genome, and individual jobs can take several hours to process the data with ideal compute capacity. The end result will be stored in Amazon S3. The company is expecting 10-15 job requests each day.

Which solution meets these requirements?

- A. Use regularly scheduled AWS Snowball Edge devices to transfer the sequencing data into AWS. When AWS receives the Snowball Edge device and the data is loaded into Amazon S3, use S3 events to trigger an AWS Lambda function to process the data.
- B. Use AWS Data Pipeline to transfer the sequencing data to Amazon S3. Use S3 events to trigger an Amazon EC2 Auto Scaling group to launch custom-AMI EC2 instances running the Docker containers to process the data.
- C. Use AWS DataSync to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Lambda function that starts an AWS Step Functions workflow. Store the Docker images in Amazon Elastic Container Registry (Amazon ECR) and trigger AWS Batch to run the container and process the sequencing data.
- D. Use an AWS Storage Gateway file gateway to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Batch job that executes on Amazon EC2 instances running the Docker containers to process the data.

Correct Answer: C

Community vote distribution

C (79%)

D (21%)

 **dev112233xx**  2 years, 8 months 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 23 times

 **Kampton** 2 years, 8 months ago

Agree - The Lambda function acts as a bridge between the S3 event and AWS Batch, allowing you to trigger AWS Batch jobs in response to S3 events.

upvoted 3 times

 **God_Is_Love**  2 years, 9 months 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 9 times

 **God_Is_Love** 2 years, 9 months ago

On Premise NAS and file servers to S3. --> Use DataSync solution

On Premise SMB or NFS file share to S3 --> Use Storage/File Gateway solution

upvoted 4 times

 **titi_r** 1 year, 9 months ago

@God_Is_Love, both articles you've provided are NOT mentioning "SAN" at all. You cannot copy data from SAN using storage GW, but you do it with DataSync ran from within a server, which is connected to that SAN. Research more on what SAN is and how does it work :)

upvoted 1 times

 **AWSum1** 1 year, 2 months ago

Nope, you need S3 events to trigger Lambda. S3 events cannot trigger batch

upvoted 1 times

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

just C

upvoted 1 times

✉️ **princajen** Most Recent ⓘ 4 months, 3 weeks ago

Selected Answer: C

Option C is correct because it uses AWS DataSync to rapidly and efficiently transfer large genomics files from the on-prem SAN to Amazon S3 over Direct Connect. Then, S3 events trigger a Lambda function that starts a Step Functions workflow, which coordinates job execution using AWS Batch, where Docker containers (stored in Amazon ECR) process the data. This approach is scalable, efficient, low-latency, and fully managed — meeting all business and technical requirements.

upvoted 1 times

✉️ **FZA24** 1 year, 2 months ago

Selected Answer: C

DataSync + Direct Connect
S3 => Lambda => SF
Docker => ECR => Batch

upvoted 1 times

✉️ **k10training02** 1 year, 4 months ago

lambda solo dura 900 segundos me voy por la D

upvoted 1 times

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

just C

upvoted 1 times

✉️ **trungtd** 1 year, 7 months ago

Selected Answer: C

Currently, S3 events can only push to three different types of destinations:

SNS topic, SQS Queue, AWS Lambda.

You cannot directly trigger a Batch job by S3 Event

upvoted 1 times

✉️ **ninomfr64** 1 year, 11 months ago

Selected Answer: C

A = 200GB very now and then doesn't need Snowball Edge

B = Data Pipeline is ETL and not suitable in hybrid scenarios

C = correct (DataSync does the job, also the app is already container based and it works well with Batch that is suited for HPC kind of workload - genomic sequencing is a typical HPC workload)

D = even tough Storage Gateway does the job you cannot directly trigger a AWS Batch job from an S3 event, you need either a Lambda in the middle or enable EventBridge notification and create a rule that triggers the AWS Batch Job

upvoted 3 times

✉️ **cox1960** 1 year, 11 months ago

... "The main requirement is that the data needs to be accessible over the network in a file format like NFS that DataSync supports."

upvoted 1 times

✉️ **cox1960** 1 year, 11 months ago

C - Amazon Q says "While it does not directly support SAN (storage area network), you can use AWS DataSync to transfer data from files stored on a SAN volume to AWS storage services like Amazon S3."

upvoted 1 times

✉️ **career360guru** 2 years ago

Selected Answer: C

Option C is better option. Though D is also possible but as the jobs are already container based C would be better.

Question is not clear whether containers used on-premise are docker based containers.

upvoted 2 times

✉️ **mosalahs** 2 years ago

Selected Answer: C

Data Transfer --- > Data Sync

Data Integration --- > Storage GW

Data Orchestration --- > Data Pipeline

upvoted 3 times

✉️ **Maygam** 2 years ago

Selected Answer: C

D doesn't seem to be correct as AWS Batch is not a destination for AWS S3 events.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html>

upvoted 2 times

✉️ **uC6rW1aB** 2 years, 3 months ago

Selected Answer: C

Option C: Use AWS DataSync to transfer data to Amazon S3. DataSync is designed for fast, easy and secure data transfer. This option also uses S3 events to trigger an AWS Lambda function, which launches an AWS Step Functions workflow and runs a Docker container using AWS Batch. This option takes into account data transfer, processing and container management, and should be the most suitable solution.

Option D: Use AWS Storage Gateway's file gateway to transfer data to Amazon S3. Storage Gateway is suitable for hybrid cloud environments, but in this case, since the company already has a high-speed AWS Direct Connect connection, it will be more efficient to use DataSync.

upvoted 2 times

 **Ganshank** 2 years, 4 months 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** 2 years, 4 months ago

Selected Answer: D

I choose D. My rationale - 200GB data for 1 genome sequence, Lets say DirectConnect is 1Gbps line, DataSync cannot efficiently transfer the data to get the processing under 1 day.

Agree with God_Is_Love's hypothesis

upvoted 1 times

 **vn_thanh tung** 2 years, 3 months ago

S3 event can't trigger direct AWS Batch job. => C

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Assuming DX is 1Gbps, it takes about 27 minutes to transfer 200GB. also, I don't see how Storage Gateway can speedup things. My point is that here both DataSync and Storage Gateway can do the job, but you cannot trigger Batch job directly from S3 object event. Thus C

upvoted 1 times

 **RGR21** 2 years, 4 months ago

Does the AWS DataSync support SAN?

upvoted 1 times

 **ggrodsckiy** 2 years, 5 months ago

Correct D.

upvoted 1 times

Question #139

Topic 1

A company runs a content management application on a single Windows Amazon EC2 instance in a development environment. The application reads and writes static content to a 2 TB Amazon Elastic Block Store (Amazon EBS) volume that is attached to the instance as the root device. The company plans to deploy this application in production as a highly available and fault-tolerant solution that runs on at least three EC2 instances across multiple Availability Zones.

A solutions architect must design a solution that joins all the instances that run the application to an Active Directory domain. The solution also must implement Windows ACLs to control access to file contents. The application always must maintain exactly the same content on all running instances at any given point in time.

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

- A. Create an Amazon Elastic File System (Amazon EFS) file share. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to install the application, join the instance to the AD domain, and mount the EFS file share.
- B. Create a new AMI from the current EC2 Instance that is running. Create an Amazon FSx for Lustre file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to join the instance to the AD domain and mount the FSx for Lustre file system.
- C. Create an Amazon FSx for Windows File Server file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to install the application and mount the FSx for Windows File Server file system. Perform a seamless domain join to join the instance to the AD domain.
- D. Create a new AMI from the current EC2 instance that is running. Create an Amazon Elastic File System (Amazon EFS) file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three Instances. Perform a seamless domain join to join the instance to the AD domain.

Correct Answer: C*Community vote distribution*

C (95%) 5%

 **God_Is_Love** Highly Voted 2 years, 3 months 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 16 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: C

Option C is correct because Amazon FSx for Windows File Server is the only service in the options that fully supports Windows Access Control Lists (ACLs) and Active Directory domain integration. It allows multiple EC2 instances to access the same shared file system across Availability Zones using the SMB protocol. It also reduces operational overhead by being fully managed and compatible with Windows-based environments.

upvoted 1 times

 **julmarcas** 1 year, 2 months ago

Selected Answer: C

C for windows, AD and ACLs
upvoted 1 times

 **rootcode** 1 year, 4 months ago

Selected Answer: C

C is the correct option
upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: C

Option C as it is windows based OS.
upvoted 1 times

 **uC6rW1aB** 1 year, 9 months ago

Selected Answer: C

Option B FSx for Lustre is not for Linux POSIX-compliant

Option C correct

upvoted 2 times

✉ **dkcloudguru** 1 year, 9 months ago

C FSx for windows is a good fit for this

upvoted 1 times

✉ **Sam202** 1 year, 11 months ago

FSx for Lustre can only be used by Linux-based instances.

upvoted 1 times

✉ **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

C for windows

upvoted 1 times

✉ **SkyZeroZx** 2 years ago

Selected Answer: C

EFS and FSx for Lustre == Linux

FSx Windows File == Windows

upvoted 3 times

✉ **mfsec** 2 years, 3 months ago

Selected Answer: C

EFS and Windows is not straight forward. C is the best solution.

upvoted 2 times

✉ **zejou1** 2 years, 3 months 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** 2 years, 4 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** 2 years, 4 months ago

Selected Answer: C

FSX for WIndows is the only option. The rest of options are not supported.

upvoted 2 times

✉ **jojom19980** 2 years, 4 months ago

Selected Answer: C

FSx for Lustre can only be used by Linux-based instances.

upvoted 2 times

✉ **zozza2023** 2 years, 5 months ago

Selected Answer: D

good answer are C or D but as it says LEAST management overhead ==> D as in C we will need a user data script

upvoted 1 times

✉ **zozza2023** 2 years, 5 months ago

sorry D is uncorrect as it use Elastic File System (Amazon EFS) itch is not windows so Iswitch to C

upvoted 1 times

✉ **lxrdm** 1 year, 11 months ago

Also that means each instance launched from the AMI will have 2TB EBS volume.. which is not ideal

upvoted 1 times

✉ **ARLV** 2 years, 5 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

Question #140

Topic 1

A software as a service (SaaS) based company provides a case management solution to customers A3 part of the solution. The company uses a standalone Simple Mail Transfer Protocol (SMTP) server to send email messages from an application. The application also stores an email template for acknowledgement email messages that populate customer data before the application sends the email message to the customer.

The company plans to migrate this messaging functionality to the AWS Cloud and needs to minimize operational overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplace. Store the email template in an Amazon S3 bucket. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the template. Use an SDK in the Lambda function to send the email message.
- B. Set up Amazon Simple Email Service (Amazon SES) to send email messages. Store the email template in an Amazon S3 bucket. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the template. Use an SDK in the Lambda function to send the email message.
- C. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplace. Store the email template in Amazon Simple Email Service (Amazon SES) with parameters for the customer data. Create an AWS Lambda function to call the SES template and to pass customer data to replace the parameters. Use the AWS Marketplace SMTP server to send the email message.
- D. Set up Amazon Simple Email Service (Amazon SES) to send email messages. Store the email template on Amazon SES with parameters for the customer data. Create an AWS Lambda function to call the SendTemplatedEmail API operation and to pass customer data to replace the parameters and the email destination.

Correct Answer: D

Community vote distribution

D (97%)

 **God_Is_Love** Highly Voted 2 years, 3 months ago

Selected Answer: D

SendTemplatedEmail
SendEmail
SendRawEmail are email api methods used in SES
upvoted 12 times

 **masetromain** Highly Voted 2 years, 5 months ago

Selected Answer: D

The correct answer is D.

In this solution, the company can use Amazon SES to send email messages, which will minimize operational overhead as SES is a fully managed service that handles sending and receiving email messages. The company can store the email template on Amazon SES with parameters for the customer data and use an AWS Lambda function to call the SendTemplatedEmail API operation, passing in the customer data to replace the parameters and the email destination. This solution eliminates the need to set up and manage an SMTP server on EC2 instances, which can be costly and time-consuming.

Option A and B are not correct because it requires to set up an SMTP server on EC2 instances, which is not necessary and will increase operational overhead.

Option C is not correct because it stores the email template in Amazon SES with parameters for the customer data which is not possible.
upvoted 11 times

 **Maria2023** 2 years ago

Ok, so according to chatgpt C is not correct because "Option C is not correct because it stores the email template in Amazon SES with

parameters for the customer data which is not possible."

However, D says exactly the same - so D is not correct as well?

Do not fully trust chatgp

upvoted 7 times

 **titi_r** 1 year, 3 months ago

ChatGPT also is saying "Option A and B are not correct because it requires to set up an SMTP server on EC2 instances", but those options are "A" and "C", not "A" and "B". Seems there is some mismatch with the options.

upvoted 2 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: D

Option D is correct because it uses Amazon SES, a fully managed and cost-effective service for sending emails. Email templates are stored and rendered within SES, removing the need to manage custom logic for merging data. A simple Lambda function calls the SendTemplatedEmail API to inject customer data and destination info. This solution is entirely serverless, reducing operational overhead and infrastructure cost to a minimum.

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: D

Option D

upvoted 1 times

 **SK_Tyagi** 1 year, 10 months ago

Selected Answer: D

D - Can send templated email with request parameters

upvoted 1 times

 **Jonalb** 1 year, 11 months ago

Selected Answer: D

DDDDDDDD

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: D

its a d

upvoted 1 times

 **Maria2023** 2 years 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 year, 10 months ago

https://docs.aws.amazon.com/ses/latest/APIReference-V2/API_CreateEmailTemplate.html

upvoted 1 times

 **pk0619** 1 year ago

There can be variables in the template.

upvoted 1 times

 **carpa_jo** 1 year, 6 months ago

D is correct.

Regarding your concerns about email templates on SES with parameters see: <https://docs.aws.amazon.com/ses/latest/dg/send-personalized-email-api.html>

upvoted 1 times

 **SkyZeroZx** 2 years ago

Selected Answer: D

keyword = SendTemplatedEmail API

upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: D

Template - easy one.

upvoted 1 times

 **zozza2023** 2 years, 5 months ago

Selected Answer: D

D should be the answer

upvoted 3 times

 **zhangyu20000** 2 years, 5 months ago

D is correct - https://docs.aws.amazon.com/ses/latest/APIReference/API_SendTemplatedEmail.html

upvoted 2 times

Question #141

A company is processing videos in the AWS Cloud by Using Amazon EC2 instances in an Auto Scaling group. It takes 30 minutes to process a video. Several EC2 instances scale in and out depending on the number of videos in an Amazon Simple Queue Service (Amazon SQS) queue.

The company has configured the SQS queue with a redrive policy that specifies a target dead-letter queue and a maxReceiveCount of 1. The company has set the visibility timeout for the SQS queue to 1 hour. The company has set up an Amazon CloudWatch alarm to notify the development team when there are messages in the dead-letter queue.

Several times during the day, the development team receives notification that messages are in the dead-letter queue and that videos have not been processed properly. An investigation finds no errors in the application logs.

How can the company solve this problem?

- A. Turn on termination protection for the EC2 Instances
- B. Update the visibility timeout for the SQS queue to 3 hours
- C. Configure scale-in protection for the instances during processing
- D. Update the redrive policy and set maxReceiveCount to 0.

Correct Answer: C*Community vote distribution*

C (70%)

D (27%)

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: C

The correct answer is C. The company can solve the problem by configuring scale-in protection for the instances during processing. This will ensure that the instances are not terminated while they are processing videos. This will prevent the messages from moving to the dead-letter queue and ensure that videos are processed properly.

Option A is incorrect because turning on termination protection for the EC2 instances will not solve the problem as it will impact the ability of the Auto Scaling group to scale instances in and out based on the number of videos in the queue.

Option B is incorrect because the company has specified a visibility timeout of 1 hour, which is enough time for the instances to process a video and there is no need to update the timeout to 3 hours.

Option D is incorrect because the company has set the maxReceiveCount to 1 and changing it to 0 will not solve the problem. maxReceiveCount allowed range is 1 to 1000.

upvoted 28 times

 **Bwutch** 2 years, 7 months ago

ChatGPT confirms this reasoning.

upvoted 10 times

 **dev112233xx** Highly Voted 2 years, 7 months 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 7 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: C

The correct answer is C, because the problem is caused by EC2 instances being terminated by Auto Scaling while processing a message, before the message can be deleted from the SQS queue. This causes the message to reappear and immediately go to the dead-letter queue due to maxReceiveCount = 1. Applying scale-in protection during processing ensures the instance is not terminated mid-task, preventing message loss.

upvoted 1 times

 **Jorkaef** 1 year, 1 month ago

Correct is C:

B. 3-hour visibility timeout

Too long for 30-minute processing
 Could delay reprocessing of failed messages

Doesn't address root cause

C. Scale-in protection during processing

Prevents instance termination while processing

Allows message processing to complete

Prevents message return to queue

Stops premature scale-in

✓ CORRECT

upvoted 1 times

 **Jorkaef** 1 year, 1 month ago

B is correct;

updating the visibility timeout to 3 hours (option B) is the most appropriate solution as it gives enough time for the messages to be processed without being prematurely marked as failures.

upvoted 1 times

 **trungtd** 1 year, 6 months ago

Selected Answer: D

D is a typo

upvoted 1 times

 **VerRi** 1 year, 10 months ago

Selected Answer: D

If Option D is a typo, then D

upvoted 2 times

 **Greanny** 1 year, 11 months ago

B.

The best solution for this problem is to update the visibility timeout for the SQS queue to 3 hours. This is because when the visibility timeout is set to 1 hour, it means that if the EC2 instance doesn't process the message within an hour, it will be moved to the dead-letter queue. By increasing the visibility timeout to 3 hours, this should give the EC2 instance enough time to process the message before it gets moved to the dead-letter queue. Additionally, configuring scale-in protection for the EC2 instances during processing will help to ensure that the instances are not terminated while the messages are being processed.

upvoted 3 times

 **tmlong18** 1 year, 11 months ago

Selected Answer: D

Option D is a typo.

I seen the same question in udemy but the Option D is 10

upvoted 4 times

 **career360guru** 2 years ago

Selected Answer: C

Option C is correct.

upvoted 2 times

 **severlight** 2 years, 1 month ago

Selected Answer: C

setting MaxReceiveCount to 0 doesn't make and send and it impossible, because messages would be send to DLQ without any attempt to consume them from source queue

upvoted 1 times

 **Russ99** 2 years, 3 months ago

Selected Answer: D

checked 4 AI, 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** 2 years, 3 months 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 6 times
```

✉ **SK_Tyagi** 2 years, 4 months ago

Selected Answer: C

Going with C only because D has value of maxReceiveCount set to 0

upvoted 2 times

✉ **rtguru** 2 years, 5 months ago

I go with C

upvoted 1 times

✉ **YodaMaster** 2 years, 5 months ago

Selected Answer: B

B.

AWS "recommends setting your queue's visibility timeout to six times your function timeout" which makes 3 hours perfect.

source: <https://docs.aws.amazon.com/lambda/latest/dg/with-sqs.html>

upvoted 2 times

✉ **ajeeshb** 1 year, 9 months ago

But this for a queue to use with lambda. Here it is EC2 in ASG

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C more likely

upvoted 1 times

Question #142

Topic 1

A company has developed APIs that use Amazon API Gateway with Regional endpoints. The APIs call AWS Lambda functions that use API Gateway authentication mechanisms. After a design review, a solutions architect identifies a set of APIs that do not require public access.

The solutions architect must design a solution to make the set of APIs accessible only from a VPC. All APIs need to be called with an authenticated user

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

- A. Create an internal Application Load Balancer (ALB). Create a target group. Select the Lambda function to call. Use the ALB DNS name to call the API from the VPC.
- B. Remove the DNS entry that is associated with the API in API Gateway. Create a hosted zone in Amazon Route 53. Create a CNAME record in the hosted zone. Update the API in API Gateway with the CNAME record. Use the CNAME record to call the API from the VPC.
- C. Update the API endpoint from Regional to private in API Gateway. Create an interface VPC endpoint in the VPC. Create a resource policy, and attach it to the API. Use the VPC endpoint to call the API from the VPC.
- D. Deploy the Lambda functions inside the VPC. Provision an EC2 instance, and install an Apache server. From the Apache server, call the Lambda functions. Use the internal CNAME record of the EC2 instance to call the API from the VPC.

Correct Answer: C

Community vote distribution

C (100%)

 **bjexamprep**  2 years ago

Selected Answer: C

Bad question design. None of the answers is correct.

None of the answers mentions how to satisfy the requirement of "All APIs need to be called with an authenticated user".

Another requirement "make the set of APIs accessible only from a VPC". "the set" doesn't mean the whole set. Here "the set" means a part of the whole set.

A: The set of APIs are still publicly accessible.

B: Removing DNS entry doesn't remove the public accessibility.

C: This is making the whole set of APIs private. If this answer can be specific to "the set" APIs, this could be a good answer.

D: Using EC2 instances is always a bad answer.

upvoted 12 times

 **altonh** 11 months, 2 weeks ago

Agree. The proper solution should be:

Create a new private API GW and move those private APIs to this newly created API GW.

upvoted 1 times

 **toma** 1 year, 6 months ago

there is only set of APIs that do not require public access, you dont need all APIs private access? so it could be that the answer is A?

upvoted 2 times

 **zozza2023**  2 years, 11 months ago

Selected Answer: C

should be C as on the question has said 'no need for public IP' ==> private in API gateway = VPC endpoint

upvoted 9 times

 **princajen**  4 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Changing the API Gateway endpoint type to private, and then accessing it via a VPC interface endpoint (PrivateLink), ensures the API is only accessible from within the VPC. A resource policy limits access, and API Gateway authentication is still supported. This approach meets all the requirements with minimal changes and lowest management overhead.

upvoted 1 times

 **AimarLeo** 1 year, 11 months ago

All given answers are not ideal.. the closest one is C BUT.. .when mentioning the requirement to have only 'a set of API to be private' means 'not all'.. turning the endpoint from public to private will turn all to Private , which is not fully correct as per the question.. I suppose the given answer or question missing an info.. or AWS starts playing with AI

upvoted 3 times

 **carpa_jo** 1 year, 12 months ago

Selected Answer: C

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html>

upvoted 1 times

✉ **career360guru** 2 years ago

Selected Answer: C

Option C

upvoted 1 times

✉ **venvig** 2 years, 3 months ago

Selected Answer: C

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

upvoted 1 times

✉ **Explorer_30** 2 years, 3 months ago

Answer is C as explain in <https://repost.aws/knowledge-center/api-gateway-vpc-connections>

upvoted 1 times

✉ **SK_Tyagi** 2 years, 4 months ago

Selected Answer: C

Regional to Private fits the use-case

upvoted 1 times

✉ **rtguru** 2 years, 5 months ago

the best possible answer from all the options is C

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

it's C, although it begs the questions about APIs that need to stay public...

upvoted 2 times

✉ **mfsec** 2 years, 9 months ago

Selected Answer: C

C. Update the API endpoint from Regional to private in API Gateway.

upvoted 1 times

✉ **masetromain** 2 years, 11 months ago

Selected Answer: C

The correct answer is C. Update the API endpoint from Regional to private in API Gateway. Create an interface VPC endpoint in the VPC. Create a resource policy, and attach it to the API. Use the VPC endpoint to call the API from the VPC.

This solution will meet the requirements with the least amount of effort because it utilizes the built-in features of API Gateway and VPC to restrict access to the API. With this method, no additional infrastructure or configurations are necessary.

A and B are not correct because they would require additional infrastructure and configurations.

D is not correct because it would require provisioning an EC2 instance and installing an Apache server, introducing additional complexity and management overhead.

upvoted 5 times

✉ **zhangyu20000** 2 years, 11 months ago

C is correct

upvoted 1 times

Question #143

A weather service provides high-resolution weather maps from a web application hosted on AWS in the eu-west-1 Region. The weather maps are updated frequently and stored in Amazon S3 along with static HTML content. The web application is fronted by Amazon CloudFront.

The company recently expanded to serve users in the us-east-1 Region, and these new users report that viewing their respective weather maps is slow from time to time.

Which combination of steps will resolve the us-east-1 performance issues? (Choose two.)

- A. Configure the AWS Global Accelerator endpoint for the S3 bucket in eu-west-1. Configure endpoint groups for TCP ports 80 and 443 in us-east-1.
- B. Create a new S3 bucket in us-east-1. Configure S3 cross-Region replication to synchronize from the S3 bucket in eu-west-1.
- C. Use Lambda@Edge to modify requests from North America to use the S3 Transfer Acceleration endpoint in us-east-1.
- D. Use Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1.
- E. Configure the AWS Global Accelerator endpoint for us-east-1 as an origin on the CloudFront distribution. Use Lambda@Edge to modify requests from North America to use the new origin.

Correct Answer: BD

Community vote distribution

BD (96%)	2%
----------	----

 **sambb** Highly Voted 2 years, 9 months 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 19 times

 **masetromain** Highly Voted 2 years, 11 months ago

Selected Answer: BD

B is correct because it involves creating a new S3 bucket in the us-east-1 region and configuring cross-Region replication to synchronize from the existing S3 bucket in eu-west-1. This will allow users in us-east-1 to access the weather maps from a closer location, improving performance.

D is correct because it involves using Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1. This will also allow users in us-east-1 to access the weather maps from a closer location, improving performance.

A and E are not correct because they do not involve creating a new S3 bucket in us-east-1, which is necessary for improving performance for the users in that region. C is not correct because it involves using the S3 Transfer Acceleration endpoint, which is a different service and not necessary for this scenario.

upvoted 8 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: BD

The best solution is to:

- (B) Set up an S3 bucket in us-east-1 with Cross-Region Replication from the primary S3 bucket in eu-west-1. This brings the data physically closer to the new users.
- (D) Use Lambda@Edge to route requests from North America to the us-east-1 S3 bucket, reducing latency and improving performance.

This combination avoids invalid services (like Global Accelerator for S3) and leverages CloudFront and regional S3 data for optimal speed and availability.v

upvoted 1 times

 **ahhatem** 1 year ago

Selected Answer: BD

Although, D is not really correct. You should be using "s3 multi-region access point". It is designed specifically for this scenario.

upvoted 1 times

 **altonh** 11 months, 2 weeks ago

The correct answer implies a CloudFront with multiple origins, i.e. pointing to two (2) S3 buckets and using Lambda@Edge to decide which origin to go to.

upvoted 1 times

 **pangchn** 1 year, 8 months ago

Selected Answer: BD

BD

C using S3 Transfer Acceleration is good but this answer option itself is wrong due to the statement that pointing to a regional endpoint, where it doesn't exist. Once enable, it is just a global endpoint URL

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration-examples.html>

upvoted 1 times

 **jpa8300** 1 year, 11 months ago

Selected Answer: AC

If you want to improve latency , you always look for Global Accelerator fro the readings and Transfer accelerator for the updates.

Yes, it is possible to configure AWS Global Accelerator to distribute traffic from an S3 bucket in one AWS Region (eu-west-1) to endpoint groups in another AWS Region (us-east-1) for TCP ports 80 and 443. This configuration can be useful for improving the performance and availability of your S3 bucket for users in both regions.

This way you save money in the storage, you don't need to duplicate the storage. And for persons that chose option D, if you update the bucket there, those objects will not be replicated to the other region since replication works only in one way.

upvoted 1 times

 **helloworldabc** 1 year, 3 months ago

just BD

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: BD

Option B & D

upvoted 1 times

 **bjexamprep** 2 years ago

Selected Answer: BD

This is not a good question design. Does that mean the application use CloudFront in EU and does not use CloudFront in the US? How weird it is!!!

upvoted 3 times

 **Jrhp** 2 years ago

Selected Answer: BD

Exactly case from this blog post <https://aws.amazon.com/blogs/networking-and-content-delivery/dynamically-route-viewer-requests-to-any-origin-using-lambdaedge/>

upvoted 4 times

 **rtguru** 2 years, 5 months ago

BD, I was initially looking at BE, I think global accelerator is used more for write requests.

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: BD

BD makes more sense

upvoted 2 times

 **SmileyCloud** 2 years, 5 months ago

Selected Answer: BD

<https://godof.cloud/dynamic-origin-s3-spa/>

Use case

upvoted 1 times

 **Eshu2009** 2 years, 9 months ago

BE- global accelerators improve performance by providing edge location for onboarding traffic.

upvoted 3 times

 **Eshu2009** 2 years, 9 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 2 times

 **mfsec** 2 years, 9 months ago

Selected Answer: BD

I'll go with BD

upvoted 1 times

 **kiran15789** 2 years, 10 months ago

Selected Answer: BD

Since only one additional region we don't need global accelerators

upvoted 5 times

 **bititan** 2 years, 10 months ago

Selected Answer: BC

S3 transfer acceleration is more efficient

upvoted 1 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: BD

A and E are not correct as there isn't a need to use aws global accel

upvoted 2 times

Question #144

A solutions architect is investigating an issue in which a company cannot establish new sessions in Amazon Workspaces. An initial analysis indicates that the issue involves user profiles. The Amazon Workspaces environment is configured to use Amazon FSx for Windows File Server as the profile share storage. The FSx for Windows File Server file system is configured with 10 TB of storage.

The solutions architect discovers that the file system has reached its maximum capacity. The solutions architect must ensure that users can regain access. The solution also must prevent the problem from occurring again.

Which solution will meet these requirements?

- A. Remove old user profiles to create space. Migrate the user profiles to an Amazon FSx for Lustre file system.
- B. Increase capacity by using the update-file-system command. Implement an Amazon CloudWatch metric that monitors free space. Use Amazon EventBridge to invoke an AWS Lambda function to increase capacity as required.
- C. Monitor the file system by using the FreeStorageCapacity metric in Amazon CloudWatch. Use AWS Step Functions to increase the capacity as required.
- D. Remove old user profiles to create space. Create an additional FSx for Windows File Server file system. Update the user profile redirection for 50% of the users to use the new file system.

Correct Answer: B*Community vote distribution*

B (89%)

8%

 **God_Is_Love**  2 years, 3 months 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 8 times

 **masetromain**  2 years, 5 months ago

Selected Answer: B

B is correct. It can prevent the issue from happening again by monitoring the file system with the FreeStorageCapacity metric in Amazon CloudWatch and using Amazon EventBridge to invoke an AWS Lambda function to increase the capacity as required. This ensures that the file system always has enough free space to store user profiles and avoids reaching maximum capacity.
 A: Removing old user profiles may not be sufficient to create enough space and does not prevent the problem from happening again.
 C: AWS Step Functions cannot be used to increase capacity, it is a service for creating and running workflows that stitch together multiple AWS services.
 D: Creating an additional FSx for Windows File Server file system and updating user profile redirection for a portion of the users may not be sufficient to prevent the problem from happening again and does not address the current capacity issue.
 upvoted 8 times

 **princajen**  4 months, 3 weeks ago

Selected Answer: B

Option B is correct because it solves both parts of the problem:

Short term: Use the update-file-system API to increase FSx storage and restore access for WorkSpaces users.
 Long term: Monitor the FreeStorageCapacity CloudWatch metric, and use Amazon EventBridge to trigger a Lambda function that automatically scales storage when thresholds are breached.

This is a scalable, cost-effective, and AWS-native solution with minimal management overhead.

upvoted 1 times

 **sse69** 1 year, 1 month ago

Selected Answer: B

Wouldn't you need a cloudwatch alarm that would trigger a Lambda based on the metric going above a certain threshold?
 Metric -> Lambda is a bit of a shortcut
 upvoted 1 times

 **red_panda** 1 year, 1 month ago

Selected Answer: D

It's D.
 Option B Simply do not prevent problem to happen again. It's not possible to resize the FSx Size after creation so option D is more suitable.
 upvoted 1 times

career360guru 1 year, 6 months ago

Selected Answer: B

Option B

upvoted 1 times

rtguru 1 year, 11 months ago

B is the correct answer

upvoted 1 times

NikkyDicky 1 year, 11 months ago

Selected Answer: B

it's B

upvoted 1 times

SkyZeroZx 2 years ago

Selected Answer: B

keyword == update-file-system

upvoted 1 times

leehjworking 2 years, 1 month 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 2 years ago

Perhaps the metric is used to trigger the step functions

upvoted 1 times

OCHT 2 years, 1 month 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 2 times

rbm2023 2 years, 1 month 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 5 times

yama234 2 years, 1 month 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 2 years, 2 months ago

Selected Answer: B

<https://chat.openai.com/chat>

upvoted 2 times

mfsec 2 years, 3 months ago

Selected Answer: B

B is correct

upvoted 2 times

zozza2023 2 years, 5 months ago

Selected Answer: B

B seems to be the correct answer.

the unique possible solution is to add storage capacity using CLI

upvoted 4 times

pitakk 2 years, 5 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 3 times

 **zhangyu20000** 2 years, 5 months ago

B is correct. It can prevent issue happen again with EventBridge and Lambda

A: not make sense at all

C: Cannot use Step Function to increase capacity

D: not prevent happen again

upvoted 2 times

Question #145

An international delivery company hosts a delivery management system on AWS. Drivers use the system to upload confirmation of delivery. Confirmation includes the recipient's signature or a photo of the package with the recipient. The driver's handheld device uploads signatures and photos through FTP to a single Amazon EC2 instance. Each handheld device saves a file in a directory based on the signed-in user, and the file name matches the delivery number. The EC2 instance then adds metadata to the file after querying a central database to pull delivery information. The file is then placed in Amazon S3 for archiving.

As the company expands, drivers report that the system is rejecting connections. The FTP server is having problems because of dropped connections and memory issues in response to these problems, a system engineer schedules a cron task to reboot the EC2 instance every 30 minutes. The billing team reports that files are not always in the archive and that the central system is not always updated.

A solutions architect needs to design a solution that maximizes scalability to ensure that the archive always receives the files and that systems are always updated. The handheld devices cannot be modified, so the company cannot deploy a new application.

Which solution will meet these requirements?

- A. Create an AMI of the existing EC2 instance. Create an Auto Scaling group of EC2 instances behind an Application Load Balancer. Configure the Auto Scaling group to have a minimum of three instances.
- B. Use AWS Transfer Family to create an FTP server that places the files in Amazon Elastic File System (Amazon EFS). Mount the EFS volume to the existing EC2 instance. Point the EC2 instance to the new path for file processing.
- C. Use AWS Transfer Family to create an FTP server that places the files in Amazon S3. Use an S3 event notification through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function. Configure the Lambda function to add the metadata and update the delivery system.
- D. Update the handheld devices to place the files directly in Amazon S3. Use an S3 event notification through Amazon Simple Queue Service (Amazon SQS) to invoke an AWS Lambda function. Configure the Lambda function to add the metadata and update the delivery system.

Correct Answer: C*Community vote distribution*

C (76%)

B (24%)

 **masetromain**  2 years, 5 months ago

Selected Answer: C

C is correct. Using AWS Transfer Family to create an FTP server that places the files in Amazon S3 and using S3 event notifications through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function will ensure that the archive always receives the files and that the central system is always updated. This solution maximizes scalability and eliminates the need for manual intervention, such as rebooting the EC2 instance.

Option A and B still use EC2 instance, which is the source of the problem. Option D requires modification to the handheld devices which is not possible.

upvoted 15 times

 **venvig**  1 year, 10 months 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 7 times

 **kgcain** 1 year, 8 months ago

From the app description, I am sure that it should work under 15min.

upvoted 1 times

 **pk0619** 1 year ago

they had to reboot the ec2 because of memory, without scaling EC2 they will still have that problem and since B does nothing about adding more memory, it cannot be right choice.

upvoted 1 times

 **pk0619** 1 year ago

Actually offloading FTP from EC2 might eliminate memory issue, so it could very well be B as well

upvoted 1 times

 **gofavad926** 1 year, 3 months ago

the text is: "The handheld devices cannot be modified, so the company cannot deploy a new application". Following your comment, you can't use neither the AWS Transfer Family. This is also new :D

upvoted 2 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: C

Why C wins: Serverless, durable, and scalable. Transfer Family preserves FTP, S3 ensures durability, SNS+Lambda handles processing & DB updates automatically. Removes EC2 as a bottleneck.

Why B is debated: Only good if you interpret "no new app" as no new backend components, but it leaves EC2 scaling/risk issues in place.

upvoted 1 times

 **EApeer** 1 year, 3 months ago

B is the best answer. The system is such that each handheld device saves a file in a directory based on the signed-in user, and the file name matches the delivery number. This means that we need a file storage that the data are stored hierarchically in a top-down network of folders. And a file system that has adaptive throughput to resolve the dropped connections and memory issues. EFS will be the suitable solution component. S3 however has all the data stored on the same flat plane requiring more comprehensive metadata (labels) to make it manageable.

upvoted 1 times

 **kz407** 1 year, 3 months ago

Selected Answer: C

It says "so the company cannot deploy a new application".

This means that it's the handheld devices they can't deploy a new application into. While B works, It still relies on one EC2 instance, which is a part of the problem.

upvoted 1 times

 **gofavad926** 1 year, 3 months ago

Selected Answer: C

C, transfer family + S3

upvoted 1 times

 **zanhsieh** 1 year, 4 months ago

Selected Answer: C

C.

A: No. FTP is not HTTP / HTTPS. FTP -> NLB. HTTP / HTTPS -> ALB.

B: No. This needs extra steps (DataSync?) to move to S3, and the billing team would still complain about not always updated since it will be certain lag-behind time.

C: Correct.

D: No. S3 event notification can directly trigger Lambda.

upvoted 2 times

 **JMAN1** 1 year, 6 months ago

Selected Answer: C

C. does not require handheld device to be changed. And it solves EC2 dropped Connection by using S3.

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: C

Option C

upvoted 1 times

 **Chung234** 1 year, 8 months ago

Selected Answer: B

The answer is A.

Q: Can I use FTP with an internet-facing endpoint?

A: No, when you enable FTP, you will only be able to use VPC hosted endpoint's internal access option. If traffic needs to traverse the public network, secure protocols such as SFTP or FTPS should be used.

Source: <https://aws.amazon.com/aws-transfer-family/faqs/>

upvoted 3 times

✉ **ele** 1 year, 3 months ago

ALB is a load balancer that operates at Layer 7. Only HTTP and HTTPS can be used as ALB protocols.

Therefore, it is not possible to set ALB at the front of the FTP server.

upvoted 1 times

✉ **rtguru** 1 year, 11 months ago

This one of those tricky questions. I'm not sure if to go with A or C

upvoted 1 times

✉ **rrrrrrrrr1** 1 year, 11 months ago

IDK yall, it does say clearly "cannot deploy a new application" and the only instance of that is A.

I Agree C is better but IDK the semantics here

upvoted 1 times

✉ **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

its a c

upvoted 1 times

✉ **Maria2023** 2 years 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** 2 years 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** 2 years, 3 months ago

Selected Answer: C

C is the most efficient

upvoted 3 times

✉ **zozza2023** 2 years, 5 months ago

Selected Answer: C

C is correct

upvoted 3 times

Question #146

A company is running an application in the AWS Cloud. The application runs on containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The ECS tasks use the Fargate launch type. The application's data is relational and is stored in Amazon Aurora MySQL. To meet regulatory requirements, the application must be able to recover to a separate AWS Region in the event of an application failure. In case of a failure, no data can be lost.

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

- A. Provision an Aurora Replica in a different Region.
- B. Set up AWS DataSync for continuous replication of the data to a different Region.
- C. Set up AWS Database Migration Service (AWS DMS) to perform a continuous replication of the data to a different Region.
- D. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule a snapshot every 5 minutes.

Correct Answer: A*Community vote distribution*

A (100%)

 **masetromain** Highly Voted 2 years, 5 months ago

Selected Answer: A

A is correct. Provision an Aurora Replica in a different Region will meet the requirement of the application being able to recover to a separate AWS Region in the event of an application failure, and no data can be lost, with the least amount of operational overhead.

- B. AWS DataSync can replicate data, but it is not a fully managed service and requires more configuration and management.
- C. AWS DMS is a fully managed service for migrating data between databases, but it may require additional configuration and management to continuously replicate data in real-time.
- D. Amazon DLM can be used for scheduling snapshots, but it does not provide real-time replication and may not meet the requirement of no data loss in case of a failure.

upvoted 8 times

 **princajen** Most Recent 4 months, 3 weeks ago

Selected Answer: A

Use Aurora cross-Region replica to meet DR and compliance needs with the least operational work. Fully managed, promotes quickly on failover, and minimizes replication lag. Other options either don't support Aurora replication, require more management, or allow potential data loss.

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: A

Option A

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: A

its an A

upvoted 2 times

 **Goatin** 2 years, 1 month ago

When you provision an Aurora Replica in a different AWS Region, the replica is kept in sync with the primary database using Aurora's replication capabilities. In the event of a failure in the primary Region, you can promote the Aurora Replica to become the new primary database, which allows you to continue operations with no data loss.

However, provisioning and maintaining an Aurora Replica in a different AWS Region requires ongoing management and monitoring to ensure that it stays in sync with the primary database

upvoted 3 times

 **mfsec** 2 years, 3 months ago

Selected Answer: A

Replica

upvoted 4 times

 **God_Is_Love** 2 years, 3 months 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** 2 years, 5 months ago

Selected Answer: A

A is correct

upvoted 4 times

 **zhangyu20000** 2 years, 5 months ago

A is correct

B: cannot use DataSync for Aurora backup

C: too complex

D: DLM is for EBS backup. Here use managed Aurora server, no access to EBS

upvoted 2 times

Question #147

A financial services company receives a regular data feed from its credit card servicing partner. Approximately 5,000 records are sent every 15 minutes in plaintext, delivered over HTTPS directly into an Amazon S3 bucket with server-side encryption. This feed contains sensitive credit card primary account number (PAN) data. The company needs to automatically mask the PAN before sending the data to another S3 bucket for additional internal processing. The company also needs to remove and merge specific fields, and then transform the record into JSON format. Additionally, extra feeds are likely to be added in the future, so any design needs to be easily expandable.

Which solutions will meet these requirements?

- A. Invoke an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Invoke another Lambda function when new messages arrive in the SQS queue to process the records, writing the results to a temporary location in Amazon S3. Invoke a final Lambda function once the SQS queue is empty to transform the records into JSON format and send the results to another S3 bucket for internal processing.
- B. Invoke an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Configure an AWS Fargate container application to automatically scale to a single instance when the SQS queue contains messages. Have the application process each record, and transform the record into JSON format. When the queue is empty, send the results to another S3 bucket for internal processing and scale down the AWS Fargate instance.
- C. Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table definition to match. Invoke an AWS Lambda function on file delivery to start an AWS Glue ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, have the ETL job send the results to another S3 bucket for internal processing.
- D. Create an AWS Glue crawler and custom classifier based upon the data feed formats and build a table definition to match. Perform an Amazon Athena query on file delivery to start an Amazon EMR ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, send the results to another S3 bucket for internal processing and scale down the EMR cluster.

Correct Answer: C

Community vote distribution

C (100%)

 **God_Is_Love** Highly Voted  2 years, 3 months 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 21 times

 **tycho** 2 years, 2 months ago

EMR and Glue are the same; Glue is managed cluster by AWS , EMR customer manages the clutster
upvoted 2 times

 **masetromain** Highly Voted  2 years, 5 months ago

Selected Answer: C

C is correct. It will process the data in batch mode using Glue ETL job which can handle large amount of data and can be scheduled to run periodically. This solution is also easily expandable for future feeds.

A: It uses multiple Lambda functions, SQS queue and S3 temporary location which will increase operational overhead.
B: Using Fargate may not be the most cost-effective solution and also it may not handle large amount of data.
D: Athena and EMR both are powerful tools but they are more complex and can be more costly than Glue.
upvoted 7 times

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

Selected Answer: C

When you need to process and transform sensitive batch data from S3 (mask, remove fields, reformat) and make it scalable for future feeds, AWS Glue is ideal. It's serverless, integrates natively with S3, and supports complex ETL in a single managed job. Avoid multi-step Lambda/SQS/Fargate setups unless streaming or ultra-low latency is required, and avoid EMR unless big data scale or specialized frameworks are needed.

upvoted 1 times

✉️ **career360guru** 1 year, 6 months ago

Selected Answer: C

Option C

upvoted 1 times

✉️ **totten** 1 year, 8 months ago

Selected Answer: C

Option C is the most suitable solution for the described scenario:

1) AWS Glue Crawler and Custom Classifier: Use AWS Glue to create a crawler and custom classifier to understand and catalogue the data feed formats. This step ensures that AWS Glue can work with the incoming data effectively.

2) AWS Glue ETL Job: Create an AWS Lambda function that triggers an AWS Glue ETL job when a new data file is delivered. This ETL job can perform the required transformation, including masking, field removal, and converting records to JSON format. AWS Glue is a suitable service for data preparation and transformation.

3) Output to S3 Bucket.

This approach is scalable, easily expandable to handle additional feeds in the future, and leverages AWS Glue's capabilities for data transformation and processing. It also maintains a clear separation of tasks, making it a robust and efficient solution for the given requirements.

upvoted 3 times

✉️ **dkclougdguru** 1 year, 9 months ago

C is the good option EMR(Big data, Spark, Hadoop) is for near real-time data processing and it isn't a good fit in this case

upvoted 1 times

✉️ **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

its a C

upvoted 1 times

✉️ **SkyZeroZx** 2 years 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** 2 years, 3 months ago

Selected Answer: C

C makes the most sense.

upvoted 2 times

✉️ **Musk** 2 years, 4 months ago

The question is at what point Athena and EMR are a better choice because it is a lot of data to store and process

upvoted 1 times

✉️ **Sarutobi** 2 years, 3 months ago

That, I agree. Honestly, I will use it from day one, regardless.

upvoted 1 times

✉️ **zozza2023** 2 years, 5 months ago

Selected Answer: C

C is correct.

upvoted 4 times

✉️ **zhangyu20000** 2 years, 5 months ago

C is correct

upvoted 1 times

Question #148

Topic 1

A company wants to use AWS to create a business continuity solution in case the company's main on-premises application fails. The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store. All the company's on-premises applications use operating systems that are compatible with Amazon EC2.

Which solution will achieve the company's goal with the LEAST operational overhead?

- A. Install the AWS Replication Agent on the source servers, including the MySQL servers. Set up replication for all servers. Launch test instances for regular drills. Cut over to the test instances to fail over the workload in the case of a failure event.
- B. Install the AWS Replication Agent on the source servers, including the MySQL servers. Initialize AWS Elastic Disaster Recovery in the target AWS Region. Define the launch settings. Frequently perform failover and fallback from the most recent point in time.
- C. Create AWS Database Migration Service (AWS DMS) replication servers and a target Amazon Aurora MySQL DB cluster to host the database. Create a DMS replication task to copy the existing data to the target DB cluster. Create a local AWS Schema Conversion Tool (AWS SCT) change data capture (CDC) task to keep the data synchronized. Install the rest of the software on EC2 instances by starting with a compatible base AMI.
- D. Deploy an AWS Storage Gateway Volume Gateway on premises. Mount volumes on all on-premises servers. Install the application and the MySQL database on the new volumes. Take regular snapshots. Install all the software on EC2 Instances by starting with a compatible base AMI. Launch a Volume Gateway on an EC2 instance. Restore the volumes from the latest snapshot. Mount the new volumes on the EC2 instances in the case of a failure event.

Correct Answer: B

Community vote distribution

B (81%)

C (19%)

✉️  **God_Is_Love**  2 years, 3 months 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-fallback-arc.png>

<https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html>

upvoted 27 times

✉️  **God_Is_Love** 2 years, 3 months ago

Moreover, B has least operational overhead of just initiating DR solution with replicating agents. C has operational overhead with DMS , SCT ,CDC,migration etc

upvoted 4 times

✉️  **swadeey** 1 year, 6 months ago

I also agreed with the answer but then see this "The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store" just database and physical server has other applications which not mentioned. Also from DR the statement gets changed to Migrate

upvoted 3 times

✉️  **Untamables**  2 years, 5 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 7 times

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

Selected Answer: B

For lift-and-shift disaster recovery of on-premises workloads (including databases) to AWS with minimal operational overhead, use AWS Elastic Disaster Recovery (AWS DRS). Install the AWS Replication Agent, configure launch settings, and AWS keeps a low-cost replica up to date. At failover, instances launch quickly in AWS without manual rebuilds. Avoid DMS or Storage Gateway unless you only need DB sync or file-level DR.

upvoted 1 times

✉️  **jimee11** 7 months, 3 weeks ago

Selected Answer: B

Poorly worded question. AWS DMS makes sense if we were just migrating the Mysql Database. Since we are migrating the database AND application - we use AWS Replication Agent to migrate the entire server.

upvoted 1 times

 **altonh** 11 months, 2 weeks ago

Selected Answer: C

The answer should be C.

Take note of the statement, "The application runs on physical servers that also run other applications". If you use the Application Migration Service, you will migrate these other applications, which have nothing to do with the application you are trying to protect.

upvoted 2 times

 **ninomfr64** 1 year, 5 months ago

Selected Answer: B

A = to use AWS DRS you first need to set it up in each AWS Region in which you want to use it. installing AWS Replication agent is not enough

B = correct (to me the sentence "Frequently perform failover and fallback from the most recent point in time" is ambiguous as this points to actual failover/fallback and not to drills)

C = SCT is not needed wwith same engine db migration. also, install the rest of the software is not enough for app DR

D = Volume Gateway can be used in a Back and Restore DR scenario, but the option D is very confused. Anyway, Storage Gateway for DR requires more overhead with respect to AWS DRS

upvoted 4 times

 **career360guru** 1 year, 6 months ago

Selected Answer: B

Option B is right option.

Option C only addresses DB instance replication and DR, it does not meet requirements of replicating other applications running on on-premise.

upvoted 1 times

 **swadeey** 1 year, 6 months ago

Selected answer C changed from B

The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store.

upvoted 1 times

 **severlight** 1 year, 7 months ago

Selected Answer: B

Elastic Disaster Recovery does the job

upvoted 1 times

 **AMohanty** 1 year, 9 months ago

C

We are looking for a Business Continuity Solution

Meaning RTO should be low

upvoted 1 times

 **chikorita** 1 year, 9 months ago

but how is failover happening

the very own purpose of DR is its automatic failover which is supported by option B

upvoted 1 times

 **cmoreira** 1 year, 9 months 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** 1 year, 10 months ago

Selected Answer: B

the question is a bit misleading, first part says "company is planning for business continuity" the later part of the sentence says "applications are migrating".

nevertheless, we should focus on the word business continuity. Going by that "no migration" is required so choose B.

that is my analysis.

upvoted 3 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: B

B for BC

upvoted 1 times

 **SkyZeroZx** 2 years ago

Selected Answer: B

keyword = AWS Elastic Disaster Recovery

B

upvoted 1 times

 **rbm2023** 2 years, 1 month 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** 2 years, 1 month 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** 2 years, 2 months ago

Selected Answer: C

C seems correct to me (DMS with SCT and CDC)

upvoted 1 times

Question #149

Topic 1

A company is subject to regulatory audits of its financial information. External auditors who use a single AWS account need access to the company's AWS account. A solutions architect must provide the auditors with secure, read-only access to the company's AWS account. The solution must comply with AWS security best practices.

Which solution will meet these requirements?

- A. In the company's AWS account, create resource policies for all resources in the account to grant access to the auditors' AWS account. Assign a unique external ID to the resource policy.
- B. In the company's AWS account, create an IAM role that trusts the auditors' AWS account. Create an IAM policy that has the required permissions. Attach the policy to the role. Assign a unique external ID to the role's trust policy.
- C. In the company's AWS account, create an IAM user. Attach the required IAM policies to the IAM user. Create API access keys for the IAM user. Share the access keys with the auditors.
- D. In the company's AWS account, create an IAM group that has the required permissions. Create an IAM user in the company's account for each auditor. Add the IAM users to the IAM group.

Correct Answer: B*Community vote distribution*

B (100%)

  **tatdatpham** Highly Voted  2 years, 4 months ago**Selected Answer: B**

Option B is the best solution. This solution creates an IAM role that trusts the auditors' AWS account and attaches the required IAM policies to the role. This ensures that the auditors have read-only access to the company's AWS account while ensuring that the company's AWS account is secure and complies with AWS security best practices. Additionally, the unique external ID assigned to the role's trust policy adds an extra layer of security.

upvoted 7 times

  **princajen** Most Recent 4 months, 2 weeks ago**Selected Answer: B**

When granting external parties access to your AWS account, use cross-account IAM roles with a trust policy for their AWS account and an external ID to prevent the confused deputy problem. Attach least-privilege permissions (e.g., `ReadOnlyAccess`). This avoids sharing permanent credentials and aligns with AWS security best practices.

upvoted 1 times

  **duriselvan** 1 year, 4 months ago

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html

upvoted 1 times

  **duriselvan** 1 year, 4 months ago

To create an IAM role that trusts the auditors' AWS account, you can do the following:

Sign in to the AWS Management Console and open the IAM console.

In the navigation pane, choose Roles, and then choose Create role.

Choose the Custom trust policy role type.

In the Custom trust policy section, enter or paste the following trust policy:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam:<auditor-account-id>:root"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

upvoted 1 times

  **career360guru** 1 year, 6 months ago**Selected Answer: B**

Option B

upvoted 1 times

 **dkcloudguru** 1 year, 9 months ago

B is correct
upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: B
its a b
upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: B
In the company's AWS account, create an IAM role that trusts the auditors' AWS account.
upvoted 3 times

 **zozza2023** 2 years, 5 months ago

Selected Answer: B
B seems to be the right answer
upvoted 3 times

 **masetromain** 2 years, 5 months ago

Selected Answer: B
The correct answer is B. In the company's AWS account, create an IAM role that trusts the auditors' AWS account. Create an IAM policy that has the required permissions. Attach the policy to the role. Assign a unique external ID to the role's trust policy.

This solution meets the requirement of providing the external auditors with secure, read-only access to the company's AWS account while also complying with AWS security best practices. In this solution, an IAM role is created that trusts the auditors' AWS account and has an IAM policy with the required permissions attached to it. The role's trust policy should include a unique external ID for added security. This allows the external auditors to assume the role and access the resources with the permissions specified in the policy, without the need to share access keys or create individual IAM users for each auditor.

upvoted 3 times

 **masetromain** 2 years, 5 months ago

Option A is incorrect because it grants access to all resources in the company's AWS account and does not provide a way to restrict the permissions that the external auditors have.

Option C is incorrect because it creates an IAM user in the company's account and shares the API access keys with the external auditors, which is not secure and does not comply with AWS security best practices.

Option D is incorrect because it creates an IAM user in the company's account for each auditor, which would be tedious and difficult to manage for the company. It would be more secure and efficient to use an IAM role that trusts the auditors' AWS account instead of creating individual users for each auditor.

upvoted 2 times

 **zhangyu20000** 2 years, 5 months ago

B is correct
upvoted 2 times

Question #150

A company has a latency-sensitive trading platform that uses Amazon DynamoDB as a storage backend. The company configured the DynamoDB table to use on-demand capacity mode. A solutions architect needs to design a solution to improve the performance of the trading platform. The new solution must ensure high availability for the trading platform.

Which solution will meet these requirements with the LEAST latency?

- A. Create a two-node DynamoDB Accelerator (DAX) cluster. Configure an application to read and write data by using DAX.
- B. Create a three-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.
- C. Create a three-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data directly from the DynamoDB table and to write data by using DAX.
- D. Create a single-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.

Correct Answer: B*Community vote distribution*

B (92%)

8%

 **Untamables**  2 years, 11 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 19 times

 **Ganshank**  2 years, 4 months 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 13 times

 **jainparag1** 2 years, 1 month ago

Caching in DAX is always write through. Correct answer is B.

upvoted 2 times

 **frfavoreto** 2 years, 3 months 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

 **princajen**  4 months, 2 weeks ago

Selected Answer: B

For latency-sensitive read-heavy DynamoDB workloads that also require high availability, use a three-node (multi-AZ) DAX cluster and configure the application to read from DAX and write directly to DynamoDB. This ensures microsecond read latency, avoids write-through delays, and meets HA requirements.

upvoted 1 times

 **ThachNguyen** 1 year, 2 months ago

Selected Answer: B

B is Correct.

- To achieve high availability for your application, we recommend that you provision your DAX cluster with at least three nodes. Ref: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.consistency.html#DAX.consistency.nodes>

- If the request specifies eventually consistent reads (the default behavior), it tries to read the item from DAX.

- With these operations, data is first written to the DynamoDB table, and then to the DAX cluster. The operation is successful only if the data is successfully written to both the table and to DAX.

Ref: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.concepts.html#DAX.concepts.request-processing>

upvoted 1 times

✉ saggy4 1 year, 10 months ago

Selected Answer: B

DAX is cache and can only be used to read so A and C are out.

Between B and D the question says Highly Available so we will select B (three node) instead of D (single node).

So correct answer B

upvoted 5 times

✉ ninomfr64 1 year, 11 months ago

A = 2 nodes DAX is not fault-tolerant

B = correct (write-around strategy ensure lower latency)

C = write-through strategy can have higher latency

D = 1 node DAX is not fault-tolerant

upvoted 1 times

✉ career360guru 2 years ago

Selected Answer: B

Option B is the best option. Though Option A is also possible solution.

upvoted 1 times

✉ MRamos 2 years ago

Selected Answer: B

The breakpoint is latency.

You write through DAX, but for latency sensitive apps, AWS instruct write directly on DynamoDB instead on DAX.

"For applications that are sensitive to latency, writing through DAX incurs an extra network hop. So a write to DAX is a little slower than a write directly to DynamoDB. If your application is sensitive to write latency, you can reduce the latency by writing directly to DynamoDB instead. For more information, see Write-around."

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.consistency.html#DAX.consistency.strategies-for-writes>

upvoted 1 times

✉ amarbeg 2 years ago

Option A would be the least latency solution for this use case. Using a two node DAX cluster with the application reading and writing via DAX provides:

Caching of both reads and writes within the DAX cluster nodes. This eliminates the need to go directly to DynamoDB for reads and writes, reducing latency.

Redundancy with two nodes to ensure high availability of the cache.

The other options would lead to some reads or writes still going directly to DynamoDB rather than being fully served from the lower latency cached data in DAX. This could increase latency compared to option A. A single node DAX cluster would work but lacks the redundancy needed for high availability.

DAX is fully managed, in-memory cache for DynamoDB that delivers low-latency data access. By caching the entire dataset in-memory across nodes, it can serve requests much faster than going to the DynamoDB tables on every request. The AWS documentation provides more details on how to configure DAX and monitor latency metrics.

upvoted 2 times

✉ covabix879 2 years, 2 months ago

Selected Answer: A

Question only ask for High Availability, not Fault Tolerant. You need 3 nodes only for the latter. You must write through to keep data getting stale as mentioned by Ganshank. I would go with two-node cluster as strong consistency adds extra latency as number of clusters increase. So for this question best answer should be A.

upvoted 1 times

✉ dkcloudguru 2 years, 3 months ago

Option B is correct: DAX is also used for caching so it improves the performance and for production 3 nodes are strongly recommended so i'll go with B.

upvoted 2 times

✉ duriselvan 2 years, 3 months ago

<https://aws.amazon.com/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>

upvoted 1 times

✉ duriselvan 2 years, 3 months ago

sorry guys a is wrong ans: B is correct ans Important

For production usage, we strongly recommend using DAX with at least three nodes, where each node is placed in different Availability Zones. Three nodes are required for a DAX cluster to be fault-tolerant.

A DAX cluster can be deployed with one or two nodes for development or test workloads. One- and two-node clusters are not fault-tolerant, and we don't recommend using fewer than three nodes for production use. If a one- or two-node cluster encounters software or hardware errors, the cluster can become unavailable or lose cached data.

upvoted 1 times

 **duriselvan** 2 years, 3 months ago

A is Ans :

Read replicas serve two additional purposes:

Scalability. If you have a large number of application clients that need to access DAX concurrently, you can add more replicas for read-scaling. DAX spreads the load evenly across all the nodes in the cluster. (Another way to increase throughput is to use larger cache node types.)

High availability. In the event of a primary node failure, DAX automatically fails over to a read replica and designates it as the new primary. If a replica node fails, other nodes in the DAX cluster can still serve requests until the failed node can be recovered. For maximum fault tolerance, you should deploy read replicas in separate Availability Zones. This configuration ensures that your DAX cluster can continue to function, even if an entire Availability Zone becomes unavailable.

upvoted 1 times

 **AMohanty** 2 years, 3 months ago

A

Once u enable DAX you cant directly write onto or Read from Dynamo DB.

upvoted 2 times

 **ggrodskiy** 2 years, 5 months ago

Correct B.

upvoted 1 times

 **Just_Ninja** 2 years, 5 months ago

Selected Answer: B

AWS recommend 3 nodes for production workloads.

So it must B

upvoted 1 times

Question #151

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.

Correct Answer: BE*Community vote distribution*

BE (90%) 10%

 **severlight** Highly Voted 2 years, 1 month ago

Selected Answer: BE

Burstable instances let you save costs, you pay for some baseline - say 40 percent, if the instance is utilized less - credits get accumulated. So, it is good for workloads with changing CPU loads.

upvoted 10 times

 **kiran15789** Highly Voted 2 years, 10 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 5 times

 **sse69** Most Recent 1 year, 7 months ago

Uhm, S3 static website with a Python backend? Am I missing something? How can S3 interact with a backend?

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just B,E

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: BE

Option B and E

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: BE

it's BE

upvoted 3 times

 **rbm2023** 2 years, 7 months 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 4 times

 **OCHT** 2 years, 8 months 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** 2 years, 8 months 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** 2 years, 8 months 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 2 times

 **mfsec** 2 years, 9 months ago

Selected Answer: BE

BE makes the most sense here

upvoted 1 times

 **God_Is_Love** 2 years, 9 months 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 5 times

 **tatdatpham** 2 years, 10 months 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** 2 years, 11 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** 2 years, 11 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** 2 years, 11 months 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 4 times

✉ **masetromain** 2 years, 11 months 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** 2 years, 11 months 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** 2 years, 11 months 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

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.

Correct Answer: D*Community vote distribution*

D (51%)	B (43%)	3%
---------	---------	----

 **Untamables** Highly Voted 2 years, 11 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 22 times

 **zhangyu20000** Highly Voted 2 years, 11 months ago

B is correct. Compute saving plan will also cover Fargate

A: use spot instance is not reliable

CD: manually scale up DB

upvoted 12 times

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

Selected Answer: D

Going with D cuz,

1. Computing Saving Plan is cover both EC2 and Fargate

2. Manually scaling the RDS is for predictable workload and cost saving that purchase RI for the RDS

upvoted 1 times

 **jhxetc** 1 month, 1 week ago

Selected Answer: D

Option B is by far the worst answer.. I'm a little worried that so many people have voted for it. Why would you purchase a savings plan for compute baselined at "medium" load? That entirely defeats the purpose of scalable resources. You are overpaying when the load is baselining and you are scaling up anyway when the load peaks...

Secondly, it says scale "Read Replicas," which gets you nothing at all if the increased load is write intensive. Using some common sense, we can deduce that an application that sells tickets to events is going to be highly transactional and likely need to scale writes along with reads.

upvoted 1 times

 **princajen** 4 months, 2 weeks ago

Selected Answer: D

While B is safer operationally due to ODCR, it's not the most cost-effective because ODCR charges at On-Demand rates. On the AWS exam, "most cost-effective" + "infrequent peaks" usually means Compute Savings Plans for the baseline (covers EC2 + Fargate) and Spot

Instances for peaks. That's why D is correct: it maximizes discounts, uses the cheapest scaling option, and avoids over-provisioning the database year-round.

upvoted 2 times

Chris_W_1234 2 months, 1 week ago

Additionally, B states "no upfront" vs. D which states "all upfront". "No upfront" costs more so even the DB option, which otherwise reads the same between B and D, is cheaper for D

upvoted 1 times

speedt115 5 months ago

Selected Answer: D

Option D was recommended because it uses Spot Instances for peak EKS loads, which are significantly cheaper than On-Demand Capacity Reservations (used in B). Infrequent demand spikes are perfect for Spot—assuming the workload can tolerate interruptions.

upvoted 2 times

bhanus 1 year ago

Selected Answer: D

Compute Savings Plans for EKS Base Load:

Spot Instances for Peaks:

1-Year All Upfront Reserved Instances for Database Base Load:

upvoted 4 times

nelgeozcin 1 year, 1 month ago

B - Fargate cannot support Spot - <https://docs.aws.amazon.com/eks/latest/userguide/fargate.html>

upvoted 1 times

Sin_Dan 1 year, 2 months ago

Selected Answer: D

No brainer, it's D. C doesn't provide any cost-effectiveness!

upvoted 5 times

FZA24 1 year, 2 months ago

Selected Answer: B

A wrong : Spot Instances to handle peaks

B: correct

C & D wrong : Temporarily scale up the DB instance manually during peaks.

upvoted 1 times

vip2 1 year, 5 months ago

Selected Answer: D

D looks more correctable

Mainly diff. between B and D is
predicable workload-- all upfront
no specific for read-replication traffic

On-Demand Capacity Reservations ensure availability during peak times without long-term commitments. but no cost-effective

upvoted 6 times

helloworldabc 1 year, 4 months ago

just B

upvoted 1 times

thotwielder 1 year, 7 months ago

Selected Answer: D

It's between b and d. D is more cost effective because of spot instances. And B is wrong because there is no reason to scale read replicas for RDS (the question doesn't say read only load)

upvoted 7 times

Dgix 1 year, 9 months ago

Selected Answer: D

I really don't understand why people are saying that Spot instances aren't suitable for production. There is a two-minute respite before they shut down, and since the application is not said to be stateful, this is plenty of time for a single request/response cycle.

With this in mind, the correct solution is D.

upvoted 7 times

Keval12345 1 year, 8 months ago

slightly difference betwee B and D {other than spot instances ofcourse}. Since the platform experinces peaks, might be a better idea to go for savings plan with medium load

upvoted 2 times

saggy4 1 year, 10 months ago

Selected Answer: B

A and C: The company will have a mix of EKS on EC2 and EKS Fargate hence reserved instance is not possible as it will cover only EKS on EC2 hence A and C are out

Between B and C:

C seems to save the most cost, but during peak load spot instances (both EC2 or Fargate) will not provide guaranteed availability. Hence we should go ahead with B.

Correct Answer: B

upvoted 2 times

 **AWSLord32** 1 year, 10 months ago

Selected Answer: C

C is the right answer. Everything about B is wrong: Compute savings plan is more expensive than RI, on demand more expensive than spot for peaks and no upfront more expensive than all upfront.

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: D

The scenario ask for the most cost-effective setup. Thus:

A = RI doesn't cover Fargate

B = ODCR doesn't bring cost benefits, they just ensure you have capacity. Read replicas are for read only, I would expect workload peaks includes writes so this is not saving money nor fully helping with capacity needs

C = EC2 Saving Plans do not cover Fargate

D = correct (this is the most cost-effective setup, Compute Savings Plans apply to both EC2 and Fargate, Spot Instances applies to both EC2 and Fargate, All Upfront Reserved Instances is most cost effective option for RDS. Manually scaling RDS adds a lot of overhead, but this is not the point of the question)

upvoted 7 times

 **ninomfr64** 1 year, 11 months ago

Also, for a temporarily limited change it is easier to manually vertically scale your instance rather than adding Read replicas as adding replicas to a single instance requires to change your app to send read requests to the reader endpoint and not to the cluster (aka writer) endpoint

upvoted 2 times

 **Jay_2pt0_1** 2 years ago

I might be leaning toward D as it does ask for the most cost-effective solution

upvoted 1 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.

Correct Answer: ACD

Community vote distribution

ACD (100%)

 **masetromain** Highly Voted 2 years, 11 months 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 16 times

 **masetromain** 2 years, 11 months 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 5 times

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

Selected Answer: ACD

You store the maintenance page in S3 (A), configure it as a secondary origin in the existing CloudFront distribution with an OAI for secure access (C), and switch the default cache behavior to use the S3 origin during maintenance (D). This avoids creating a new distribution and ensures visitors see the maintenance page instead of an error.

upvoted 1 times

 **carpa_jo** 1 year, 12 months ago

Selected Answer: ACD

From the given options ACD makes the most sense.

In real life the CloudFront feature to show custom error responses might make a lot more sense:

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

This would avoid the manual steps and by that is less prone to human errors.

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: ACD

A, C and D is correct.

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: ACD

CacheBehaviour defines path and origin

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: ACD

ACD morelikely

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: ACD

A C D

E is good option but is more overhead and propone error human then C is more accesible

upvoted 2 times

 **Jesuisleon** 2 years, 6 months ago

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

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: ACD

ACD is the best fit

upvoted 3 times

 **Musk** 2 years, 10 months ago

Selected Answer: ACD

About E, the lowest possible value for the "Origin Priority" field in AWS CloudFront is 1

upvoted 4 times

 **sam2ng** 1 year, 2 months ago

behavior precedence can be set to zero

upvoted 1 times

 **zozza2023** 2 years, 11 months ago

Selected Answer: ACD

ACD is correct

upvoted 4 times

 **zhangyu20000** 2 years, 11 months ago

ABD is correct

upvoted 1 times

 **zhangyu20000** 2 years, 11 months ago

ACD is correct

upvoted 2 times

Question #154

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.

Correct Answer: D

Community vote distribution

D (100%)

 **tatdatpham** Highly Voted 2 years, 4 months 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 12 times

 **masetromain** Highly Voted 2 years, 5 months 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 5 times

 **masetromain** 2 years, 5 months 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

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

Selected Answer: D

Create a Lambda alias and have the app invoke the alias ARN. After testing, point the alias to the new version. This avoids updating the client for every version change and reduces operational overhead.

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: D

Option D has least operational overhead.

upvoted 1 times

 **edder** 1 year, 6 months ago

Selected Answer: D

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

upvoted 1 times

 **SK_Tyagi** 1 year, 10 months ago

Selected Answer: D

Look for ALIAS

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: D

D

B is ok, but more overhead

upvoted 1 times

 **SkyZeroZx** 2 years ago

Selected Answer: D

keyword = Lambda ALIAS

then D

upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: D

Create a Lambda function alias.

upvoted 1 times

 **zhangyu20000** 2 years, 5 months 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.

Correct Answer: C*Community vote distribution*

C (100%)

 **God_Is_Love** Highly Voted 2 years, 3 months 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 22 times

 **zhangyu20000** Highly Voted 2 years, 5 months ago

C is correct

ABD all have CNAME record that is not allowed for apex domain

upvoted 10 times

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

Selected Answer: C

Global Accelerator = easiest + fastest + works with your existing DNS + solves the apex domain + multi-region routing problem.

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: C

Option C

upvoted 2 times

 **yuliaqwert** 1 year, 6 months ago

C <https://aws.amazon.com/blogs/networking-and-content-delivery/solving-dns-zone-apex-challenges-with-third-party-dns-providers-using-aws/>

upvoted 3 times

 **Explorer_30** 1 year, 10 months ago

The answer is C

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

C

no CNAME for apex

upvoted 2 times

 **SkyZeroZx** 2 years 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** 2 years ago

fun fact: CNAME records does not support APEX domain which simply rules out the options with CNAME in it
answer is C
upvoted 4 times

✉ **mfsec** 2 years, 3 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** 2 years, 5 months 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 5 times

✉ **masetromain** 2 years, 5 months 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** 2 years, 5 months 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

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.

Correct Answer: D*Community vote distribution*

D (71%)

B (29%)

 **lunt**  2 years, 10 months 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 46 times

 **rtgfdv3** 2 years, 9 months ago

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 3 times

 **c73bf38** 2 years, 10 months 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** 2 years, 10 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 4 times

 **rbm2023** 2 years, 7 months 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 4 times

 **Gabehcoud** 2 years, 4 months 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 3 times

 **Untamables**  2 years, 11 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 8 times

 **princajen**  4 months, 2 weeks ago

Selected Answer: D

If multiple Lambdas need the same dependencies, either use Lambda layers (for zip-based functions) or container images in ECR (for container-based functions). Here, since we want to bundle dependencies once and reuse without managing layers separately, a Docker image in ECR for Lambda is the simplest.

upvoted 1 times

 **albert_kuo** 9 months, 4 weeks ago

Selected Answer: D

Lambda Layer does not support Docker image.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: D

If any of you ever really worked in lambda with docker image, you will instantly choose D without hesitation.

zipped package can be deployed straightaway and it doesn't need a container. Don't get those two things(lambda zip deployment vs lambda container deployment) mixed up

upvoted 1 times

 **zolthar_z** 1 year, 5 months ago

Selected Answer: D

Please read the requirement, "simplify the deployment" with D you need only to maintain the docker image, with B you need to maintain the docker image and the process to deploy the lambda as ZIP Packages.

upvoted 1 times

 **Nicoben** 2 years ago

Selected Answer: B

Option B is the right one, see: <https://docs.aws.amazon.com/lambda/latest/dg/images-create.html>

upvoted 2 times

 **career360guru** 2 years ago

Selected Answer: D

Option D

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: D

check Iunt's answer

upvoted 1 times

 **rif** 2 years, 2 months ago

B.

* A Lambda layer is a .zip file archive that contains supplementary code or data. Layers usually contain library dependencies, a custom runtime, or configuration files.

* 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 2 times

 **dkcloudguru** 2 years, 3 months 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** 2 years, 4 months 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** 2 years, 4 months ago

<https://www.youtube.com/watch?v=17R0vN8bt-0>

upvoted 1 times

✉  **ggrodskiy** 2 years, 5 months ago

Correct B.

upvoted 2 times

✉  **NikkyDicky** 2 years, 5 months ago

Selected Answer: D

D

layers not supported w container-based lambdas

upvoted 1 times

✉  **pupsik** 2 years, 6 months ago

Selected Answer: D

Docker images cannot be used in Lambda layers.

upvoted 1 times

✉  **Jackhemo** 2 years, 6 months 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** 2 years, 6 months ago

Answer : B

upvoted 1 times

Question #157

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.

Correct Answer: B*Community vote distribution*

B (94%) 6%

 **God_Is_Love**  2 years, 3 months 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 19 times

 **Appon**  2 years, 4 months ago

Selected Answer: B

<https://aws.amazon.com/blogs/machine-learning/anomaly-detection-with-amazon-sagemaker-edge-manager-using-aws-iot-greengrass-v2/>

upvoted 5 times

 **princajen**  4 months, 2 weeks ago

Selected Answer: B

AWS IoT Greengrass enables local Lambda functions, container apps, and ML inference.

Works offline and can send results to the local API instantly.

AWS best practice for on-premises ML model deployment when internet downtime is a factor.

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: B

Option B

upvoted 1 times

 **dkcloudguru** 1 year, 9 months ago

Option B: Greengrass supports offline operation

upvoted 1 times

 **SK_Tyagi** 1 year, 10 months ago

Selected Answer: B

Offline = IoT Greengrass

upvoted 2 times

 **SK_Tyagi** 1 year, 10 months 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** 1 year, 11 months ago

Selected Answer: B

B for offline

upvoted 1 times

 **SkyZeroZx** 2 years ago

Selected Answer: B

keyword = WS IoT Greengrass

upvoted 1 times

 **consultornetwork** 2 years, 1 month 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 3 times

 **Diego1414** 2 years, 1 month 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** 2 years, 3 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** 2 years, 3 months 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

 **Untamables** 2 years, 4 months ago

Selected Answer: B

The point is how to offload ML workloads to the local.

upvoted 2 times

 **Musk** 2 years, 4 months ago

Selected Answer: B

Monitron is something different

upvoted 1 times

 **bititan** 2 years, 4 months 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** 2 years, 4 months 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** 2 years, 4 months ago

B is wrong, D is correct.

upvoted 2 times

 **schalke04** 2 years, 4 months 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 3 times

 **youngprinceton** 2 years, 4 months 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

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.

Correct Answer: B

Community vote distribution

B (90%)	10%
---------	-----

 **ZZ5** Highly Voted 2 years, 4 months 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 18 times

 **God_Is_Love** Highly Voted 2 years, 3 months 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 11 times

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

Selected Answer: B

If the question is about creating a migration business case from existing on-prem inventory data (like CMDB exports), the correct tool is Migration Evaluator. Application Discovery Service is more for automated data collection, not cost modeling from an existing inventory file.

upvoted 1 times

 **liquen14** 1 year, 3 months ago

This is again another example of completely stupid, nonsensical and useless exposition to ambiguity. Which one is correct because yeah, B seems to be well supported by <https://aws.amazon.com/blogs/architecture/accelerating-your-migration-to-aws/> but in the faqs for AWS Application Discovery Service <https://aws.amazon.com/blogs/architecture/accelerating-your-migration-to-aws/> there is literally a question about Application Discovery service

Q: Can I ingest data into Application Discovery Service from my existing configuration management database (CMDB)?

"Yes, you can import information about your on-premises servers and applications into the Migration Hub so you can track the status of application migrations. To import your data, you can download and populate the import CSV template and then upload it using the Migration Hub import console or by invoking the Application Discovery Service APIs"

So which one is correct? And what real knowledge are we getting from this pile of shit?

upvoted 2 times

 **Chris_W_1234** 2 months, 1 week ago

The scenario asks for a cost analysis. Yes, you can import CMDB data into Application Discovery Service but ADS doesn't do cost analysis.

upvoted 1 times

 **saggy4** 1 year, 4 months ago

Selected Answer: B

- A - It is a questionnaire tool used to assess your AWS architecture
C - We will need to create Complex Application using SDK
D- Application Discovery is free and does support CMDB import but it can only give you plan and not a business use case
B - Correct answer: Free and helps you create business use case.

upvoted 2 times

 **career360guru** 1 year, 6 months ago

Selected Answer: B

Option B

upvoted 1 times

 **bjexamprep** 1 year, 6 months ago

Selected Answer: B

Yes B is correct. But can you imagine any real architect in the world would trust such a solution for migration? It's a joke.
upvoted 1 times

 **joleneinthebackyard** 1 year, 8 months ago

Selected Answer: B

When you see business case for migration, you think of Migration Evaluator.
According to ChatGPT,
A: AWS Well-Architected Tool: no option to import CMDB data
C: only provide insight about current data, doesn't consider the nuances of migration task
D: Application Discovery Service is for discover, not for building business cases
upvoted 1 times

 **bustedd** 1 year, 8 months ago

Migration evaluation
B
upvoted 1 times

 **duriselvan** 1 year, 9 months ago

<https://www.youtube.com/watch?v=2qautbhujC8>
upvoted 1 times

 **Jonalb** 1 year, 11 months 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** 1 year, 11 months ago

Selected Answer: B

B - use case for ME
upvoted 1 times

 **SkyZeroZx** 2 years ago

Selected Answer: B

Question say : Migration
then Answer is : Migration Evaluator and other respond in this comments
upvoted 1 times

 **mfsec** 2 years, 3 months ago

Selected Answer: B

B is the best fit
upvoted 3 times

 **kiran15789** 2 years, 4 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** 2 years, 4 months ago

Selected Answer: B

B is right answer
upvoted 2 times

 **CloudFloater** 2 years, 4 months ago

Selected Answer: B

B

Free service, focus on cost of migration

upvoted 3 times

Question #159

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.

Correct Answer: B*Community vote distribution*

B (89%) 11%

 **God_Is_Love** Highly Voted 2 years, 9 months 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 14 times

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

Selected Answer: B

Designed for both network and application layer attacks.

Works automatically with ALB and WAF.

Minimal manual configuration after setup.

AWS-managed mitigation = least operational overhead.

upvoted 1 times

 **shmoeee** 10 months, 3 weeks ago

Selected Answer: B

I chose B since this is a DDOS attack and also option A could cause issues if legitimate traffic gets thrown on the ACL deny list

upvoted 1 times

 **nelgeozcin** 1 year, 1 month ago

Selected Answer: B

" The access logs show that each attack originates from different IP addresses. " implies DDOS

upvoted 1 times

 **Incognito013** 1 year, 4 months ago

Selected Answer: A

Nothing mentioned about DDOS in the question, plus A is simpler and less operational overhead

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just B

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: B

Option B sounds most logical answer in terms of least operational overhead.
though it does not provide details about how to identify and add those IP addresses to Shield Advanced for DDoS protection.
upvoted 2 times

✉ **Reejith** 2 years, 1 month ago

I think its option A. Option B is a paid service and it is for DDoS. Here that attack is not DDoS and it is excess traffic generated at application layer by certain IPs. Not in a distributed attack pattern. Advanced shield will give DDoS+WAF. But you already have WAF and using which you can block the IPs that is crossing set threshold. So option A is better choice. Option B is additional cost. Option C is wrong as you can not add deny rule in route table. Route table has only routes. Option D is operational overhead and then if you block the whole country , genuine traffic will also get blocked, which is not good.

upvoted 4 times

✉ **SK_Tyagi** 2 years, 4 months ago

Selected Answer: B

"Least" Operational Overhead - B

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B 100%

upvoted 1 times

✉ **SkyZeroZx** 2 years, 6 months 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** 2 years, 7 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 4 times

✉ **SkyZeroZx** 2 years, 7 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** 2 years, 7 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

✉ **SkyZeroZx** 2 years, 7 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

✉ **Daniel76** 1 year, 2 months ago

The attack is at the application layer. Solution A detects attack by IP which is at network layer, hence it is not valid.

upvoted 1 times

✉ **dev112233xx** 2 years, 8 months ago

Selected Answer: B

"with the LEAST operational overhead" is AWS SHIELD Advanced without doubts ✓

upvoted 3 times

✉  **hpirpit** 2 years, 9 months ago

Selected Answer: B

B 100% AWS SHIELD

upvoted 2 times

✉  **mfsec** 2 years, 9 months ago

Selected Answer: B

Deploy AWS Shield Advanced in addition to AWS WAF.

upvoted 2 times

✉  **rtgfdv3** 2 years, 10 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** 2 years, 10 months 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** 2 years, 10 months ago

Selected Answer: B

Reading more about option B, I pick B

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

Correct Answer: AD

Community vote distribution

AD (88%)

13%

 **testingaws123** Highly Voted 2 years, 3 months 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 10 times

 **taer** Highly Voted 2 years, 3 months 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 5 times

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

Selected Answer: AD

When RTO/RPO requirements are minutes or less, think real-time replication (Aurora Global Database, DynamoDB Global Tables). Backup/restore or manual recovery is too slow.

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: AD

A and D

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: AD

A and D

upvoted 1 times

 **SK_Tyagi** 1 year, 10 months ago

Selected Answer: AD

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

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: AD

its AD

upvoted 1 times

 **pupsik** 2 years ago

Selected Answer: AD

For DynamoDB use global table, for Aurora use cross-region read-replicas.

upvoted 3 times

 **easytoo** 2 years ago

a-d-a-d-a-d-a-d-a-d

upvoted 1 times

 **Roontha** 2 years ago

Answer : A, D

<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html>

upvoted 1 times

 **God_Is_Love** 2 years, 3 months 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](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/CrossRegionAccountCopyAWS.html)

upvoted 3 times

 **SK_Tyagi** 1 year, 10 months 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** 2 years, 3 months 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 4 times

 **schalke04** 2 years, 4 months ago

Selected Answer: AD

A and D

upvoted 4 times

 **bititan** 2 years, 4 months ago

Selected Answer: AD

you can create only db's not global tables, hence A and D

upvoted 4 times

Question #161

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 addresses 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 addresses 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.

Correct Answer: B*Community vote distribution*

B (93%) 4%

 **Untamables**  2 years, 4 months 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 22 times

 **jojom19980**  2 years, 4 months ago

Selected Answer: B

it uses path-based routing to forward requests based on the URL path
 upvoted 6 times

 **saggy4**  1 year, 4 months ago

Selected Answer: B

A - Cannot assign static IP to ALB
 C - Cannot attach target group directly as path-based forwarding is not possible with NLB
 D - Gateway load balancer supports only Instance and IP as target
 B - This is correct since using NLB we can have a static IP assigned and also attach ALB as target to NLB
 upvoted 5 times

 **Spnohal** 1 year, 5 months ago

<https://aws.amazon.com/solutions/implementations/git-to-s3-using-webhooks/>
 upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: B

Option B is only feasible option is ALB is using path based routing.
 upvoted 1 times

 **CProgrammer** 1 year, 6 months ago

bjexamprep "Anyone help why A not correct?"
 Where is the On Prem element, the Direct Connect, the ALB covering Multi AZ ?

"The objective of this question is achieved"
You don't even have the basic structure implemented
to attempt to address the questions requirements in your scenario
Regarding answer A :
<https://repost.aws/knowledge-center/alb-static-ip>
You can't assign a static IP address to an Application Load Balancer.
upvoted 1 times

 **bjexamprep** 1 year, 6 months ago

Selected Answer: A

Anyone can help explain why A is not correct? I created a private network facing ALB and it has a private IP address automatically created. Which means by adding the private IP address to the firewall, the objective of this question is achieved.

upvoted 2 times

 **saggy4** 1 year, 4 months ago

A is not correct because, though the IP attached to the ALB is the private IP, the control of which IP is assigned in with AWS, any change in the ALB can result in change of IP or even over a period of time AWS can change the IP (though it will be something in the CIDR)
upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: B

Option B as ALB can not have static IP address so Option A is not possible.

upvoted 2 times

 **task_7** 1 year, 9 months ago

D is also not the write answer

Target type

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

The following are the possible target types:

instance

The targets are specified by instance ID.

ip

The targets are specified by IP address.

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

The subnets of the VPC for the target group

10.0.0.0/8 (RFC 1918)

100.64.0.0/10 (RFC 6598)

172.16.0.0/12 (RFC 1918)

192.168.0.0/16 (RFC 1918)

upvoted 1 times

 **task_7** 1 year, 9 months ago

Elastic IP support

Network Load Balancer also allows you the option to assign an Elastic IP per Availability Zone (subnet) thereby providing your own fixed IP. Both B and C state single IP for multiple zones

upvoted 1 times

 **Gabehcoud** 1 year, 10 months 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 ALAdd the NLB IP addresses to the firewall appliance. Update the clients to connect to the NLB.

upvoted 1 times

 **khksoma** 1 year, 11 months 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** 1 year, 11 months ago

Selected Answer: B

B

need to keep ALB behind NLB for path routing

upvoted 1 times

 **Maria2023** 2 years 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** 2 years 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** 2 years, 1 month 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 3 times

✉️ **God_Is_Love** 2 years, 3 months 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** 2 years, 3 months 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 3 times

✉️ **God_Is_Love** 2 years, 3 months 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** 2 years, 2 months ago

I think main question is can it support static IP address which is needed by the firmware to waitlist it?

upvoted 2 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.

Correct Answer: C

Community vote distribution

C (100%)

 **masssa** Highly Voted 2 years, 4 months ago

Selected Answer: C

https://docs.amazonaws.cn/en_us/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html
AWS managed prefix list is more recommended.

upvoted 12 times

 **rbm2023** Highly Voted 2 years, 1 month 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 5 times

 **career360guru** Most Recent 1 year, 6 months ago

Selected Answer: C

Option C

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: C

Option C

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

C for sure

upvoted 1 times

 **mfsec** 2 years, 3 months ago

C. Add a security group rule to the ALB to allow traffic from the AWS managed prefix list for CloudFront only.
upvoted 2 times

 **ExamTopix01** 2 years, 4 months 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** 2 years, 4 months ago

Selected Answer: C

<https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-cloudfront-managed-prefix-list/>
upvoted 3 times

Question #163

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.

Correct Answer: B

Community vote distribution

B (74%)

A (26%)

 **princajen** 4 months, 2 weeks ago

Selected Answer: B

AWS "What's New" Announcement (Dec 28, 2022)

"Amazon ElastiCache for Redis now supports updates to encryption in transit on existing cluster resources. You can change the TLS configuration of your Redis clusters without re-building or re-provisioning them or impacting application availability. ... Upgrade your Redis cluster to version 7 or above. You can then modify the encryption-in-transit property for your cluster using the ElastiCache Console, API or CLI."

https://aws.amazon.com/about-aws/whats-new/2022/12/amazon-elasticsearch-redis-enabling-encryption-transit-existing-clusters/?utm_source=chatgpt.com

upvoted 1 times

 **jimee11** 7 months, 3 weeks ago

Selected Answer: B

ElastiCache can be updated to support AUTH. Note: RBAC replaces AUTH now.

upvoted 2 times

 **zhen234** 10 months, 3 weeks ago

Selected Answer: A

Encryption in transit cannot be enabled on an existing ElastiCache cluster. A new cluster must be created.

upvoted 3 times

 **d401c0d** 10 months, 4 weeks ago

Selected Answer: B

Amazon ElastiCache for Redis now supports updates to encryption in transit on existing cluster resources. You can change the TLS configuration of your Redis clusters without re-building or re-provisioning them or impacting application availability. When enabling encryption in transit, your overall solution can remain connected to Redis clusters.

To get started, upgrade your Redis cluster to version 7 or above. You can then modify the encryption-in-transit property for your cluster using the ElastiCache Console, API or CLI. This feature is available in all regions at no additional cost. To learn more, see the ElastiCache user guide.

upvoted 3 times

 **kylix75** 11 months, 1 week ago

Selected Answer: A

The correct answer is A - Create an AUTH token, store it in Parameter Store, and create a new cluster with AUTH and in-transit encryption. Key reasons:

ElastiCache doesn't allow enabling AUTH on existing clusters
SSL certificates aren't used for Redis authentication
Parameter Store is more cost-effective than Secrets Manager for this case
Solution meets both requirements: AUTH authentication and end-to-end encryption

upvoted 1 times

TewatiaAmit 1 year, 2 months ago

Selected Answer: A

A or B? Option B is suggesting to update the cluster which is not feasible. Once a cluster is created without encryption in transit, it cannot be modified to enable encryption in transit.

upvoted 1 times

Sin_Dan 1 year, 2 months ago

Selected Answer: A

Enabling encryption in transit on an existing ElastiCache cluster that wasn't originally configured with this feature is not possible. Encryption in transit, as well as encryption at rest, can only be specified at the time the cluster is created.

AWS Documentation on Encryption in Transit:

According to AWS ElastiCache documentation, if you want to enable encryption in transit, you must set this option when creating the ElastiCache cluster. Once a cluster is created without encryption in transit, it cannot be modified to enable this feature later. The same applies to Redis AUTH.

Thus, if a Redis cluster was deployed without encryption in transit, the only way to enable it is to create a new ElastiCache cluster with this setting enabled. Then, the data would need to be migrated from the existing cluster to the new one.

upvoted 3 times

JoeTromundo 1 year, 2 months ago

Selected Answer: B

B=Better :-)

upvoted 1 times

ke1dy 1 year, 7 months ago

Selected Answer: A

It seems to configure in-transit encryption in both new cluster and existing cluster, but updating is supported on Redis version 7 and later. So I will choose option A.

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/in-transit-encryption.html#in-transit-encryption-constraints>

upvoted 1 times

attila9778 1 year ago

<https://docs.aws.amazon.com/AmazonElastiCache/latest/dg/in-transit-encryption.html#in-transit-encryption-constraints>
"Modifying the in-transit encryption setting, for an existing cluster, is supported on replication groups running Valkey 7.2 and later, and Redis OSS version 7 and later." => modifying is possible => so B

upvoted 1 times

helloworldabc 1 year, 4 months ago

just B

upvoted 3 times

gofavad926 1 year, 9 months ago

Selected Answer: B

A or B? I didn't read any comparison between these 2 options... For sure we need an auth token. Both, using SSM Parameter Store or Secrets Manager will work. Both, create a new cluster or update the current one will work. I will choose B because this approach avoids the need to set up a new cluster, potentially reducing effort and costs associated with migration or duplication of resources...

upvoted 3 times

career360guru 2 years ago

Selected Answer: B

Option B

upvoted 2 times

career360guru 2 years, 1 month ago

Selected Answer: B

Option B

upvoted 2 times

NikkyDicky 2 years, 5 months ago

Selected Answer: B

B, per redis docs.

EC encr in transit is a config option

upvoted 2 times

 **easytoo** 2 years, 6 months ago
b-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 4 times

 **mfsec** 2 years, 9 months ago
Selected Answer: B
Create an AUTH token. Store the token in AWS Secrets Manager.
upvoted 1 times

 **God_Is_Love** 2 years, 9 months 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 4 times

 **Zek** 2 years, 9 months 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 3 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.

Correct Answer: B

Community vote distribution

B (100%)

 **bititan**  2 years, 10 months 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 14 times

 **Simon523**  2 years, 4 months 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 6 times

 **princajen**  4 months, 2 weeks ago

Selected Answer: B

Spot reliability comes from diversity. A single instance type + placement groups is too constrained and leads to "insufficient capacity" on Spot. Switch the launch template to attribute-based instance type selection (ABS) so the ASG can pick from many compatible types.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: B

Correct answer: B

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: B

Option B

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B

upvoted 1 times

 **totten** 2 years, 2 months ago

Selected Answer: B

When you use attribute-based instance type selection, you allow AWS to diversify the instances across different instance types within a specified instance family or similar characteristics. This helps in reducing the risk of Spot Instance termination due to capacity issues or price fluctuations.

upvoted 5 times

 **rl97** 2 years, 5 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 years, 5 months ago

Selected Answer: B

key word "spot instance launch failure"-> attribute based selection

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

its a b

upvoted 1 times

 **easytoo** 2 years, 6 months 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 5 times

 **mfsec** 2 years, 9 months ago

Selected Answer: B

B. Create a new launch template version that uses attribute-based instance type selection.

upvoted 2 times

 **Roontha** 2 years, 7 months ago

Agreed with B

upvoted 1 times

 **God_Is_Love** 2 years, 9 months 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 2 times

 **kiran15789** 2 years, 10 months ago

Selected Answer: B

Confused between B and D , will choose B

upvoted 1 times

 **saurabh1805** 2 years, 10 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** 2 years, 10 months ago

Selected Answer: B

B is correct

upvoted 1 times

Question #165

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.

Correct Answer: B*Community vote distribution*

B (70%)

C (26%)

 **dev112233xx** Highly Voted  2 years, 8 months ago

Selected Answer: B

B is correct imo

C is incorrect, FSx for Lustre doesn't support NFS protocol

It actually supports only POSIX protocol:

Custom (POSIX-compliant) protocol optimized for performance
upvoted 27 times

 **schalke04** Highly Voted  2 years, 10 months 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 23 times

 **lxrdm** 2 years, 5 months 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 5 times

 **rbm2023** 2 years, 7 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 9 times

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

Selected Answer: C

Nuanced question. B vs C.

B. S3 File GW = yes. Mount to EC2 via NFS = yes.

When changes occur in S3, RefreshCache API to update S3 File GW = No - if I am the server and I upload the file to S3 I don't need to refresh the S3 File GW to see the file, its already visible on the S3 File GW, this would only make sense if say something like a container stored the file on S3 bucket that is also linked to the S3 File GW > then yes. B also wants an API action per upload.

C. Mount text is the misdirect. If I follow the C and cannot mount the NFS volume because its not possible = solution still works. Also note,

this is one time setup with no regular mandated action - set and forget vs B which run an API command each time.
Answer is C.

upvoted 1 times

✉ **Blair77** 2 months, 3 weeks ago

Selected Answer: B

If you prioritize "least amount of effort", the S3 File Gateway (Option B) is the most straightforward. It's a simple mount that works with a legacy application without code changes, and it's a very common migration pattern.

upvoted 1 times

✉ **princajen** 4 months, 2 weeks ago

Selected Answer: B

This is a "can't update the app, need S3" scenario. S3 File Gateway is designed for exactly this — mount as NFS, writes go local then sync to S3. FSx for Lustre is more for HPC use cases, and DataSync won't give you continuous sync with <30min latency without extra work.

upvoted 1 times

✉ **d401c0d** 10 months, 4 weeks ago

Selected Answer: B

Luster does not support NFS.

upvoted 1 times

✉ **AWSum1** 1 year, 2 months ago

Note that it keeps saying "The Server" implying 1 server and not a fleet or multiple. NFS is from 1 client to 1 server.

So C is incorrect

upvoted 1 times

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

Selected Answer: B

Option C is not possible: how will you mount the document store on the EC2 instance through the Lustre client using NFS? Lustre is not compatible with NFS!

upvoted 1 times

✉ **xktm** 1 year, 4 months ago

The English in this question is very confusing, what is it trying do? what is the problem? where is the processing server?

upvoted 8 times

✉ **duriselvan** 1 year, 10 months ago

<https://repost.aws/knowledge-center/storage-gateway-automate-refreshcache>

upvoted 1 times

✉ **ninomfr64** 1 year, 11 months ago

Selected Answer: B

A = migrating to lambda requires a lot of work and doesn't solve the need to have fast access to files

B = correct

C = FSx for Lustre doesn't support NFS

D = DataSync can schedule transfer hourly, daily or weekly, cannot meet 30 minutes requirement

upvoted 7 times

✉ **career360guru** 2 years ago

Selected Answer: B

Option B as Fsx Luster though supports Linux, it does not support NFS.

upvoted 3 times

✉ **career360guru** 2 years, 1 month ago

Selected Answer: B

B is right. Though it is meant to be used to with on-premise in Hybrid environment, it is possible to use it on EC2.

upvoted 3 times

✉ **Dougmaster** 1 year, 1 month ago

B is right. If it wasn't possible to update that Linux server at that moment it implies they would have to remain it on premises for a while, in this case Amazon S3 File Gateway is the way to go.

upvoted 1 times

✉ **severlight** 2 years, 1 month ago

Selected Answer: B

just because NFS mentioned with Lustre, but everything else is pointing to the Lustre: Linux, fast, read/writes to S3

upvoted 2 times

✉ **covabix879** 2 years, 2 months ago

Selected Answer: C

B. Extra effort due to refreshCache API

D. DataSync runs in task schedule, which can't run faster than once per hour.

So remaining answer is C

upvoted 1 times

 **task_7** 2 years, 3 months ago

Selected Answer: D

The core of the problem is make the file available in S3 for 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? I think Option D (AWS DataSync) is a more straightforward and efficient choice.

upvoted 1 times

 **covabix879** 2 years, 2 months ago

DataSync task cannot run faster than 1 hour. "Even with a cron expression, you can't schedule a task to run at an interval faster than 1 hour." <https://docs.aws.amazon.com/datasync/latest/userguide/task-scheduling.html>

upvoted 5 times

 **Gabehcoud** 2 years, 3 months ago

Selected Answer: B

The server is running Linux, How can we use Fsx?

upvoted 4 times

 **chikorita** 2 years, 3 months ago

FSX for Lustre is for Linux and does not support Windows

upvoted 3 times

Question #166

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.

Correct Answer: C

Community vote distribution

C (69%)	A (26%)	5%
---------	---------	----

 **Untamables**  2 years, 10 months 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 17 times

 **Amac1979** 2 years, 9 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

 **kjcncjek** 2 years, 4 months ago

how can you use 1 sqs queue for all microservices?

upvoted 3 times

 **jainparag1** 2 years ago

You can have many consumers which means any of the consumers can receive and process the message.

upvoted 5 times

 **Chris_W_1234** 2 months, 1 week ago

Wrong. An SQS queue can have multiple consumers, but each message only gets processed by a single consumer, not ALL consumers, which would be required here. Not A.

upvoted 1 times

 **CloudFloater**  2 years, 10 months ago

Selected Answer: C

C seems correct; SQS is one queue to one microservice, could not find anything on dynamodb event notifications.

upvoted 17 times

 **aka1177**  3 weeks, 1 day ago

Selected Answer: B

" 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." -> but we need to delete user data not delete user from DynamoDB.

upvoted 1 times

✉ **princajen** 4 months, 2 weeks ago

Selected Answer: C

For immediate, multi-subscriber deletion across microservices, use EventBridge. Post a user-deleted event to a custom bus and create one rule per microservice to trigger its own delete logic. SQS is competing-consumer (not fan-out), and DynamoDB doesn't have direct "event notifications to SNS." EventBridge gives clean, serverless fan-out with filtering.

upvoted 1 times

✉ **jimee11** 7 months, 3 weeks ago

Selected Answer: C

Poorly worded question. DynamoDB Streams is designed to do exactly what is required here. But, attempting multiple microservices reading the same SQS queue and updating the same table is wrong.

C is the best option of the mess.

upvoted 2 times

✉ **juanife** 10 months, 2 weeks ago

it is MUCH MORE faster to send the event through eventbridge to microservices once the event of deletion needs to happen. I first read option A and thought it was the right one but have the microservices polling SQS QUEUE is less performant than the other one. AND it's impossible for SQS to have multiple consumers as this is not the main purpose of this service, this is not a fan-out architecture with SQS and SNS.

Totally sure that C is the correct answer, I repeat, I thought it was A but it's not.

upvoted 1 times

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

Selected Answer: C

C, The problem with A the SQS solution ist that the "other microservices which stores data chunks seperately". We do not know how many services are storing the userdata, and with SQS we would have one message on the queue which is processed by one of these microservices. how could the other microservices know that they have to delete the data when the message is allready consumed and processed?

upvoted 1 times

✉ **ry1999** 1 year, 3 months ago

Selected Answer: C

SQS does not have a fan-out capability. You need SNS --> SQS to achieve the microservices to be notified. Hence A is incorrect and C is correct.

upvoted 3 times

✉ **Dgix** 1 year, 9 months ago

Selected Answer: C

A is not viable since SQS is not used in a fan-out situation.

B is not viable since there's no such thing as "DynamoDB event notifications".

C is viable.

D is not viable, again due to the fact that SQS is not used for fan-out.

upvoted 4 times

✉ **career360guru** 2 years ago

Selected Answer: C

This is tricky question. C seems to be best and feasible. Rest options are not correct as they are using SQS where messages can be delivered only to one reader while in this scenario there are multiple microservices that needs to read the same message and delete the user information.

upvoted 4 times

✉ **CProgrammer** 2 years ago

Lets Ignore the insanity of

Several other microservices store in ---- different storage services. -----

central user service deletes a user, every other microservice must

also delete its copy of the data immediately.

YET ALL the options attempt a delete in the OG DynamoDB

Yeah OK Whatever Blue is green and Red is Orange these days.

BTW ans. == C , A will work but why poll SQS when Evt Brdg can invoke Microservice.

Personally I'd invoke a lambda to delete related records from the disparate data sources per KeyId and not bother the services but I'm not Architecting this mess maybe they want a clean log trail of the delete process as invoked by central user service whatever

upvoted 4 times

✉ **dankositze** 1 year, 10 months ago

Agreed. If this is an actual exam question, I am concerned about the intellect of the exam writers.

upvoted 4 times

✉ **Bad_Mat** 2 years ago

I vote for C because the question says: Delete the user IMMEDIATELY

A and D use SQS and messages in SQS can stay a pretty long time

upvoted 3 times

✉ **jainparag1** 2 years ago

Selected Answer: 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 1 times

 **jainparag1** 2 years ago

this is for Q165,

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C

upvoted 1 times

 **vjp_training** 2 years, 3 months ago

Selected Answer: A

https://aws.amazon.com/vi/getting-started/hands-on/send-fanout-event-notifications/?nc1=f_ls

upvoted 2 times

 **Ganshank** 2 years, 4 months 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 4 times

 **SK_Tyagi** 2 years, 4 months ago

Selected Answer: A

Event trigger from DynamoDb -- Choose DynamoDb Streams

upvoted 2 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.

Correct Answer: C

Community vote distribution

C (93%)	5%
---------	----

 **Untamables** Highly Voted 2 years, 10 months 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 20 times

 **masssa** Highly Voted 2 years, 10 months 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 18 times

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

Selected Answer: C

ALB doesn't support static IPs. If a customer needs fixed IPs, put AWS Global Accelerator in front of the ALB. You get two static anycast IPs, keep ALB+WAF unchanged, and avoid the complexity of swapping to NLB.

upvoted 1 times

 **AWSum1** 1 year, 2 months ago

Selected Answer: C

Global Accelerator provides two global static public IPs that act as a fixed entry point to your application endpoints, such as Application Load Balancers, Network Load Balancers, Amazon Elastic Compute Cloud (EC2) instances, and elastic IPs.

<https://aws.amazon.com/global-accelerator/>

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: C

A = NLB does not integrate with WAF

B = ALB cannot have Elastic IP attached, ALB cannot have static IP at all

C = correct

D = CloudFront distributions replies from many IPs, AWS manages a prefix list for this. Not easy to configure on customers side
upvoted 5 times

 **chsiri** 1 year ago

Why can't we create prefixlist with static ipaddress and assign to Cloudfront

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: C

Option C

upvoted 1 times

CProgrammer 2 years ago

An Application Load Balancer cannot be assigned an Elastic IP address --

<https://aws.amazon.com/blogs/networking-and-content-delivery/using-aws-lambda-to-enable-static-ip-addresses-for-application-load-balancers/>

upvoted 1 times

career360guru 2 years, 1 month ago

Selected Answer: C

Option C has least operational overhead. Option A is possible but changing ALB to NLB requires higher operational effort.

upvoted 2 times

NikkyDicky 2 years, 5 months ago

Selected Answer: C

C - basic use case for GA

upvoted 1 times

mfsec 2 years, 9 months ago

Selected Answer: C

C. Create an AWS Global Accelerator standard accelerator.

upvoted 1 times

God_Is_Love 2 years, 9 months 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 2 years, 9 months 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 2 years, 10 months ago

Selected Answer: C

<https://aws.amazon.com/premiumsupport/knowledge-center/alb-static-ip/>

Can assisng Static IP to ALB

upvoted 1 times

jojom19980 2 years, 10 months ago

Selected Answer: A

.....

upvoted 2 times

CloudInfrastructures 2 years, 10 months ago

C

WAF cannot be assoiated with NLB

upvoted 1 times

masssa 2 years, 10 months ago

NLB cannot be used when WAF is used

upvoted 1 times

ExamTopix01 2 years, 10 months ago

A

<https://aws.amazon.com/jp/premiumsupport/knowledge-center/alb-static-ip/>

upvoted 1 times

ExamTopix01 2 years, 10 months ago

Sorry C

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.alb-accelerator.html>

upvoted 1 times

schalke04 2 years, 10 months 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 2 years, 10 months 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

Question #168

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.

Correct Answer: CDF*Community vote distribution*

CDF (68%)	14%	Other
-----------	-----	-------

 **God_Is_Love** Highly Voted 2 years, 3 months 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/controltower/latest/userguide/controls.html>

upvoted 13 times

 **Untamables** Highly Voted 2 years, 4 months 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 5 times

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

Selected Answer: CDF

Pick Control Tower when you see "built-in blueprints and guardrails."

Do it in the management account, organize Prod/Dev OUs, and enroll/invite existing accounts.

Attach the EBS-encryption guardrail to the Production OU so it covers current and future prod accounts only.

upvoted 1 times

 **BelloMio** 8 months, 3 weeks ago

Selected Answer: CDE

I mean E is technically correct. The guardrail is created FROM the management account in Control Tower.

Even tho I would select F as well during the exam

upvoted 1 times

 **eboehm** 1 month ago

I thought so too sooo decided to let AI take a wack at it... it said

Guardrails in Control Tower are applied to OUs, not "from the management account" in an ad-hoc way.

The wording is off: you don't create a "guardrail from the management account" that hits everything; you attach guardrails to specific OUs

upvoted 1 times

 **career360guru** 1 year, 6 months ago

Selected Answer: CDF

C, D, F are the right choices.

upvoted 1 times

✉ career360guru 1 year, 7 months ago

Selected Answer: CDF

C, D, F

upvoted 1 times

✉ bur4an 1 year, 9 months ago

Basically order is DCF of the setup

upvoted 1 times

✉ NikkyDicky 1 year, 11 months ago

Selected Answer: CDF

CDF for sure

upvoted 1 times

✉ SkyZeroZx 2 years 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 3 times

CDF is correct

upvoted 1 times

✉ SkyZeroZx 2 years ago

Selected Answer: BCF

<https://www.examtopics.com/discussions/amazon/view/97939-exam-aws-certified-solutions-architect-professional-sap-c02/>
upvoted 1 times

✉ SkyZeroZx 2 years ago

Selected Answer: BCF

<https://www.examtopics.com/discussions/amazon/view/97939-exam-aws-certified-solutions-architect-professional-sap-c02/>
upvoted 1 times

✉ Windows98 2 years 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 3 times

✉ Windows98 2 years ago

I meant to say A and F because we're going to use Controls and Config

upvoted 1 times

✉ Roontha 2 years ago

Answer : C,D,F

upvoted 1 times

✉ DWsk 2 years, 2 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/controlltower/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 2 times

✉ xenodamus 2 years, 1 month 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 2 years, 3 months ago

Selected Answer: CDF

CDF seems the best choice

upvoted 1 times

 **dummy1777** 2 years, 4 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** 2 years, 4 months ago

Selected Answer: CDF

Answer is CDF

<https://docs.aws.amazon.com/controlltower/latest/userguide/controls.html>

<https://docs.aws.amazon.com/controlltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>

upvoted 1 times

 **c73bf38** 2 years, 4 months 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** 2 years, 4 months ago

moderator, delete above as the statement is incorrect that I posted, don't approve post.

upvoted 1 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?

- A. 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.
- B. 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.
- C. 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.
- D. 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.

Correct Answer: A

Community vote distribution

A (96%)	4%
---------	----

 **God_Is_Love** Highly Voted 2 years, 9 months 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 23 times

 **bititan** Highly Voted 2 years, 10 months 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 11 times

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

Selected Answer: A

EC2 with AWS Elastic Disaster Recovery → meets App RPO ~seconds (\leq 2 min target) and RTO \leq 30 min by spinning up in DR Region.

RDS cross-Region read replica → DB RPO \leq 5 min, promote on failover to meet RTO \leq 30 min.

ALB in second Region + AWS Global Accelerator → health-based regional failover with optimal latency post-failover (anycast entry + optimized paths).

DNS pointed to Global Accelerator → stable endpoint; no big app changes.

upvoted 1 times

 **sarlos** 1 year, 7 months ago

Why not C?

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just A

upvoted 1 times

 **tushar321** 1 year, 8 months ago

DRS Maintains state of EC2 machines while snapshot doesn't

upvoted 1 times

 **career360guru** 2 years ago

Selected Answer: A

Option A

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

Option A

upvoted 1 times

 **DiaaCloud** 2 years, 2 months ago

A is correct

D is not correct because snapshot is one region and must be copied and keep in sync to DR region which cannot meet the RTO...for sure

D is wrong

upvoted 1 times

 **nharaz** 2 years, 3 months ago

Selected Answer: A

DRS is faster to recover than Backups > https://youtu.be/07EHsPuKXc0?si=w_dZQKOAynE2T4JY

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

A for low RPO

upvoted 1 times

 **Jesuisleon** 2 years, 7 months 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** 2 years, 8 months 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 5 times

 **OCHT** 2 years, 8 months 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 2 times

 **OCHT** 2 years, 8 months 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 years, 5 months 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

 **OCHT** 2 years, 8 months 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** 2 years, 8 months 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

 **michele_scar** 1 year, 7 months ago

Option D doesn't mention DNS, so it's not correct

upvoted 1 times

 **Musk** 2 years, 10 months ago

Selected Answer: A

I agree it's A

upvoted 2 times

 **schalke04** 2 years, 10 months 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.

Correct Answer: CD

Community vote distribution

CD (91%)	9%
----------	----

 **God_Is_Love** Highly Voted 2 years, 9 months 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 11 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: CD

The correct answers are C and D. CloudWatch agent (C) collects memory metrics in addition to CPU and network. Compute Optimizer (D) uses those metrics to recommend properly sized instances. Trusted Advisor (B) isn't enough because it does not consider memory.

upvoted 1 times

 **LuongTo** 1 year ago

I would go for CD
B is more "CPU utilization"
C is more "memory metrics"
D is more CPU and network metrics

then CD is more comprehensive while DB miss the "memory" part

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: CD

Correct answer: C and D
"Memory utilization metrics are analyzed for the following resources: EC2 instances with the CloudWatch agent that's installed on them."

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: CD

NOT Option B - To have Compute Optimizer analyze the memory utilization metric 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#ec2-metrics-analyzed>

upvoted 2 times

 **career360guru** 2 years ago

Selected Answer: CD

Option C and D
upvoted 2 times

 **AWSStudyBuddy** 2 years ago

The solutions architect should take the following two steps to meet the requirements:

Configure AWS Compute Optimizer in the AWS account to receive findings and optimization recommendations. Compute Optimizer uses machine learning to analyze historical utilization metrics and provides recommendations to reduce costs and increase workload performance by recommending the optimal instance types.

Turn on AWS Trusted Advisor and review any "Low Utilization Amazon EC2 Instances" recommendations. Trusted Advisor checks for underutilized instances and provides recommendations to right-size them, helping optimize costs.

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: CD

C and D

upvoted 2 times

 **Russ99** 2 years, 2 months ago

Selected Answer: BD

AWS Trusted Advisor and AWS Compute Optimizer can both provide recommendations for right-sizing EC2 instances without requiring the installation of the CloudWatch agent or the collection of memory metrics.

The CloudWatch agent is primarily used for monitoring EC2 instances and collecting data for performance analysis. While it can be helpful to collect memory metrics for EC2 instances, it is not required for cost-optimizing and appropriately sizing them.

upvoted 3 times

 **Simon523** 2 years, 4 months 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** 2 years, 4 months ago

Selected Answer: CD

Cloud Watch Agent for memory metric & Compute Optimizer for recommendations

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: CD

cd for sure

upvoted 1 times

 **iamunstopable** 2 years, 8 months ago

A & B will incur more cost. CD are correct

upvoted 2 times

 **Roontha** 2 years, 7 months ago

Agreed. Answers are C,D

<https://docs.aws.amazon.com/compute-optimizer/latest/ug/metrics.html>

upvoted 1 times

 **mfsec** 2 years, 9 months ago

Selected Answer: CD

CD is right

upvoted 1 times

 **saurabh1805** 2 years, 10 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** 2 years, 10 months ago

D,OK.. but, why not B trusted advisor rather than C cloudwatch ?

upvoted 1 times

 **hobokabobo** 2 years, 9 months 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 is 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

 **rtgfdv3** 2 years, 10 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 3 times

 **Musk** 2 years, 10 months ago

Selected Answer: CDCD according to <https://docs.aws.amazon.com/compute-optimizer/latest/ug/metrics.html>

upvoted 2 times

Question #171

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

Correct Answer: C

Community vote distribution

C (97%)

 **bjexamprep** Highly Voted 2 years 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>

Hard to believe a product from AWS can be designed in such an amateur way.

upvoted 13 times

 **GabrielShiao** 11 months, 2 weeks ago

It is unbelievable for such a solution. In particular, it happens in the company like AWS

upvoted 1 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: C

Pick C because CodeCommit is not supported by AWS Backup and has no snapshot feature. The reliable pattern is to trigger on repo events (EventBridge) → run a build job (CodeBuild) → clone and archive the repo → store in cross-Region S3. This directly satisfies "store a backup copy in a second Region."

upvoted 1 times

 **nimbus_00** 1 year, 1 month ago

Selected Answer: C

Yeah...Deprecating CodeCommit was the right decision!

upvoted 1 times

 **AWSum1** 1 year, 2 months ago

AWS Backup does not support AWS CodeCommit directly.

upvoted 2 times

 **AWSum1** 1 year, 2 months ago

C is correct

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C

upvoted 2 times

 **severlight** 2 years, 1 month ago

Selected Answer: C

yes, AWS Backup cannot do this for you, so you should use Code Build to clone repo and upload zip to s3

upvoted 3 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

its a C

upvoted 1 times

✉ **easystoo** 2 years, 6 months ago

b-b-b-b-b-b-b-b
upvoted 1 times

✉ **easystoo** 2 years, 6 months ago

b in incorrect as AWS Backup does not backup code commit as a source.
upvoted 3 times

✉ **easystoo** 2 years, 6 months ago

C-C-C-C-CC-C-C-C-C-C-C
upvoted 3 times

✉ **Roontha** 2 years, 7 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 4 times

✉ **mfsec** 2 years, 9 months ago

Selected Answer: C

C for sure
upvoted 2 times

✉ **God_Is_Love** 2 years, 9 months 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** 2 years, 10 months ago

Selected Answer: C

<https://www.automat-it.com/post/backup-aws-codecommit>
upvoted 3 times

✉ **c73bf38** 2 years, 10 months ago

Selected Answer: C

C is correct, AWS Backup does not backup code commit as a source.
upvoted 2 times

✉ **lunt** 2 years, 10 months ago

Selected Answer: C

B is wrong > AWS Backup does not support CodeCommit as source.
A is out.
C is right.
upvoted 2 times

✉ **Musk** 2 years, 10 months 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** 2 years, 10 months 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** 2 years, 10 months ago

Changing to C, thanks.
upvoted 2 times

✉ **spd** 2 years, 10 months 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

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.

Correct Answer: C

Community vote distribution

C (95%)	5%
---------	----

 **spd**  2 years, 10 months ago

Selected Answer: C

Private link is the solution for IP Overlapping and Securely access the app between accounts

upvoted 16 times

 **c73bf38**  2 years, 10 months 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 11 times

 **princajen**  4 months, 1 week ago

Selected Answer: C

Pick C (PrivateLink) for private, cross-account access when CIDRs overlap and you want the least operational overhead. PrivateLink uses interface endpoints (ENIs) in the consumer VPCs, avoids complex routing/peering/VPNs/NAT, and keeps traffic on AWS's private network. Options A/B are heavy and fragile with overlaps; D adds unnecessary API Gateway complexity unless you specifically need API features.

upvoted 1 times

 **alexanteeno** 2 years ago

Selected Answer: B

"LEAST OPERATIONAL OVERHEAD" - is key word in a question. Its not so easy to migrate any on-premise infra to any AWS. Looking at the answers here I see no one eve done that before and just answering as from AWS docs.

The easiest way to migrate any on-premise infra - ec2

upvoted 1 times

 **StevePace** 1 year, 9 months ago

who mentioned migration?!

upvoted 2 times

 **helloworldabc** 1 year, 4 months ago

just C

upvoted 2 times

 **honoga4853** 2 years ago

Selected Answer: B

"LEAST OPERATIONAL OVERHEAD" - is key word in a question. Its not so easy to migrate any on-premise infra to any AWS. Looking at the answers here I see no one eve done that before and just answering as from AWS docs.

The easiest way to migrate any on-premise infra - ec2

upvoted 1 times

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

just C

upvoted 2 times

✉️ **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C

upvoted 1 times

✉️ **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C for sure

upvoted 1 times

✉️ **Alabi** 2 years, 6 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** 2 years, 9 months ago

Selected Answer: C

Private link

upvoted 1 times

✉️ **God_Is_Love** 2 years, 9 months ago

Selected Answer: C

Networking & Content Delivery blog -

<https://aws.amazon.com/blogs/networking-and-content-delivery/connecting-networks-with-overlapping-ip-ranges/>

upvoted 5 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.

Correct Answer: B

Community vote distribution

B (95%)	5%
---------	----

 **dkx** Highly Voted 1 year, 11 months 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 15 times

 **God_Is_Love** Highly Voted 2 years, 3 months ago

Selected Answer: B
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-analyzer.html>
 upvoted 12 times

 **God_Is_Love** 2 years, 3 months 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 8 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: B

Pick B because IAM Access Analyzer natively detects public access on S3 buckets and emits precise findings. Use EventBridge to filter for isPublic: true and send to the existing SNS topic. The other options either rely on unsupported events (A), only detect policy changes (C), or reference an unrelated Config rule (D).

upvoted 1 times

 **AimarLeo** 1 year, 4 months ago

This question.. is seriously ! a googling one

upvoted 1 times

 **dkclougdguru** 1 year, 9 months ago

Option B

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: B

it's B

upvoted 2 times

 **Maria2023** 2 years 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 2 times

 **SkyZeroZx** 2 years ago

Selected Answer: B

keyword = AWS Identity and Access Management Access Analyzer

then B

upvoted 2 times

 **leehjworking** 2 years, 1 month 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** 2 years, 1 month ago

Selected Answer: B

Aws is letter B

Previous writing is a error

upvoted 1 times

 **SkyZeroZx** 2 years, 1 month ago

Letter C

upvoted 1 times

 **SkyZeroZx** 2 years, 1 month 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 2 times

 **SkyZeroZx** 2 years, 1 month 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** 2 years, 1 month ago

Selected Answer: B

<https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-eventbridge.html>

upvoted 1 times

✉  **mfsec** 2 years, 3 months ago

Selected Answer: B

B eventbirdge and access analyser

upvoted 2 times

✉  **c73bf38** 2 years, 4 months 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 7 times

✉  **masssa** 2 years, 4 months 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

✉  **mdijoux25** 2 years, 4 months ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-analyzer.html>

upvoted 2 times

✉  **spd** 2 years, 4 months ago

Selected Answer: D

D by elimination rule

upvoted 2 times

✉  **Jay_2pt0_1** 2 years, 1 month 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.

Correct Answer: C

Community vote distribution

C (97%)

 **spd** Highly Voted 2 years, 10 months ago

Selected Answer: C

First need to evaluate
upvoted 17 times

 **c73bf38** Highly Voted 2 years, 10 months 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 8 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: C

Migration Evaluator builds the business case and server inventory, Migration Hub provides a single view of the portfolio, and Application Discovery Service reveals application/database dependencies. The other options focus on migration execution (SMS, DMS, MGN) or governance (Control Tower), not assessment and discovery, which is the actual requirement.
upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C
upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C for sure
upvoted 1 times

 **Roontha** 2 years, 7 months ago

Answer : C
<https://aws.amazon.com/migration-evaluator/>
upvoted 2 times

 **F_Eldin** 2 years, 7 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

 **helloworldabc** 1 year, 4 months ago

just C

upvoted 1 times

 **mfsec** 2 years, 9 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.

Correct Answer: A*Community vote distribution*

A (100%)

 **c73bf38** Highly Voted 2 years, 10 months 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 11 times

 **spd** Highly Voted 2 years, 10 months ago

Selected Answer: A

EFS = Fastest storage performance compare to S3/EBS

upvoted 7 times

 **masssa** 2 years, 10 months 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** 2 years, 10 months ago

typo.

EBS faster than S3/EFS.

upvoted 2 times

 **Musk** 2 years, 10 months ago

I just read the question refers to multiple AZs, so B is not an option.

upvoted 10 times

 **AWSum1** 1 year, 2 months ago

I missed this too 🍏 good spot

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just A

upvoted 1 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: A

(EFS) because it's shared, multi-AZ, and high-performance for many small files, and integrates with AWS Backup for 1-year retention.

B (EBS) is AZ-bound, not cross-node shared.

C (S3) is object storage, slower for small-file workloads.

D (local storage) isn't shared and is ephemeral.

upvoted 1 times

career360guru 2 years, 1 month ago

Selected Answer: A

Option A

upvoted 1 times

joleneinthebackyard 2 years, 1 month ago

Selected Answer: A

A: sounds valid

B: EBS multi attach can only do same AZ -> out

C: S3 is for durability, not for performance

D: can drop when seeing third party tool.

upvoted 5 times

NikkyDicky 2 years, 5 months ago

Selected Answer: A

A - EFS for multi-AZ

upvoted 2 times

dkx 2 years, 5 months 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 4 times

mfsec 2 years, 9 months ago

Selected Answer: A

A for sure

upvoted 2 times

ramyaram 2 years, 9 months ago

Selected Answer: A

Keyword here is multiple small files and shared between multiple clusters

upvoted 3 times

God_Is_Love 2 years, 9 months 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 2 years, 9 months 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 2 years, 9 months 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 2 years, 10 months ago

I've been reading here and there, and B does not seem that feasible, although if supported it would be faster than A.
upvoted 2 times

Question #176

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.

Correct Answer: A*Community vote distribution*

A (96%)	4%
---------	----

 **God_Is_Love** Highly Voted  2 years, 3 months 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 13 times

 **princajen** Most Recent  4 months, 1 week ago

Selected Answer: A

Amazon Connect provides a fully managed cloud call center, and Amazon Pinpoint supports two-way SMS surveys. This meets all requirements with the least operational overhead.

B (SNS) = one-way only.

C (EC2) = heavy ops burden.

D (Pinpoint alone) = no call center support.

upvoted 1 times

 **pichunya** 7 months, 1 week ago

Selected Answer: A

amazon pinpoint EoS 2025/5/20

upvoted 1 times

 **alexstanteeno** 1 year, 6 months ago

"LEAST OPERATIONAL OVERHEAD" - is key word in a question. Its not so easy to migrate any on-premise infra to any AWS. Looking at the answers here I see no one eve done that before and just answering as from AWS docs.

The easiest way to migrate any on-premise infra - ec2

upvoted 2 times

 **career360guru** 1 year, 7 months ago

Selected Answer: A

Option A

upvoted 1 times

 **rrrrrrrrr1** 1 year, 11 months ago

Why not b though? SNS is easy as heck to use.

upvoted 1 times

✉️ **VerRi** 1 year, 4 months ago

"managed, interactive, two-way experience" means a personalised and customised message, so it should be Pinpoint here.
upvoted 5 times

✉️ **rrrrrrrrr1** 1 year, 11 months ago

nvm text message surveys are probably a pinpoint thing. I was thinking like a link to a survey.
upvoted 3 times

✉️ **NikkyDicky** 1 year, 11 months ago

Selected Answer: A

A - basic AWS connect use case

upvoted 1 times

✉️ **Maria2023** 2 years ago

Selected Answer: A

Amazon connect + Pinpoint are the best choice here

upvoted 1 times

✉️ **Roontha** 2 years ago

Answer: A

upvoted 1 times

✉️ **mfsec** 2 years, 3 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** 2 years, 4 months 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 4 times

✉️ **spd** 2 years, 4 months ago

Selected Answer: A

<https://docs.aws.amazon.com/pinpoint/latest/userguide/channels-sms-two-way.html>

upvoted 2 times

Question #177

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.

Correct Answer: D

Community vote distribution

D (76%)	12%	12%
---------	-----	-----

 nyxs_19 Highly Voted 2 years, 10 months 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 10 times

 spd Highly Voted 2 years, 10 months ago

Selected Answer: D

D looks most appropriate

upvoted 9 times

 princajen Most Recent 4 months, 1 week ago

Selected Answer: C

Pick C because pre-claiming phone numbers and preloading contact flows in the DR Region minimizes recovery time. Users can be added quickly at failover. Option D delays number creation, which slows recovery and raises RTO.

upvoted 2 times

 29fb203 9 months, 1 week ago

Selected Answer: C

C accounts for the phone numbers and all other resources. D doesn't

upvoted 1 times

 Sin_Dan 1 year, 2 months ago

Selected Answer: C

Setting up phone numbers is more complex and time consuming, than setting up users. Option D waits until the disaster happens to provision the phone numbers. Option C is right, because it is quicker as compared to option D. Also, it makes sure the users are not duplicated upfront.

upvoted 1 times

 **cashyc** 1 year, 2 months ago

Selected Answer: C

by pre-provisioning a new Amazon Connect instance in a second AWS Region with the necessary contact flows and phone numbers already in place. The remaining task at the time of disaster recovery is to deploy the users, which can be done using an AWS Lambda function triggered by a CloudWatch alarm when the primary instance becomes unavailable, as determined by a Route 53 health check.

upvoted 1 times

 **marszalekm** 1 year, 11 months ago

Amazon Connect is not on the list of services required for this exam. At least as of 08.01.24 https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS-Certified-Solutions-Architect-Professional_Exam-Guide.pdf

upvoted 6 times

 **career360guru** 2 years, 1 month ago

Selected Answer: D

Option D

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: D

Amazon Connect gives you a URL, for which you can add a record in route 53 and hence have a health check.

upvoted 1 times

 **SK_Tyagi** 2 years, 4 months 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 3 times

 **MRL110** 2 years, 5 months 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 years, 5 months ago

Selected Answer: D

D i guess

upvoted 1 times

 **Maria2023** 2 years, 6 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** 2 years, 7 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 3 times

 **dev112233xx** 2 years, 8 months 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** 2 years, 9 months ago

why not C?

upvoted 1 times

 **ninomfr64** 1 year, 11 months ago

I think, but I was not able to verify it, that if your instance is active and you have phone numbers configured it is receiving actual phone traffic that is a and Active/Active scenario, however you do not have users (aka Agents) configured to handle calls. This is just me guessing

upvoted 3 times

 **shmoeee** 10 months, 2 weeks ago

Same thinking i had

upvoted 1 times

 **mfsec** 2 years, 9 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

Question #178

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.

Correct Answer: B

Community vote distribution

B (94%)	6%
---------	----

 **youngmanaws** Highly Voted 1 year, 8 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 11 times

 **renegadedme** Highly Voted 1 year, 8 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 9 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: B

AWS Data Exchange now supports Redshift datashares, letting you securely and automatically share live, up-to-date Redshift data with subscribers. This includes built-in subscription verification. Compared to exporting to S3 (C) or building APIs (A), this has least operational overhead. Option D is incorrect because Open Data is for public datasets, not verified customers.

upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: B

it's a B

upvoted 1 times

 **SmileyCloud** 1 year, 5 months ago

Selected Answer: B

Keyword is datashare

<https://docs.aws.amazon.com/redshift/latest/dg/adx-getting-started.html>

upvoted 5 times

 **easytoo** 1 year, 6 months ago

b-b-b-b-bb-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 3 times

 **TECHNOWARRIOR** 1 year, 6 months 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 5 times

 **Roontha** 1 year, 7 months ago

Answer : B

<https://www.youtube.com/watch?v=BeIoTSqI4IM>

(AWS Data Exchange for Amazon Redshift demo | Amazon Web Services)

upvoted 3 times

 **Sarutobi** 1 year, 7 months 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

 **OCHT** 1 year, 8 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** 1 year, 8 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.

Correct Answer: B

Community vote distribution

B (52%)

A (48%)

 **Sarutobi**  2 years, 8 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 33 times

 **SuperDuperPooperScooper**  2 years, 1 month ago

Selected Answer: A

Configuring scaling based on the age of the oldest message is nowhere near as good as scaling based on size of the Queue for this use case.

age of the oldest message will grow linearly based on time. If there is a dramatic spike in the Queue size due to increased traffic, like 100X increase in size. Then the queue will have grown a lot but the oldest message will only increase in age linearly, so the scaling will not be able to realize how much the workload has increased.

upvoted 11 times

 **sonyaws** 2 years, 1 month ago

makes sense

upvoted 1 times

 **jainparag1** 2 years ago

very good explanation. Moreover, go serverless as much as possible. EC2 vs Lambda - Lamda is always preferred.

upvoted 1 times

 **mns0173** 1 year, 4 months ago

there will just be a lag in scaling, but eventually this metric will scale as needed

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just B

upvoted 1 times

 **Blair77**  2 months, 3 weeks ago

Selected Answer: B

B is good. Amazon SQS decouples the event producers and consumers, providing a queue to hold events until processed. A: This option uses Amazon SNS, which is a publish-subscribe service. While it can trigger a Lambda function, it is not a message queue and is not designed for a high-volume event processing workflow that requires a separate queue for failed events.

upvoted 1 times

 **Murtuza** 3 months, 2 weeks ago

Selected Answer: B

While Option A (SNS + Lambda) is a strong serverless choice with very low operational overhead, Option B is a well-established and robust architectural pattern that is arguably a more complete and direct answer for this specific question.

upvoted 1 times

 **princajen** 4 months, 1 week ago

Selected Answer: B

SQS gives buffering + native scaling signals and a straightforward DLQ for failed events. It cleanly satisfies "scale with number of events" and "move failed events to a separate queue." The other options either misuse services for DLQ/targets or add unnecessary complexity.

upvoted 1 times

 **Kaps443** 6 months, 2 weeks ago

Selected Answer: B

This one is easy haven't people heard about SQS dead-letter queues (DLQs).

upvoted 2 times

 **eesa** 7 months, 2 weeks ago

Selected Answer: B

B is correct:

Scalability: The EC2 Auto Scaling group can automatically scale in and out based on the SQS metric (ApproximateAgeOfOldestMessage), which reflects how long messages have been waiting to be processed.

Error handling: SQS supports dead-letter queues (DLQs) to isolate and handle failed messages for later analysis or reprocessing.

Decoupled architecture: SQS enables a loosely coupled and fault-tolerant system design.

upvoted 1 times

 **f3f4935** 8 months ago

Selected Answer: B

also think B will be good there

upvoted 1 times

 **CAIYasia** 8 months ago

Selected Answer: B

I would go B for the DLQ

upvoted 1 times

 **itsjunukim** 10 months ago

Selected Answer: B

By utilizing the ApproximateAgeOfOldestMessage metric, you can scale out and scale in based on the workload, ensuring that your application can handle increases in traffic.

upvoted 1 times

 **820b83f** 10 months, 2 weeks ago

Selected Answer: B

100 % its B, My reasons are:

1. SNS is for pub/sub, not event processing. SNS sends events to multiple subscribers but does not provide queue-based scaling.

2. Lambda also has concurrency limits, which might cause failures at high event rates.

upvoted 1 times

 **kylix75** 11 months, 1 week ago

Selected Answer: B

The correct answer is B.

Reasons:

1. SQS + Auto Scaling provides event-based scalability
2. ApproximateAgeOfOldestMessage metric enables workload-based scaling
3. SQS native dead-letter queue handles error messages
4. Most resilient and cost-effective solution for event processing at scale

Issues with other options:

A: SNS doesn't store messages for reprocessing

C: DynamoDB Streams has scalability and retention limitations

D: ALB + EC2 is more complex and expensive than serverless processing

upvoted 1 times

 **ahhatem** 1 year ago

Selected Answer: B

While A would probably work fine most of the time, B is more resilient. Once a message is in the Q, it will either be marked as complete or go to DLQ. In A, in edge cases like lambda exceeding concurrency limit, the message would be throttled after the SNS returns success to the sender.... Without SNS DLQ, the message would be lost.

upvoted 3 times

 **FZA24** 1 year, 1 month ago

Selected Answer: B
scale in scale out => ALB
a separate queue => DLQ
upvoted 3 times

 **Woody1848** 1 year, 2 months ago

Selected Answer: A

- By sending event details to an Amazon SNS topic and configuring an AWS Lambda function as a subscriber, the solution automatically scales with the number of incoming events.
- Lambda functions scale in and out based on the event load without manual intervention.
- Adding an on-failure destination to the Lambda function that targets an Amazon SQS queue ensures that any processing errors move the event into a separate queue for review.
- This setup meets both the scalability and error-handling requirements efficiently.

upvoted 2 times

 **Sin_Dan** 1 year, 2 months ago

Selected Answer: B
Option A uses Lambda to process the solution. However, we don't know if the processing finishes within 15 mins or not. Also, SNS isn't as well-suited for handling large event queues as SQS, and scaling based on message queue metrics is not supported in this configuration. So, the correct option is definitely B.

upvoted 2 times

 **Daniel76** 1 year, 2 months ago

Selected Answer: B
Only B and D mention about reviewing error in a separate queue by dead letter Q, with D never use SQS where this is supported.
upvoted 2 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.

Correct Answer: B

Community vote distribution

B (88%)	8%
---------	----

✉️  momo3321  2 years, 7 months 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 20 times

✉️  bjexamprep  2 years ago

Selected Answer: B

In real life, I wouldn't trust SQS to handle such large amount of data.

upvoted 6 times

✉️  princjen  4 months, 1 week ago

Selected Answer: B

API Gateway → SQS provides a durable, scalable buffer to absorb bursty traffic, ensuring no data loss, while Lambda scales processing based on queue depth with near-zero ops. A and D are invalid integrations; C lacks a durable buffer and risks loss under spikes.

upvoted 1 times

✉️  altonh 10 months ago

Selected Answer: D

A - SQS as an ALB target is wrong

B - Cannot integrate an AWS service using an HTTP API Gateway

C - Data cannot be passed to EC2 because the integrated AWS service is an ASG.

upvoted 1 times

✉️  vip2 1 year, 5 months ago

Selected Answer: B

Restful API is not REST API, so HTTP API-GW + SQS

upvoted 2 times

✉️  jAtlas7 1 year, 1 month ago

REST APIs and HTTP APIs are both RESTful API products. Ref: <https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>

upvoted 2 times

✉ **nzin4x** 1 year, 10 months ago

but normally API gateway can not handle high burst request. it will make 429 too many requests error.

upvoted 2 times

✉ **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B

upvoted 1 times

✉ **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B

upvoted 1 times

✉ **severlight** 2 years, 1 month ago

Selected Answer: B

yes you can integrate API Gateway HTTP Api with SQS

upvoted 2 times

✉ **SK_Tyagi** 2 years, 4 months ago

Selected Answer: B

KDS need to implement Sharding for unpredictable bursts

upvoted 1 times

✉ **rxhan** 2 years, 5 months ago

Similar to #179

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B is right

upvoted 1 times

✉ **Roontha** 2 years, 7 months ago

Answer : B

upvoted 1 times

✉ **rbm2023** 2 years, 7 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 2 times

✉ **AMEJack** 2 years, 7 months ago

Selected Answer: B

Kinesis DataStreams can't be the origin for the CloudFront

upvoted 2 times

✉ **mrfretz** 2 years, 8 months ago

Selected Answer: D

Kinesis retention

upvoted 1 times

✉ **mrfretz** 2 years, 8 months ago

Selected Answer: B

Kinesis retention

upvoted 1 times

✉ **mrfretz** 2 years, 8 months ago

Answer D, sorry typo

upvoted 1 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.

Correct Answer: C

Community vote distribution

C (78%)	12%	8%
---------	-----	----

 **SK_Tyagi**  2 years, 4 months ago

Selected Answer: C

Fits the use case

<https://aws.amazon.com/transit-gateway/>

upvoted 13 times

 **SK_Tyagi** 2 years, 4 months ago

<https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-isolated.html>

upvoted 2 times

 **ninomfr64**  1 year, 11 months ago

Option C is very poorly worded: "Provision a transit gateway in an account in each OU" to me this results in having 3 Transit Gateways, but then it goes ahead just referring to a single Transit Gateway "Share the transit gateway across the organization ..."

upvoted 7 times

 **princajen**  4 months, 1 week ago

Selected Answer: C

Transit Gateway per OU provides scalable hub-and-spoke connectivity within the OU and default isolation across OUs, with minimal operational overhead. Peering meshes (A/B) don't scale and are non-transitive; VPNs with third-party routing (D) are heavy to operate.

upvoted 1 times

 **bhanus** 12 months ago

Selected Answer: C

TGW would be used to create hub and spoke. VPCs are in same region so tgw can be shared via RAM.

Answer is C

upvoted 1 times

 **43c89f4** 1 year, 8 months ago

Typical transit gateway use case

upvoted 1 times

 **bjexamprep** 1 year, 9 months ago

Selected Answer: C

The question is asking "a solution in which VPCs in the same OU can communicate with each other but cannot communicate with VPCs in other OUs".

A: It works. But it may create 2500+ VPC peering in each OU

B: It works. But it may create 2500+ VPC peering in each OU

C: This is wrong, cause it is sharing the transit gateway to all the accounts in the organization instead of sharing to all the accounts in that OU.

D: That means 2500+ VPN connections in each OU and cost a lot of internet bandwidth.

I guess the C was worded with mistake. It should be sharing the transit gateway to the accounts in each OU and create VPC attachment for each VPC in that OU.

upvoted 5 times

 **Sin_Dan** 1 year, 2 months ago

I don't understand why there are so many poorly written questions and options in the AWS exams. I am wondering if we are writing an exam for English or AWS. Many questions are just elongated for adding complexity. Not a right way to assess technical skills of a person based on their English skills.

upvoted 2 times

 **VerRi** 1 year, 10 months ago

Selected Answer: A

The requirement said, "VPCs in the same OU can communicate with each other but cannot communicate with VPCs in other OUs". There is no reason to share the TGW across the organization with RAM because it will enable cross OUs communication.

upvoted 1 times

 **itsjunukim** 10 months ago

VPCs within the same OU can communicate with each other. Each OU has 100 accounts, and having all 100 accounts perform VPC peering would be inefficient.

upvoted 1 times

 **learnwithaniket** 1 year, 12 months ago

Selected Answer: A

"Least operational overhead"

A is correct.

C creating Transit Gateway in each account.. and there are more than 100 accounts in each OU. Which is time consuming and requires lot of efforts.

upvoted 2 times

 **chicagobeef** 1 year, 11 months ago

"A" would mean having 1:1 peering attachments with EACH ACCOUNT which is too much operational overhead. A transit gateway is more viable so it's "C".

upvoted 4 times

 **jainparag1** 2 years ago

Selected Answer: A

typical use case of intra region peering with transit gateway.

upvoted 1 times

 **jainparag1** 2 years ago

oops right answer is 'C'.
upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C

upvoted 3 times

 **rif** 2 years, 2 months ago

C.

Transit gateway and RAM is a regional service.

AWS RAM is a Regional service, and a resource share is Regional. Therefore, a resource share can contain resources from the same AWS Region as the resource share, and any supported global resources.

<https://docs.aws.amazon.com/ram/latest/userguide/working-with-regional-vs-global.html>

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

upvoted 6 times

 **LuongTo** 1 year ago

the best explanation, share across but the same Region -> same OU

upvoted 1 times

 **MRL110** 2 years, 5 months 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** 2 years, 5 months 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 years, 5 months ago

Selected Answer: C

I thik C

upvoted 3 times

 **dkx** 2 years, 5 months 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 5 times

 **xflare** 2 years, 4 months 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** 2 years, 6 months ago

Selected Answer: C

A separate transit GW for each OU.

upvoted 2 times

 **Maria2023** 2 years, 6 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 2 times

 **Jackhemo** 2 years, 6 months ago

Olabiba.ai says C.

upvoted 2 times

 **Ashas** 2 years, 6 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 2 times

Question #182

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.

Correct Answer: B*Community vote distribution*

B (93%)

7%

 **SkyZeroZx** Highly Voted 2 years, 6 months ago

if you have come far it means that you are persistent, good luck in your exam
upvoted 35 times

 **easytoo** 2 years, 6 months ago

My man. Respect, we are all cloud brothers here.
upvoted 10 times

 **joleneinthebackyard** 2 years, 1 month ago

I went backward, does it count?
upvoted 8 times

 **kgpoj** 1 year, 4 months ago

Man, what can I say
upvoted 2 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: C

S3 provides 11 9's durability, high availability, and native integration with KMS customer-managed keys for company-controlled encryption and rotation. Bucket policies enforce HTTPS-only and encryption at rest. Options A and D rely on block storage/VMs (not fully managed), and C is wrong data type.
upvoted 1 times

 **gutomarson** 1 year, 5 months ago

Answer is B
upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B
upvoted 1 times

 **SK_Tyagi** 2 years, 4 months ago

Selected Answer: B

Easy breezy
upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

its a b

upvoted 1 times

 **Maria2023** 2 years, 6 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 3 times

 **Alabi** 2 years, 6 months ago

Selected Answer: B

B for sure

upvoted 1 times

 **erhard** 2 years, 6 months ago

Not C because _large_ documents and

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/ServiceQuotas.html#limits-items>

upvoted 2 times

 **Alabi** 2 years, 6 months ago

Selected Answer: B

Definitely B

upvoted 2 times

 **kfrum4** 2 years, 6 months ago

Selected Answer: B

Answer: B

upvoted 1 times

 **AMEJack** 2 years, 7 months ago

Selected Answer: B

Answer is B

upvoted 2 times

 **Roontha** 2 years, 7 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.

Correct Answer: C

Community vote distribution

C (100%)

 **dkx** Highly Voted 1 year, 5 months 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 11 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: C

AWS WAF's managed SQL injection rule group automatically blocks SQL injection attacks while allowing legitimate traffic, with low operational overhead.

A only monitors, no blocking.

B focuses on bots, not SQLi.

D is manual and high-maintenance.

upvoted 1 times

 **career360guru** 1 year, 1 month ago

Selected Answer: C

Option C

upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: C

C 100%

upvoted 1 times

 **pupsik** 1 year, 6 months ago

Selected Answer: C

C for sure

upvoted 1 times

 **Alabi** 1 year, 6 months ago

Selected Answer: C

C for sure

upvoted 1 times

 **nexus2020** 1 year, 6 months 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 3 times

 **Snap** 1 year, 7 months 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** 1 year, 7 months ago

why not B?

upvoted 1 times

 **AMEJack** 1 year, 7 months ago

Selected Answer: C

Answer is C

upvoted 1 times

 **Roontha** 1 year, 7 months ago

Answer : C

<https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-use-case.html>

upvoted 4 times

 **deegadaze1** 1 year, 7 months ago

B- is correct---> AWS WAF Bot Control

upvoted 1 times

Question #184

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.

Correct Answer: C

Community vote distribution

C (100%)

 **F_Eldin** Highly Voted 2 years, 7 months 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 9 times

 **ShenYuying** 1 year, 5 months ago

The above URL is not available now. You can refer to this URL: <https://aws.amazon.com/blogs/iot/how-to-implement-a-disaster-recovery-solution-for-iot-platforms-on-aws/>

upvoted 1 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: C

IOT Core endpoints in both Regions with Route 53 failover for ingestion and DynamoDB global tables for multi-Region replication, giving both ingestion and storage continuity.

A/B use wrong database engines.

D misuses DynamoDB Streams; global tables are the right solution.

upvoted 1 times

 **JosephDZhou** 1 year, 11 months ago

For C, how failover routing policy have the ability to ingest and store data in two AWS Regions, there is only one active record

upvoted 3 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C Business continuity = Failover -> DynamoDB Global DB

upvoted 4 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

its a C

upvoted 3 times

 **Maria2023** 2 years, 6 months ago

Selected Answer: C

The only answer which configures DynamoDB properly for multi-region is C

upvoted 2 times

 **rbm2023** 2 years, 7 months ago

Selected Answer: C
Removed B because is replacing Dynamo, unnecessary
upvoted 2 times

 **andreitugui** 2 years, 7 months ago

Selected Answer: C
Answer is C
upvoted 2 times

 **Roontha** 2 years, 7 months ago

Answer: C
upvoted 1 times

Question #185

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.

Correct Answer: B

Community vote distribution

B (88%)

12%

 **andreitugui** Highly Voted  2 years, 7 months ago

Selected Answer: B

Answer is B

upvoted 10 times

 **princajen** Most Recent  4 months, 1 week ago

Selected Answer: B

DynamoDB's fine-grained access control is done with IAM policy conditions on the accessing role, and cross-account access is delivered by STS role assumption into the resource owner account. SCPs don't grant access (A), DynamoDB doesn't support resource-based policies (C), and permissions boundaries aren't for attribute-level cross-account access (D).

upvoted 1 times

 **pk0619** 1 year ago

Selected Answer: C

B was right answer until DynamoDB started supporting resource based policies, which makes C right.

upvoted 1 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: B

I prefer B over C. Attach the policy (specific DynamoDB attributes) to the DynamoDB table. This will result in the finance team's account not being able to fully access DynamoDB.

upvoted 1 times

 **fartosh** 1 year, 7 months ago

Selected Answer: C

I choose C over B.

Both solutions work and are standard approaches for allowing cross-account access. But as compared to S3, option C allows the marketing account to use their usual IAM identities without compromising their permissions. When you assume the role in a different account (option B), you can no longer access resources in your own account.

The resource-based policy for the DynamoDB table supports conditions as well:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/rbac-examples.html#rbac-examples-cross-account>

upvoted 2 times

 **helloworldabc** 1 year, 4 months ago

just B

upvoted 1 times

✉ **kgpoj** 1 year, 3 months ago

Dude stop generating garbage info for everyone. I've seen you replying a lot of 'just X'. If you have a reason for some choice, then write it down. 'just x' sounds so dumb and premature.

upvoted 13 times

✉ **sse69** 1 year, 7 months ago

Selected Answer: B

Starting march 24', DynamoDB supports resource based policies :

<https://aws.amazon.com/about-aws/whats-new/2024/03/amazon-dynamodb-resource-based-policies/>

So another way to achieve this would be to create an index for the marketing team, and have the policy restrict their role to that particular index.

On the one hand the new index would incur more costs, on the other hand, having only certain attributes fetched would mean less read units consumed...

upvoted 3 times

✉ **yuliaqwerty** 2 years ago

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

upvoted 3 times

✉ **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B as DynamoDB does not support Resource based policies.

upvoted 2 times

✉ **LuongTo** 1 year ago

Amazon DynamoDB now supports resource-based policies from Mar 20, 2014 <https://aws.amazon.com/about-aws/whats-new/2024/03/amazon-dynamodb-resource-based-policies/>

upvoted 1 times

✉ **erenbiku1** 2 years ago

Service-linked roles for DynamoDB is not supported

Service roles for DynamoDB is supported

Identity-based policies for DynamoDB is supported

Resource-based policies within DynamoDB is not supported

upvoted 1 times

✉ **AMohanty** 2 years, 4 months 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** 2 years, 3 months 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 years, 5 months ago

Correct C.

upvoted 1 times

✉ **Gmail78** 2 years, 4 months 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** 2 years, 4 months ago

No, Resource based policies can specify which Principals to give access to Cross Account.

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B. DynamoDB fine-grained access using IAM

upvoted 1 times

✉ **SkyZeroZx** 2 years, 5 months ago

Selected Answer: B

B for sure.

Key word: trust

upvoted 3 times

✉ **Maria2023** 2 years, 6 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 3 times

 **0c118eb** 2 years ago

This would not be a good use case for permissions boundaries by itself. Even with permissions boundaries you would still need to implement a solution like B to provide the required permissions.

upvoted 1 times

 **Alabi** 2 years, 6 months ago

Selected Answer: B

B for sure.

Key word: trust

upvoted 3 times

 **kfrum4** 2 years, 6 months 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 2 times

 **ggrodskiy** 2 years, 5 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** 2 years, 6 months ago

Selected Answer: C

Resource-based IAM policy

upvoted 1 times

 **Roontha** 2 years, 7 months ago

Answer : B

upvoted 2 times

Question #186

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

Correct Answer: ABE

Community vote distribution

ABE (100%)

 **chathur** Highly Voted 1 year, 6 months 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 18 times

 **SkyZeroZx** Highly Voted 1 year, 5 months 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 7 times

 **career360guru** Most Recent 1 year, 1 month ago

Selected Answer: ABE

A, B, E

upvoted 1 times

 **SK_Tyagi** 1 year, 4 months ago

Selected Answer: ABE

Reason as explained by everyone

upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: ABE

ABE for sure

upvoted 1 times

 **rbm2023** 1 year, 7 months 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** 1 year, 6 months ago

yes, Cross Region Replication can be implemented only when the versioning of both the buckets is enabled.
upvoted 2 times

 **Snape** 1 year, 7 months 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 5 times

 **F_Eldin** 1 year, 7 months 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** 1 year, 7 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** 1 year, 7 months ago

Selected Answer: ABE

Answer is A B E

upvoted 1 times

 **Roontha** 1 year, 7 months ago

Answer : A,B,E

upvoted 2 times

Question #187

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

Correct Answer: BDE*Community vote distribution*

BDE (100%)

 **rbm2023** Highly Voted 1 year, 7 months 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 6 times

 **career360guru** Most Recent 1 year, 1 month ago

Selected Answer: BDE

B, D, E
upvoted 3 times

 **SK_Tyagi** 1 year, 4 months ago

Selected Answer: BDE

F is EKS on EC2 and question is Least Operational overhead
upvoted 3 times

 **softarts** 1 year, 4 months ago

E=> how does step function run periodic jobs?
upvoted 1 times

 **ggrodsckiy** 1 year, 5 months ago

Correct BDE.
upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: BDE

BDE for sure
upvoted 2 times

 **andreitugui** 1 year, 7 months ago

Selected Answer: BDE

Answer is B D E

upvoted 1 times

 **AMEJack** 1 year, 7 months ago

Selected Answer: BDE

Support B D E

upvoted 3 times

 **Roontha** 1 year, 7 months ago

Answer : B,D,E

<https://aws.amazon.com/step-functions/use-cases/>

upvoted 4 times

 **deegadaze1** 1 year, 7 months ago

Correct is ABD

upvoted 1 times

 **ShinLi** 1 year, 7 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.

Correct Answer: C

Community vote distribution

C (79%)

D (21%)

 geoakes Highly Voted 1 year, 7 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 13 times

 pk0619 Most Recent 1 year ago

Selected Answer: D

Local zone provides that low latency without having to manage the infrastructure

upvoted 1 times

 career360guru 1 year, 1 month ago

Selected Answer: C

Option C

upvoted 1 times

 SK_Tyagi 1 year, 4 months ago

Selected Answer: C

Wavelength doesn't make sense here

upvoted 1 times

 NikkyDicky 1 year, 5 months ago

Selected Answer: C

C works

upvoted 1 times

 pupsk 1 year, 6 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** 1 year, 7 months 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** 1 year, 7 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** 1 year, 7 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, require 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** 1 year, 7 months ago

Selected Answer: D

Local Zone reduce the latency issue
upvoted 4 times

✉  **ShinLi** 1 year, 7 months ago

<https://docs.aws.amazon.com/wavelength/latest/developerguide/what-is-wavelength.html>

upvoted 1 times

✉  **Roontha** 1 year, 6 months 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** 1 year, 7 months ago

Wavelength is not present in every country with a datacenter, so B and D options are automatically wrong

upvoted 1 times

✉  **Roontha** 1 year, 7 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

✉  **geoakes** 1 year, 7 months ago

Yes, a local zone reduces latency, but local zone are not in every country. The closest thing to an every country option is Snowball and Outpost

upvoted 1 times

Question #189

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.

Correct Answer: AE*Community vote distribution*

AE (78%)

BE (22%)

 **Jackhemo** Highly Voted 2 years, 6 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 6 times

 **Iunt** Most Recent 2 weeks ago

Selected Answer: AE

Concentrate on the misread & misdirect.

Must prevent attacks + ensure BC with minimal service interruptions during an ongoing attack.

- A. Protects against CF bypass attacks, or direc to ALB if attacker can scrape the ALB name. Custom headers.
- B. BC = yes but this also costs more and widens the attack surface. Are you really going to ask the attacker - attack region A but leave region B alone please? Nope.
- C. DAX is expensive - no justification. Nope.
- D. Nope.

E. This covers BC > ECS cluster never sees bad traffic = cannot overwhelm with bad requests. This is the misdirect - when the question states ensure bc - you are automatically thinking I need to select specific option so go for B, B is HA not security mitigation.

Pay attention to the words then how AWS describes the tech. When all else fails default to AWS design patterns - even if other options sound better CF + WAF is well known DP.

AE

upvoted 1 times

 **princajen** 4 months, 1 week ago

Selected Answer: AE

Put CloudFront + WAF in front of the ALB to filter attacks at the edge and prevent ALB bypass with a custom header (A, E).

This combo is most cost-effective: uses managed, pay-as-you-go security at the edge rather than expensive multi-Region or unnecessary caching layers that don't stop attacks.

upvoted 1 times

 **sammyhaj** 1 year ago

Selected Answer: BE

broken question

B has business continuity

E must be chosen

A has no business continuity, just recovery or mitigation

upvoted 2 times

 **43c89f4** 1 year, 8 months ago

simple BCD are not at all related to question

upvoted 1 times

 **Russ99** 2 years ago

Selected Answer: BE

none of the previous responses really make use of Business continuity as indicated in the scenario. my picks are options B and E. The combination of these two options (E and B) provides both security (via AWS WAF) and high availability (via multi-region deployment) for your application. It helps in preventing attacks and ensuring business continuity with minimal service interruptions during ongoing attacks, making it a cost-effective choice.

upvoted 3 times

 **kejam** 1 year, 11 months ago

Can't use E without A. E depends on A for the CloudFront distribution.

upvoted 8 times

 **career360guru** 2 years, 1 month ago

Selected Answer: AE

A and E

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: AE

its AE

upvoted 2 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: AE

The only options that helps to protect are A E

upvoted 1 times

 **rbm2023** 2 years, 7 months 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 4 times

 **andreitugui** 2 years, 7 months ago

Selected Answer: AE

The only options that helps to protect are A E

upvoted 2 times

 **Roontha** 2 years, 7 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.

Correct Answer: C

Community vote distribution

C (73%)

D (27%)

 **pupsik**  2 years, 6 months ago

Selected Answer: C

Origin Groups in CloudFront is what we need here.

upvoted 6 times

 **Jackhemo**  2 years, 6 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 5 times

 **princajen**  4 months, 1 week ago

Selected Answer: C

Use CloudFront origin failover with ALB primary and S3 static website secondary so that on ALB 503, CloudFront immediately serves your custom error page from S3—fast, simple, least ops.

upvoted 1 times

 **chris_spencer** 1 year, 2 months ago

Selected Answer: C

C because of custom error pages

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

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: D

A and B are plainly wrong and can be eliminated straight away. The choice therefore is between C and D. The question asks for an immediate display of a custom error page - NOT about permanent failover. Therefore, the correct answer is D.

upvoted 4 times

 **altonh** 11 months, 1 week ago

D is wrong because of this statement: "Update the function to read the S3 bucket and serve the error page to the end users." CloudFront function cannot do any network access.

upvoted 1 times

 **fartosh** 1 year, 7 months ago

According to https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html CloudFront always tries to serve the content from the primary origin first.

> CloudFront routes all incoming requests to the primary origin, even when a previous request failed over to the secondary origin. CloudFront only sends requests to the secondary origin after a request to the primary origin fails.

Therefore option C is still valid as it does not leave CloudFront in "permanent failover".

upvoted 1 times

 **chelbsik** 1 year, 11 months ago

Selected Answer: D

I go for D: it contains all steps to setup the requested solution, and CloudFront function suits here

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

"URL redirects or rewrites – You can redirect viewers to other pages based on information in the request, or rewrite all requests from one path to another".

upvoted 1 times

 **AimarLeo** 1 year, 11 months ago

Selected Answer: D

'The company wants to display a custom error message page when these errors occur. The page should be displayed immediately for this error code.' The purpose of the question obviously is to return that error page not really a FAILOVER mechanism --> Leaves D as an answer

upvoted 3 times

 **carpa_jo** 1 year, 12 months ago

For people are asking why C is better than A:

The approach of A is more suited for scenarios where there is a complete failure of the primary endpoint rather than intermittent errors. The health checks may not register a failure if the 502 errors are sporadic and the system is generally operational, thus the failover might not be triggered.

With the approach of C CloudFront will always automatically switch to the secondary origin when the primary origin returns specific HTTP status code failure responses.

upvoted 3 times

 **Niko13** 2 years ago

Selected Answer: C

Least Operational Overhead is C

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Least Operational Overhead is C

upvoted 2 times

 **KCjoe** 2 years, 2 months ago

I know C is good, but why not A, seems to me A is much easier.

upvoted 1 times

 **SuperDuperPooperScooper** 2 years, 1 month ago

Route 53 failover will not be as immediate as C. Cloudfront will immediately seerve up the error page if the request to the primary origin fails, so there is no delay between the primary origin health being degraded and the failover page being served.

upvoted 2 times

 **bur4an** 2 years, 3 months ago

Repeat question?

upvoted 1 times

 **kjcncjek** 2 years, 3 months ago

why not A?

upvoted 3 times

 **hamimelon** 1 year, 2 months ago

Route 53 fail over to S3? How can Route 53 display the image?

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

it's a C

upvoted 2 times

 **rbm2023** 2 years, 7 months ago

Almost went for D but this would take too much operational overhead.

upvoted 2 times

 **rbm2023** 2 years, 7 months ago

Option C

upvoted 1 times

 **andreitugui** 2 years, 7 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 3 times

 **Roontha** 2 years, 7 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.

Correct Answer: A*Community vote distribution*

A (100%)

 **princajen** 4 months, 1 week ago

Selected Answer: A

(ECS Fargate + EFS) because the question requires no infrastructure management (Fargate) and an NFSv4 file share (EFS). B uses the wrong storage (Lustre), C/D require managing EC2, and D uses block storage (EBS) rather than NFS.

upvoted 1 times

 **chris_spencer** 1 year, 2 months ago

It's very easy... you read docker => ECS. NFS => EFS, no underlaying infrastructure => Fargate

upvoted 1 times

 **saggy4** 1 year, 10 months ago

Selected Answer: A

C and D: Both these options have hassles of EC2 management

Between A and B: Mounting FSx for Lustre on an AWS Fargate launch type isn't supported.

Hence the correct option is A

upvoted 3 times

 **Niko13** 2 years ago

Selected Answer: A

ECS, EFS - answer A

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

Option A -

EFS = NFS 4

Fargate = No mgmt or provisioning overheads for servers

upvoted 3 times

 **Christina666** 2 years, 5 months ago

Selected Answer: A

Amazon EFS is a managed NAS filer for EC2 instances based on Network File System (NFS) version 4.

upvoted 4 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

A for sure
upvoted 1 times

 **SkyZeroZx** 2 years, 5 months 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 years, 5 months 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** 2 years, 6 months ago

Selected Answer: A

<https://aws.amazon.com/fsx/when-to-choose-fsx/>
upvoted 2 times

 **rbm2023** 2 years, 7 months 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** 2 years, 7 months ago

Selected Answer: A

The correct answer is A, fargate(no infra management) & efs for NFSv4
upvoted 2 times

 **deegadaze1** 2 years, 7 months ago

A is correct due to -- NFS version 4.
upvoted 3 times

 **Roontha** 2 years, 7 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.

Correct Answer: B*Community vote distribution*

B (100%)

✉️  **princajen** 4 months, 1 week ago

Selected Answer: B

ALB weighted target groups give an exact 90/10 traffic split, and ALB target group stickiness keeps each customer on the same version for the testing window. Route 53 weighting (A) isn't user-sticky, rolling updates (C) control instances not customer percentage, and changing to LOR (D) doesn't provide precise canary percentage.

upvoted 1 times

✉️  **career360guru** 1 year, 1 month ago

Selected Answer: B

B is better option considering the fact that a customer should get same business logic during testing window. This means we need session stickiness that only option B can provide.

upvoted 4 times

✉️  **Pupu86** 1 year, 1 month ago

Selected Answer: B

This is canary deployment not blue/green

upvoted 3 times

✉️  **joleneinthebackyard** 1 year, 1 month ago

Selected Answer: B

I was struggled between A and B because I overlooked this line "A customer must use the same version of the business logic during the testing window."

So we need session stickiness in place, then B is the obvious choice.

upvoted 1 times

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

Oops. It does mention stickiness...

upvoted 1 times

✉️  **ggrodsckiy** 1 year, 5 months ago

Correct B.

upvoted 1 times

✉  **NikkyDicky** 1 year, 5 months ago

Selected Answer: B

B better

upvoted 1 times

✉  **SkyZeroZx** 1 year, 6 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 aproiate is ALB with stickiness

upvoted 2 times

✉  **Maria2023** 1 year, 6 months ago

Selected Answer: B

<https://docs.aws.amazon.com/prescriptive-guidance/latest/load-balancer-stickiness/target-group-stickiness.html>

upvoted 1 times

✉  **rbm2023** 1 year, 7 months ago

Selected Answer: B

Agree with B

blue green deployment, using target group

upvoted 4 times

✉  **rbm2023** 1 year, 7 months ago

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/>

upvoted 3 times

✉  **F_Eldin** 1 year, 7 months ago

Selected Answer: B

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/>

upvoted 4 times

✉  **Roontha** 1 year, 7 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

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.

Correct Answer: B

Community vote distribution

B (50%)

A (50%)

 **F_Eldin** Highly Voted 2 years, 7 months 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 18 times

 **Sab** 2 years, 2 months ago

Storage type can be modified

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-type.html>

upvoted 8 times

 **AK2020** 2 years, 2 months ago

You can change your file system storage type from HDD to SSD using the Amazon FSx console or Amazon FSx API. You can't change your file system storage type from SSD to HDD. So A is correct as we can do this during the downtime

upvoted 3 times

 **AK2020** 2 years, 2 months ago

So B is correct. my apologies

upvoted 2 times

 **Andres123456** Highly Voted 2 years, 1 month ago

Selected Answer: B

Storage type can be modified

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-type.html>

upvoted 10 times

 **evargasbrz** Most Recent 2 weeks, 4 days ago

Selected Answer: B

B is the right!

Let me clarify - the ability to change storage type depends on which FSx file system type you're using:

FSx for Windows File Server: Yes (with limitations)
- You CAN switch from HDD to SSD storage type

- Available since a feature update in 2022
 - Done through console or CLI using the "Update storage type" option
 - The process involves data migration in the background
 - May take several hours depending on data size
 - File system remains available during the switch
- upvoted 1 times

Murtuza 1 month, 3 weeks ago

Selected Answer: B

Historically (pre-2023), Option A was correct, because FSx didn't support in-place conversion — you had to restore to a new file system.

However, AWS updated FSx for Windows File Server to support:

Throughput scaling in place (2021)

HDD → SSD storage type updates in place (2023+)

Therefore, as of 2025 exams, AWS expects you to know the current capability.

upvoted 1 times

Murtuza 3 months, 2 weeks ago

Selected Answer: B

B makes sense

upvoted 1 times

princajen 4 months, 1 week ago

Selected Answer: B

FSx for Windows File Server now allows HDD → SSD conversion and throughput scaling in-place. That makes it a single operation during a maintenance window, which is less effort than backup/restore (A). Options C and D add complexity without solving the core performance problem.

<https://aws.amazon.com/fsx/windows/faqs/#topic-1>

upvoted 1 times

matt200 4 months, 2 weeks ago

Selected Answer: A

The best option with the least administrative effort to improve the performance of the FSx for Windows File Server file system configured on HDD storage with 16 MBps throughput is: A

Why other options are less suitable:

B: You cannot modify storage type or throughput capacity in-place via console or API for FSx for Windows File Server; these require creating a new file system.

C: Using DataSync adds operational complexity (agent setup, task scheduling) and is not necessary since AWS Backup supports FSx.

D: Shadow copies are for point-in-time snaps inside Windows file systems, not for migrating or upgrading FSx file systems or storage types.

upvoted 1 times

0dc6cac 6 months, 2 weeks ago

Selected Answer: B

Tough question, in 10/10 cases I would pick A over B, it's objectively the more appropriate method. However, B technically requires a step or two less than A to perform. It also depends on how much administrative load will be added during the downtime (it can be long, because AWS sometimes takes forever to stop and start stuff).

So if we assume no time constraint, and no issues with downtime, B is correct. In reality, it's always going to be A.

upvoted 1 times

Kaps443 6 months, 2 weeks ago

Selected Answer: A

B is Incorrect: You cannot change the storage type from HDD to SSD after creation of the FSx file system.

upvoted 2 times

820b83f 10 months, 2 weeks ago

Selected Answer: A

My reasons for its A:

1. FSx does not support live storage type changes from HDD to SSD. You must create a new file system.

upvoted 2 times

bhanus 12 months ago

Selected Answer: B

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/updating-storage-type.html>

HDD can be changed to SSD

upvoted 1 times

✉ **SIJUTHOMASP** 1 year ago

Selected Answer: B

Comparing between A and B, the trade-off decision would be on the key requirement for 'least administrative efforts'. Which seems to be lesser in B, because it's single step but on the other hand on A, there are multiple steps of backup, creating new FSx etc should be of more admin efforts. Hence B.

upvoted 1 times

✉ **pk0619** 1 year ago

Selected Answer: B

You can update both throughput capacity as well as storage capacity of an existing filesystem

upvoted 1 times

✉ **LuongTo** 1 year ago

Selected Answer: B

SSD to HDD is impossible, but HDD to SSD is okay => B is feasible.

B is less effort since B just disconnects users from the file system for a while, and then updates the FSx. While A needs a new FSx, backup, restore, clean up then switch, more steps to do than A

upvoted 2 times

✉ **FZA24** 1 year, 1 month ago

Selected Answer: A

Let consider that B is correct (updating storage type is possible).

Between A and B, A needs the LEAST administrative effort.

A is seamless for users. However, B requires to disconnect users and thus service interruption and administrative effort to manage that!

upvoted 2 times

✉ **Sin_Dan** 1 year, 2 months ago

Selected Answer: A

I pity those who are selecting B.

updating the storage type (from HDD to SSD) is not supported for an existing FSx for Windows File Server file system. You would need to create a new file system to change the storage type. Therefore, this solution is not feasible.

upvoted 2 times

✉ **Zinnia_Wang** 1 year ago

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/updating-storage-type.html>

upvoted 1 times

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

Selected Answer: B

"You CAN CHANGE your file system storage type from HDD to SSD using the AWS Management Console and AWS CLI."

"You CANNOT CHANGE your file system storage type from SSD to HDD."

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-configuration.html#managing-storage-type>

upvoted 1 times

Question #194

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.

Correct Answer: B*Community vote distribution*

B (86%)

14%

✉ EzKkk 2 weeks, 2 days ago

Selected Answer: B

At first, I chose C because it has the least operational overhead, then I thought B should be a better choice
upvoted 1 times

✉ princajen 4 months, 1 week ago

Selected Answer: B

S3 Multi-Region Access Points + bidirectional CRR is the AWS-native way to run an application across two Regions with minimal overhead. A fails on writes, C isn't symmetric (adds ops burden), and D is irrelevant.
upvoted 1 times

✉ a54b16f 1 year, 9 months ago

Selected Answer: B

C is missing "bidirectional S3 Cross-Region Replication"
upvoted 2 times

✉ career360guru 2 years, 1 month ago

Selected Answer: B

B is always a better option. C is possible but less preferred.
Irrespective of B or C application will need modification to deploy in 2nd region as Bucket URL has to be change in application.
upvoted 3 times

✉ Russ99 2 years, 2 months ago

Selected Answer: C

An S3 Multi-Region Access Point is a global endpoint that provides access to data in one or more S3 buckets. To create an S3 Multi-Region Access Point, you must specify a set of S3 buckets that you want to include in the Multi-Region Access Point. You must also configure routing rules to determine which requests are routed to which S3 buckets.

Once you have created an S3 Multi-Region Access Point, you must modify your application to use the Multi-Region Access Point endpoint instead of the S3 bucket endpoints. This requires changes to your application code and configuration.

Option C does not require the creation of an S3 Multi-Region Access Point. Instead, you can simply deploy the application in two Regions and configure the application to use the S3 bucket endpoints in each Region. This is a simpler and more straightforward approach, which reduces operational overhead.

upvoted 3 times

✉ carpa_jo 1 year, 12 months ago

Option C includes "Set up S3 Cross-Region Replication (CRR) from the original S3 bucket to the new S3 bucket". By that the application in the new region will have access to the files from the "old" and the new region, and the application running in the "old" region only has access to the data of the "old" region, as no bidirectional CRR is being set up. That doesn't make a lot of sense. Option B contains bidirectional CRR which keeps both buckets in sync.

upvoted 3 times

✉ helloworldabc 1 year, 4 months ago

just B

upvoted 1 times

✉ **MasterP007** 2 years, 4 months 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 4 times

✉ **azizmo** 2 years, 5 months ago

Selected Answer: B

The answer is B

upvoted 1 times

✉ **nicecurls** 2 years, 5 months ago

Selected Answer: B

it's a B

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

its a B

upvoted 2 times

✉ **NikkyDicky** 2 years, 5 months 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 3 times

✉ **phattran** 2 years, 5 months ago

Selected Answer: B

S3 CRR prefer S3 Multi-Region Access Point

upvoted 3 times

✉ **YodaMaster** 2 years, 5 months ago

B sounds right for deploying in 2 different regions though.

upvoted 1 times

✉ **YodaMaster** 2 years, 5 months ago

this question seems incomplete?

upvoted 1 times

✉ **Masonryeho** 2 years, 7 months ago

B, enable the S3 sync

upvoted 3 times

✉ **Roontha** 2 years, 7 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.

Correct Answer: C

Community vote distribution

C (100%)

 **Roontha** Highly Voted 2 years, 1 month ago

Answer : C

<https://aws.amazon.com/blogs/database/building-a-real-time-gaming-leaderboard-with-amazon-elasticsearch-for-redis/>
upvoted 12 times

 **rbm2023** Highly Voted 2 years 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 5 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: C

the question stresses high-performance compute and fast-changing leaderboard. C5 instances (compute optimized) with On-Demand reliability meet the HPC requirement, and ElastiCache for Redis is the AWS-native solution for real-time leaderboards. A and D use the wrong instance family, B uses the wrong data store, and Spot Instances (A, B) are not reliable enough for a gaming platform.
upvoted 1 times

 **Win007** 1 year ago

D is the write answer
upvoted 1 times

 **voccer** 1 year, 5 months ago

Answer: C
B/c: not use spot instance
upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: C

Option C
upvoted 1 times

 **dkcloudguru** 1 year, 9 months ago

Agree with option C
upvoted 1 times

 **SK_Tyagi** 1 year, 10 months ago

Selected Answer: C

Agree with C.
upvoted 1 times

 **ggrodskiy** 1 year, 11 months ago

Correct C.
upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: C
C for sure
upvoted 1 times

 **YodaMaster** 1 year, 11 months ago

Selected Answer: C
C is the way
upvoted 1 times

 **Alabi** 2 years ago

Selected Answer: C
C for sure
upvoted 1 times

 **F_Eldin** 2 years ago

Selected Answer: C
A, B : Wrong. Spot instances. B: OpeSearch instead of Redis
D: Wrong, DynamoDB instead of Redis
upvoted 2 times

 **andreitugui** 2 years ago

Selected Answer: C
The answer is C as compute optimized instance is required c5, and ElastiCache is the for Redis.
upvoted 2 times

 **Masonryeho** 2 years, 1 month ago

Agree with C
upvoted 2 times

Question #196

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.

Correct Answer: CE

Community vote distribution

CE (48%)	BE (43%)	6%
----------	----------	----

 **emiliocb4** Highly Voted  2 years, 6 months 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 20 times

 **altonh** 11 months, 1 week ago
 C implies that the front end is static while the back end is dynamic.
 upvoted 1 times

 **Gmail78** 2 years, 4 months 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

 **YodaMaster** Highly Voted  2 years, 5 months 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 12 times

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

Selected Answer: CE
 exam's "minimize operational overhead" means serveless this the biggest clue
 upvoted 1 times

 **princaben** 4 months, 1 week ago

Selected Answer: CE
 Choose serverless (C+E) because:
 C handles unpredictable spikes with auto-scaling Lambda + API Gateway, while keeping ops near zero.
 E provides cheap, scalable reporting using Athena + QuickSight without cluster mgmt.

B+E is acceptable but less aligned with the exam's "minimize operational overhead" keyword.

upvoted 1 times

 **4845c28** 4 months, 2 weeks ago

Selected Answer: BE

C is complete nonsense

upvoted 2 times

 **0dc6cac** 6 months, 1 week ago

Selected Answer: BE

BE, there's nothing saying that the frontend is static, and nothing saying that we need to have an API backend. B is much more flexible than C.

upvoted 1 times

 **Kaps443** 6 months, 2 weeks ago

Selected Answer: CE

C is best for frontend/API

E is best for storage + reports

upvoted 2 times

 **JaffaDaffa** 12 months ago

Selected Answer: CE

C is better option than B bcz it is managed/serverless than ECS (without mentioning Fargate)

upvoted 2 times

 **JaffaDaffa** 12 months ago

Selected Answer: CE

B is not right option as ECS management overhead unless specified with Fargate Launch type.

upvoted 2 times

 **deepakR20** 1 year ago

Selected Answer: BE

Key parameter is " with most of the submissions occurring on Friday." hence BE is the right answer

upvoted 1 times

 **LuongTo** 1 year ago

Selected Answer: BE

E is apparently.

I would go for B rather than C. Even serverless lambda is best suited for minimizing operational overhead; however the point is "mobile devices"; the mobile application is the frontend => "Deploy the application front end to an Amazon S3 bucket served by Amazon CloudFront" from C does not make sense.

upvoted 1 times

 **youonebe** 1 year, 1 month ago

Selected Answer: CE

CE-CE-CE

upvoted 2 times

 **zersa** 1 year, 1 month ago

Selected Answer: BE

i'm going with BE.

upvoted 1 times

 **Halliphax** 1 year, 1 month ago

Selected Answer: BE

High availability = multiple availability zones (clue in the answer, B)

Cannot be C as it's a web application so cannot be on S3. Lambda not suitable either because Lambdas only run in a single chosen region of deployment.

upvoted 1 times

 **LuongTo** 1 year ago

C feasible. Frontend (html, js) will be in S3 with Cloudfront, lambda for backend. Lambda is the best approach for "minimizing operational overhead". The "requirement" here is about high-availability not DR which requires multi-region

upvoted 2 times

 **0b43291** 1 year, 1 month ago

Selected Answer: CE

Option A (EC2 On-Demand Instances with Auto Scaling) requires managing and scaling EC2 instances, which adds operational overhead compared to a serverless approach.

Option B (Amazon ECS with Service Auto Scaling) also requires managing and scaling container instances, which adds operational overhead compared to a serverless approach.

Option D (Amazon Redshift) is a data warehousing solution better suited for large-scale analytics workloads, which may be overkill for the

given requirements and introduce unnecessary complexity and cost.

By choosing the combination of options C and E, the solutions architect can implement a highly available, scalable, and cost-effective solution with minimal operational overhead, leveraging the benefits of serverless computing, object storage, and managed analytics services.

upvoted 2 times

 **sashenka** 1 year, 2 months ago

Selected Answer: CE

Options A and B involve managing EC2 instances or containers, which would require more operational effort than a fully serverless solution with C and E.

upvoted 2 times

 **AWSum1** 1 year, 2 months ago

Selected Answer: BE

It's B & E, the question says that timeshares will need to be submitted. Therefore making it dynamic.

Selecting option C to use S3 to host webapp can't work because S3 can host static sites.

upvoted 1 times

Question #197

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.

Correct Answer: ADF

Community vote distribution

ADF (61%) BDF (37%)

 **cmoreira**  2 years, 3 months 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 13 times

 **kaby1987**  2 years ago

Selected Answer: ADF

ADF are correct choices.

upvoted 7 times

 **4a86914**  3 months ago

Selected Answer: ADF

Bad question. Anyway, A, D, F are the correct answers for the context of this question. B is incorrect, as S3 server access log is based on best-effort basis. There is a chance security team may not get notified.

However, in real-life, even CloudTrails may not provide the absolute details an auditor may come to expect: <https://repost.aws/knowledge-center/s3-audit-deleted-missing-objects>

upvoted 1 times

 **princajen** 4 months, 1 week ago

Selected Answer: ADF

CloudTrail (A) = required for object-level activity logs.

EventBridge → SNS (D) = best way to notify security team on delete events (email).

S3 + lifecycle (F) = cheapest way to retain logs for 5 years.

Don't pick B (server access logs, redundant), C (invalid SES flow), or E (Timestream, too costly)

upvoted 1 times

 **altonh** 10 months ago

Selected Answer: BDF

The requirement is for the most cost-effective.

A - You will pay for the data event delivered to S3

C - No integration to SES

D - Paying more for Timestream

upvoted 1 times

 **altonh** 10 months ago

The requirement is for the most cost-effective.

A - You will pay for the data event delivered to S3

C - No integration to SES
E - Paying more for Timestream
upvoted 1 times

 **820b83f** 10 months, 2 weeks ago

Selected Answer: ADF

The conflict is between AWS Cloudtrail (A) and S3 Server Access Log (B).
B is incorrect because S3 Server access logs track requests at the bucket level, not object-level operations (e.g., deletions).

A is correct because CloudTrail is required for detailed tracking including object level.
upvoted 1 times

 **altonh** 11 months, 1 week ago

Selected Answer: BDF

BDF flows well. ADF, however, does not provide details on how you will store the logs in the new S3 bucket.
upvoted 1 times

 **HSong** 1 year, 3 months ago

"We recommend that you use CloudTrail for logging bucket-level and object-level actions for your Amazon S3 resources."
upvoted 3 times

 **dragongoseki** 1 year, 6 months ago

Selected Answer: ADE

ADF is right answer.
upvoted 1 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: BDF

Both A and B can log s3 activities. Difference is A real time log but cost more. B log has delay but cheaper. The requirement is the most cost-effective so choose B to meet this requirement.
upvoted 4 times

 **seetpt** 1 year, 7 months ago

Selected Answer: ADF

ADF logs everything, BDF doesn't.
upvoted 3 times

 **titi_r** 1 year, 9 months ago

Selected Answer: BDF

BDF meet the requirements.
upvoted 3 times

 **liquen14** 1 year, 9 months ago

Selected Answer: ADF

Probably B is cheaper but A is safer and more accurate and remember the "The company must log ALL activities for objects"

According to this <https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerLogs.html#LogDeliveryBestEffort>

"The log record for a particular request might be delivered long after the request was actually processed, or it might not be delivered at all."

so for me is A not B
upvoted 5 times

 **Russss99** 1 year, 10 months ago

Selected Answer: BDF

Given the requirement to log all activities for objects in an S3 bucket and keep logs for 5 years, combined with a focus on cost-effectiveness, S3 server access logging (Option B) would indeed be a cheaper solution for capturing basic access logs. However, for advanced auditing and compliance requirements where detailed API call tracking is needed, CloudTrail's data event logging provides valuable insights that S3 access logs do not.
upvoted 4 times

 **ninomfr64** 1 year, 11 months ago

Selected Answer: BDF

B is cheaper than A
AWS CloudTrail (A) - Management events (first delivery) are free; data events incur a fee, in addition to storage of logs
S3 Server Logs (B) - No other cost in addition to storage of logs

[https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html#:~:text=S3%20Server%20Logs-,Price,-Management%20events%20\(first](https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html#:~:text=S3%20Server%20Logs-,Price,-Management%20events%20(first)
upvoted 1 times

 **gagol14** 1 year, 11 months ago

Selected Answer: ADF

For capturing object-level events, such as object deletions, you would typically use Amazon S3 Event Notifications or enable AWS CloudTrail data events for S3.

upvoted 4 times

 **Jane1234YIP** 1 year, 11 months ago

S3 server access logging does not capture object-level events like object deletions. so I will go ADF.

upvoted 3 times

 **cox1960** 1 year, 11 months ago

wrong. check "operation" in <https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html>
BDF

upvoted 5 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.

Correct Answer: AD

Community vote distribution

AD (100%)

 **cmoreira** Highly Voted 2 years, 3 months 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 26 times

 **GabrielShiao** 11 months, 2 weeks ago

Vote D.

You can access the AWS public resources if you create a public VIF well. By setting the AWS site-to-set VPN, one of AWS's public resources, you can leverage this VPN to connect to the multiple VPC accordingly.

upvoted 2 times

 **Roontha** Highly Voted 2 years, 7 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 12 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: AD

DXGW (A) = cheapest way to extend a single DX to multiple cross-Region VPCs (private access).

Public VIF (D) = cost-effective access to AWS public services via the same DX.

Avoid B (extra circuits \$\$), C/E (wrong patterns / won't meet requirements).

upvoted 1 times

 **Zac15** 11 months ago

Selected Answer: AD

<https://docs.aws.amazon.com/whitepapers/latest/aws-direct-connect-for-amazon-connect/virtual-interfaces-vif.html>
upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

Selected Answer: AD

A, D for sure.

Must have access to AWS public services.

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: AD

A and D

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: AD

its AD

upvoted 1 times

 **SkyZeroZx** 2 years, 5 months 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** 2 years, 6 months ago

Selected Answer: AD

got to use Public VIN in order to connect to AWS Services via Direct Connect.

upvoted 2 times

 **easytoo** 2 years, 6 months ago

a-d-a-d-a-d-a-d

upvoted 1 times

 **Jesuisleon** 2 years, 6 months 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 5 times

 **rbm2023** 2 years, 7 months ago

Selected Answer: AD

agree with A and D tks to Roontha

upvoted 3 times

 **andreitugui** 2 years, 7 months 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

Correct Answer: ACD

Community vote distribution

ACD (76%)	5%	Other
-----------	----	-------

 **Roontha**  2 years, 7 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 18 times

 **ShinLi** 2 years, 7 months ago
why you pickup C? why we need enable all the features?
upvoted 2 times

 **Roontha** 2 years, 6 months 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 23 times

 **princajen**  4 months, 1 week ago

Selected Answer: ACD
For org-wide WAF baseline:
Enable AWS Config (prereq for compliance enforcement).
Enable all features in AWS Organizations (prereq for Firewall Manager).
Use AWS Firewall Manager to centrally deploy/manage AWS WAF rules (including OWASP Top 10).

Not GuardDuty, Shield, or Security Hub — they serve different purposes (threat detection, DDoS, posture management).
upvoted 3 times

 **sakibmas** 1 year, 3 months ago

Selected Answer: ACD
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.

A firewall administrator AWS Account: You must designate one of the AWS accounts in your organization as the administrator for AWS Firewall Manager.
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.
Reference: <https://aws.amazon.com/blogs/security/using-aws-firewall-manager-and-waf-to-protect-your-web-applications-with-master-rules-and-application-specific-rules/>

upvoted 2 times

 **Russ99** 1 year, 8 months ago

Selected Answer: ACD

ACD is the correct combination to establish a base line security when deploying within the organization in AWS Organization.

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: ACD

Answer - ACD

Prerequisites - AWS Config and All Features should be enabled in the organization.

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: ACD

A, C, D

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: ACD

AWS config must be enabled in all accounts to identify new resources so AWS Firewall manager works properly

upvoted 3 times

 **easytoo** 2 years, 5 months 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 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: ACD

its ACD

upvoted 1 times

 **javitech83** 2 years, 6 months 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** 2 years, 6 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>

upvoted 3 times

 **easytoo** 2 years, 6 months ago

baseline for OWASP = b-d-f

upvoted 1 times

 **emiliocb4** 2 years, 6 months 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 4 times

 **Jonalb** 2 years, 6 months 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** 2 years, 6 months 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 2 times

✉ **Jesuisleon** 2 years, 6 months 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 threat 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** 2 years, 6 months 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** 2 years, 4 months 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

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.

Correct Answer: BCE

Community vote distribution

BCE (73%)	13%	13%
-----------	-----	-----

 **Rajivjain** Highly Voted 2 years ago

Kindly correct the Answers' sequence. A to F
upvoted 24 times

 **Rajivjain** 2 years 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 2 years 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 22 times

 **princaben** Most Recent 4 months, 1 week ago

Selected Answer: BCE
B: IAM role trust must point to the SAML provider (principal + sts:AssumeRoleWithSAML).

C: The federation flow must call STS:AssumeRoleWithSAML with the correct ARNs and the SAML assertion.

E: The IdP SAML assertion must include the role mappings (role/provider pairs) so users are authorized for the right IAM roles.
upvoted 1 times

 **sarlos** 1 year, 1 month ago

B1,C,E
upvoted 6 times

 **37b2ab7** 1 year, 7 months ago

Selected Answer: BCE
For sure - BCE
upvoted 3 times

 **severlight** 1 year, 7 months ago

Selected Answer: BCE
B1, C, E
upvoted 3 times

 **dkcloudguru** 1 year, 9 months ago

BDF is correct
upvoted 1 times

CloudHandsOn 1 year, 9 months ago

Selected Answer: BCE

B,C, & E was my first choice

upvoted 2 times

Gmail78 1 year, 10 months ago

C- STS AssumerolewithSAML

B1- Define trust policy for IAM assumed by the principal

E - SAML Assertion

upvoted 3 times

SK_Tyagi 1 year, 10 months ago

Selected Answer: BD

BDF is correct

upvoted 1 times

anttan 1 year, 10 months 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 2 times

breadops 1 year, 11 months ago

Selected Answer: B

BDF is the right answers

upvoted 2 times

ggrodskiy 1 year, 11 months ago

Correct BCE.

upvoted 1 times

Just_Ninja 1 year, 11 months ago

Selected Answer: BD

Admin The Order from the Question is not right.. Answer is BDF!

upvoted 1 times

NikkyDicky 1 year, 11 months ago

Selected Answer: BCE

B (the 1st B, as there are two in this version of question) CE

upvoted 2 times

easytoo 2 years ago

it's B-D-F Jeff.

upvoted 2 times

Roontha 2 years, 1 month ago

Answer : B, C, E

upvoted 2 times

Roontha 2 years, 1 month ago

Sorry...it is BDF

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

upvoted 4 times

Question #201

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.

Correct Answer: A*Community vote distribution*

A (100%)

 **Masonryeh**  2 years, 7 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 7 times

 **princajen**  4 months, 1 week ago

Selected Answer: A

RDS Proxy = solves overloaded connections via pooling/multiplexing for Aurora.

Secrets Manager = secure storage + automatic rotation of DB creds.

Replicas don't help write-heavy loads; Parameter Store lacks built-in rotation.

→ Therefore, A best satisfies performance + security requirements.

upvoted 1 times

 **85b5b55** 10 months, 1 week ago

Selected Answer: A

To handle the overloaded connections and keep the secrets in the Amazon Secret Manager.

upvoted 1 times

 **carpa_jo** 1 year, 12 months ago

Selected Answer: A

Use replicas to scale read, this use-case is about writing so C & D are out.

Secret manager offers rotation, parameter store doesn't.

So its A.

upvoted 2 times

 **duriselvan** 2 years ago

D. Aurora Replica with Parameter Store:

Pros:

Improves database capacity and reduces load on the primary instance.

Parameter Store provides centralized configuration management.

Cons:

Manually rotating credentials in Parameter Store poses security risks.

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just A

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

Option A

upvoted 2 times

  **joleneinthebackyard** 2 years, 1 month ago**Selected Answer: A**

straight A. love these questions 😊

upvoted 1 times

  **NikkyDicky** 2 years, 5 months ago**Selected Answer: A**

easy A

upvoted 1 times

  **pupsik** 2 years, 6 months ago**Selected Answer: A**

Agree with other explanations here.

upvoted 1 times

  **rbm2023** 2 years, 7 months 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

  **Roontha** 2 years, 7 months ago

Answer : A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 4 times

Question #202

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.

Correct Answer: B

Community vote distribution

B (90%)	5%
---------	----

 **bjexamprep** Highly Voted 2 years ago

Selected Answer: B

Bad question design. EC2 is in ASG, which means the application part is stateless, so no need to backup or replicate. Only database need replication.

upvoted 7 times

 **Snape** Highly Voted 2 years, 7 months 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 5 times

 **princaben** Most Recent 4 months, 1 week ago

Selected Answer: B

RPO 30s ⇒ Replication, not backups: Use RDS cross-Region read replica (cost-effective vs Aurora Global).

RTO 10 min ⇒ Pilot-light/warm standby: Use AWS Elastic Disaster Recovery for EC2; launch & scale at failover time, not 24/7.

Failover DNS: Route 53 failover routing (not geolocation/simple).
→ Therefore, B meets RPO/RTO at the lowest cost.
upvoted 1 times

 **FZA24** 1 year, 1 month ago

Selected Answer: B

RPO seconds, RTO minutes => warm standby
warm standby => always running but smaller
always running but smaller => B. Run the EC2 instances at the minimum capacity in the DR Region
upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B most cost effective for RTO=10 min and RPO=30 min.
upvoted 3 times

 **career360guru** 2 years, 1 month ago
RPO=30 sec
upvoted 2 times

 **Pupu86** 2 years, 1 month ago

Selected Answer: B
RPO of 30 seconds can be achieved with Elastic disaster recovery for continuous EC2 instance replication, while DB read replica can be promoted to primary within 30 seconds
upvoted 3 times

 **SK_Tyagi** 2 years, 4 months ago

Selected Answer: B
Close between B & D but Max out ASG is tie-breaker
upvoted 3 times

 **softarts** 2 years, 4 months ago

Selected Answer: D
I think (D) only aurora global database can meet RPO 30 seconds? although B is cost-effective
upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B
B for sure
upvoted 1 times

 **SkyZeroZx** 2 years, 6 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 3 times

 **Jackhemo** 2 years, 6 months ago

olabiba.ai said B.
upvoted 1 times

 **Jonalb** 2 years, 6 months 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 5 times

 **Moallal** 2 years, 6 months ago

Selected Answer: A
Do the math, option A is 5.55 days.
upvoted 1 times

 **rbm2023** 2 years, 7 months 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** 2 years, 7 months 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 fot the RPO of 30 seconds.

upvoted 1 times

 **dbaroger** 2 years, 7 months ago

Selected Answer: B

Cost efective = B

upvoted 2 times

 **AMEJack** 2 years, 7 months ago

Selected Answer: B

Agree with B

upvoted 1 times

Question #203

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.

Correct Answer: C

Community vote distribution

C (97%)

 **F_Eldin** Highly Voted 2 years 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 27 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: C

Goal: least time with limited internet → avoid the internet using Snowball Edge (offline bulk transfer).

Destination is Aurora MySQL → use AWS DMS to load from S3 into Aurora.

DataSync can't outpace a slow link; MGN isn't for database-to-Aurora migrations; DX adds procurement time.
→ Therefore, C is the fastest, exam-correct choice.

upvoted 1 times

 **TonytheTiger** 1 year, 2 months ago

Selected Answer: C

Option C : How To

<https://aws.amazon.com/blogs/storage/enable-large-scale-database-migrations-with-aws-dms-and-aws-snowball/>
upvoted 2 times

 **Maygam** 1 year, 5 months ago

Selected Answer: C

AWS Snowball and Snowball Edge refers the same thing. From the Snowball FAQ "AWS Snowball is a service that provides secure, rugged devices, so you can bring AWS computing and storage capabilities to your edge environments, and transfer data into and out of AWS. Those rugged devices are commonly referred to as AWS Snowball or AWS Snowball Edge devices.". Between C and D, it's C using Snowball edge with AWS DMS.

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: C

Option C - Direct connection would take 1 month
upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

Basic Snowball edge / DMS use case
upvoted 1 times

 **Moallal** 2 years ago

Do the math, option A is 5.55 days. It's A
upvoted 2 times

 **covabix879** 1 year, 8 months ago

Keyword is one-time migration. In addition to time it takes to deliver, it will be huge waste for one-time task.
upvoted 2 times

 **Jackhemo** 2 years ago

it takes ages to order a 1G circuit.
upvoted 2 times

 **breadops** 1 year, 11 months ago

It can take months to provision a DX connection, its not A.
upvoted 2 times

 **andreitugui** 2 years 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 4 times

 **rbm2023** 2 years 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

 **dbaroger** 2 years ago

Selected Answer: D

D better cost than C and it does the same for S3. Need adapter too
upvoted 1 times

 **Roontha** 2 years, 1 month 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

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.

Correct Answer: C

Community vote distribution

C (86%)

12%

 **andreitugui**  2 years, 7 months 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 22 times

 **Roontha** 2 years, 6 months 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 years, 5 months 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

 **helloworldabc** 1 year, 4 months ago

just C

upvoted 1 times

 **princaben**  4 months, 1 week ago

Selected Answer: C

Meets RPO 1 day: Daily AWS Backup + cross-Region copy to a DR vault.

Meets RTO 1 business day: Guided EC2 instance & multi-volume restore workflow.

Least ops & cost: Centralized policies, lifecycle/retention, no extra runbooks or standing compute.

Why not A/B/D: A = more DIY ops; B = DLM can't restore instances; D = wrong tool (DataSync) + higher cost
upvoted 1 times

Soliner_Bilgi_Teknolojileri 4 months, 2 weeks ago

Selected Answer: C

AWS Backup can back up EC2 instances and all attached EBS volumes in a single plan, including full configuration, and automatically copy these backups to a target Region with its cross-Region backup copy feature. This provides operational simplicity by managing all backup and copy processes without the need for additional scripts or automation runbooks. In the event of a failure, the network can be set up in the target Region using CloudFormation, and both volumes and instance configurations can be restored from the AWS Backup vault to quickly bring the system online.

upvoted 1 times

sergza888 10 months, 1 week ago

Selected Answer: A

With these RTO/RPO WE don't need to backup entire EC2 especially for cost efficiency. We Only need to maintain CF In another region as well as EBS Backups. System Manager allows you to script and execute backup and copy it to another region instead of DL
upvoted 1 times

chris_spencer 1 year, 2 months ago

Selected Answer: C

C because of this one. "The company has limited staff and needs a backup solution that optimizes operational efficiency and cost." AWS Backup really optimizes your backup solution. We backup everthing now with AWS Backup. B works too but it more complicated. The restore from AWS Backup is nearly a no brainer

upvoted 1 times

gfhbox0083 1 year, 5 months ago

Selected Answer: C

C, for sure.
Use AWS Backup.
DLM itself does not directly support restore operations.
upvoted 2 times

saggy4 1 year, 10 months ago

Correct Answer is C.

Why not B, DLM can only take backup on restore. The options says using DLM restore the volumes.

upvoted 1 times

saggy4 1 year, 10 months ago

I meant DLM cannot restore so the option B is wrong.

upvoted 1 times

career360guru 2 years, 1 month ago

Selected Answer: C

Option C
upvoted 2 times

severlight 2 years, 1 month ago

Selected Answer: C

Because AWS Back ups supports restore and DLM doesn't
upvoted 1 times

SK_Tyagi 2 years, 4 months 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 years, 5 months ago

Selected Answer: C

C
B would be ok, if DLM supported restore. it doesn't
upvoted 2 times

javitech83 2 years, 6 months ago

Selected Answer: C

I think correct is C. AWS Backup is easier and perfectly fits the scenario
upvoted 1 times

Maria2023 2 years, 6 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 2 times

 **easytoo** 2 years, 6 months ago

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

upvoted 1 times

 **Jonalb** 2 years, 6 months ago

Selected Answer: B

Its B!!!!!!!!!!!!!!

upvoted 1 times

 **clownfishman** 2 years, 6 months ago

Why not A?

upvoted 3 times

 **Jesuisleon** 2 years, 6 months 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

Question #205

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.

Correct Answer: ACE*Community vote distribution*

ACE (95%)	3%
-----------	----

 **SkyZeroZx** Highly Voted 2 years, 5 months 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 19 times

 **Just_Ninja** Highly Voted 2 years, 5 months ago

Selected Answer: ACE

ACE.
 But A is deprecated :)
 because since the 05.01.2023 S3 use automatical atRest encryption for new objects.
 upvoted 6 times

 **dankositze** 1 year, 10 months ago

Right I would go with CEF for 2024 onwards
 upvoted 2 times

 **Chris_W_1234** 2 months, 1 week ago

There is no "RequireSSL" in S3 (to my knowledge). TLS connections are enforced via a bucket policy with "aws:SecureTransport". I say BCE.
 upvoted 1 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: ACE

At rest: Enable S3 server-side encryption (A).

In transit: Force HTTPS for users ↔ CloudFront (E) and CloudFront ↔ S3 via bucket policy aws:SecureTransport (C).

Ignore ACLs, CloudFront SSE-KMS, and "RequireSSL" (they don't apply).

upvoted 1 times

 **khchan123** 1 year, 9 months ago

Selected Answer: BCE

BCE
 You need B to enforce encryption in transit with S3. Other options cannot do that.
 upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just ACE

upvoted 1 times

✉️  **Dgix** 1 year, 9 months ago

This question was obviously formulated before S3 buckets were encrypted by default.

upvoted 1 times

✉️  **duriselvan** 2 years ago

- A. Turn on S3 server-side encryption for 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.

Here's why these steps are necessary:

- A. S3 server-side encryption: This encrypts data in the S3 bucket at rest, ensuring data confidentiality even if someone gains unauthorized access to the bucket.
- D. CloudFront SSE-KMS: This encrypts data in transit between CloudFront and the client, ensuring data confidentiality when users upload and download files.
- E. HTTP to HTTPS redirect: This ensures all communication between the client and CloudFront occurs over HTTPS, encrypting data in transit and preventing eavesdropping.

upvoted 2 times

✉️  **career360guru** 2 years, 1 month ago

Selected Answer: ACE

Options A, C , E

upvoted 1 times

✉️  **task_7** 2 years, 3 months ago

Selected Answer: ADE

- A. Turn on S3 server-side encryption for 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.

Data at rest encrypted for Both S3 and Cloudfront

E for data in transit

upvoted 1 times

✉️  **Simon523** 2 years, 4 months 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 2 times

✉️  **RotterDam** 2 years, 4 months ago

ACE but why not F?

upvoted 1 times

✉️  **chikorita** 2 years, 3 months 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 3 times

✉️  **kgpoj** 1 year, 4 months ago

When you have pre-signed urls, you don't even necessarily need cloudFront

upvoted 1 times

✉️  **Christina666** 2 years, 5 months ago

Selected Answer: ACE

we don't have a "encryption at rest" for cloudfont in the console

upvoted 1 times

✉️  **NikkyDicky** 2 years, 5 months 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** 2 years, 6 months ago

a-d-e a-d-e a-d-e

upvoted 2 times

✉️  **chathur** 2 years, 6 months 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** 2 years, 7 months ago

Why not B?

upvoted 2 times

✉  **BabaP** 2 years, 6 months ago

Because C does just that

upvoted 1 times

✉  **chathur** 2 years, 6 months ago

<https://repost.aws/knowledge-center/s3-bucket-policy-for-config-rule>

it is not enough

upvoted 1 times

✉  **Jesuisleon** 2 years, 6 months 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 6 times

✉  **andreitugui** 2 years, 7 months ago

Selected Answer: ACE

I will go with ACE

upvoted 2 times

✉  **Roontha** 2 years, 7 months ago

Answer : ACE

upvoted 4 times

Question #206

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.

Correct Answer: D*Community vote distribution*

D (81%)

A (19%)

 **Snape** Highly Voted 2 years, 7 months ago

Selected Answer: D

Answer : D
Rotation = Secret Manager (and Not Parameter store)

upvoted 14 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: D

Secrets Manager is the right place for DB creds; integrates cleanly with Lambda.

KMS customer managed key → IT security controls access and key rotation.

IAM: Lambda execution role gets read/decrypt; humans restricted to IT security.

→ Therefore, D best matches security, key rotation, and operational best practice.

upvoted 1 times

 **_Jassybanga_** 1 year, 4 months ago

Answer should be A , As we are talking of encryption Key rotation by customer IT key responsible person and not the database credential rotation

upvoted 2 times

 **AA001** 1 year, 4 months ago

Selected Answer: D

To use parameters from Parameter Store in AWS Lambda functions without using an SDK, you can use the AWS Parameters and Secrets Lambda Extension.

To use parameters in a Lambda function without the Lambda extension, you must configure your Lambda function to receive configuration updates by integrating with the GetParameter API action for Parameter Store.

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: D

Option D

upvoted 1 times

✉  **NikkyDicky** 2 years, 5 months ago

Selected Answer: D

its a D

upvoted 1 times

✉  **javitech83** 2 years, 6 months ago

Selected Answer: D

Keys is DB credentials rotation

upvoted 2 times

✉  **easystoo** 2 years, 6 months ago

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

upvoted 1 times

✉  **Jackhemo** 2 years, 6 months 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 years, 5 months 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** 2 years, 6 months ago

Answer is D. This is for the next question.

upvoted 2 times

✉  **rbm2023** 2 years, 7 months 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 4 times

✉  **F_Eldin** 2 years, 7 months ago

A does not satisfy the requirement "This key must be rotated on a regular basis."

upvoted 3 times

✉  **kejam** 1 year, 11 months ago

Agreed. Requirement is to rotate the Key. KMS CMKs can be rotated:

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

upvoted 1 times

✉  **andreitugui** 2 years, 7 months ago

Selected Answer: D

Answering D

upvoted 1 times

✉  **Masonryeho** 2 years, 7 months ago

Selected Answer: D

D, Secret Manager is the accurate solution

upvoted 1 times

✉  **Roontha** 2 years, 7 months ago

Answer : D

Keys is DB credentials rotation

upvoted 1 times

Question #207

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.

Correct Answer: A*Community vote distribution*

A (84%)

C (16%)

 **bjexamprep**  2 years ago

Selected Answer: A

"does not want to rewrite the application." leaves the possible answer between A and C, cause B and D will force the application team to rewrite the data access part of the application.

C is using EKS, which makes AutoScalingGroup is not required. ASG scales instances. ASG doesn't scale PODs in EKS. Babelfish is the key point in this question. "Babelfish for Aurora PostgreSQL is a new capability for Amazon Aurora PostgreSQL-Compatible Edition that enables Aurora to understand commands from applications written for Microsoft SQL Server."

upvoted 13 times

 **F_Eldin**  2 years, 7 months 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 7 times

 **princajen**  4 months, 1 week ago

Selected Answer: A

Scaling: EC2 Auto Scaling + ALB handles spikes without code changes.

Cost: Aurora PostgreSQL with Babelfish removes SQL Server licensing while keeping app changes minimal.

Managed: Aurora + ALB are managed; no heavy ops.

→ Therefore, A best meets "solve scaling + minimize licensing, no rewrite."

upvoted 1 times

 **85b5b55** 7 months, 3 weeks ago

Selected Answer: C

C - Fully managed Service, cost-effective and doesn't want to rewrite, those points pushed me to select C only.

upvoted 1 times

 **SIJUTHOMASP** 1 year ago

Selected Answer: A

The key is 'minimise licensing cost' so, option A is the best because it can radically cut down the SQL Server licensing cost by putting it to Aurora PostgreSQL. Option C has equivalent licensing cost since it is SQL RDS.

upvoted 2 times

 **0b43291** 1 year, 1 month ago

Selected Answer: C

Option C is the most cost-effective solution as it leverages containerization with Amazon EKS, Auto Scaling groups with Network Load Balancers, and Amazon RDS for SQL Server. This approach allows for efficient scaling, resource utilization, and minimizes licensing costs without requiring significant application changes.

Containerizing the web and application tiers enables portability and scalability. Amazon EKS provides a fully managed Kubernetes service, reducing operational overhead. Auto Scaling groups and Network Load Balancers enable automatic scaling based on demand. Amazon RDS for SQL Server offers a fully managed database service with various licensing models, including BYOL, to optimize costs as the application scales.

The other options have drawbacks, such as requiring replatforming the database (Option A), significant application changes (Option B), or a complete rewrite (Option D), which goes against the requirements.

upvoted 1 times

 **8693a49** 1 year, 4 months ago

Selected Answer: C

All answers are wrong. A is not using managed services where possible (EKS would be better than EC2 and can run windows) and on C you can't have Auto Scaling group for EKS. Realistically C is the better option if scaled with Karpenter, etc.

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just A

upvoted 1 times

 **BrijMohan08** 1 year, 7 months ago

Selected Answer: C

Key here is AWS Managed = EKS

A. Says both Web tier and Application tier is behind ALB, which is not secure.

A good design should have web tier behind ALB, and application tier behind NLB

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: A

Option A: Babelfish for Aurora PostgreSQL is a capability for Amazon Aurora PostgreSQL-Compatible Edition developed using the PostgreSQL extension framework that enables Aurora to understand commands from applications written for Microsoft SQL Server. Babelfish for Aurora PostgreSQL understands T-SQL, Microsoft SQL Server's SQL dialect, and supports

<https://aws.amazon.com/blogs/database/run-sql-server-reporting-services-reports-against-babelfish-for-aurora-postgresql/>

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

Option A

upvoted 1 times

 **Pupu86** 2 years, 1 month ago

Selected Answer: C

As much as I would like to choose A but the question request for lift and shift approach rather than a replatform

upvoted 2 times

 **enk** 2 years, 1 month ago

Selected Answer: C

I vote C. Babelfish - another layer to keep an eye on. Is it really going to translate all SQL app calls perfectly, or will they need tuning?

upvoted 1 times

 **kjcncjek** 2 years, 3 months ago

why not C

upvoted 1 times

 **Mikado211** 2 years, 1 month ago

C would be probably the most realistic way a team work to engage such case regarding to the choices we have. However Babelfish is a tool made to execute Microsoft SQL on a PostgreSQL server. In practice Babelfish is a toy and should not be used for a real strong usage since the database engine is the last thing you want to play with. Still, people who answered A have followed the theory, and it's probably the expected answer here.

upvoted 4 times

 **chikorita** 2 years, 4 months ago

A : the best of the worst

upvoted 4 times

 **ggrodsckiy** 2 years, 5 months ago

Correct A.

upvoted 1 times

✉️  **YodaMaster** 2 years, 5 months ago

Selected Answer: A

A. The other options sound fishy.

upvoted 5 times

✉️  **rxhan** 2 years, 4 months ago

golden.

upvoted 1 times

✉️  **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

A by elimination

upvoted 2 times

Question #208

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.

Correct Answer: C

Community vote distribution

C (72%)	B (22%)	4%
---------	---------	----

 **andreitugui**  2 years, 7 months 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 11 times

 **nexus2020** 2 years, 6 months 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.

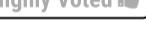
upvoted 2 times

 **sam2ng** 1 year, 4 months ago

as the ALB and EKS are running in one region only which is us-east-1, how does the global accelerator help when traffic comes from other region e.g. EU ?

Also you don't configure origin in global accelerator, you configure endpoint group.

upvoted 1 times

 **ayadmawla**  2 years ago

Selected Answer: C

imho answer is C. Here is my thinking: There are two issues that we need to consider:

1- Non US Users are reporting long and inconsistent response times for these APIs

2- The APIs are running in EKS and are exposed by the ALB (i.e., not the other way round)

So the issue is about latency not API design.

upvoted 5 times

 **aka1177**  3 weeks ago

Selected Answer: C

In reality, you should deploy additional API Gateways and ALBs, along with EKS clusters in the appropriate Regions. Given the limited answer choices here, I would pick option C

upvoted 1 times

 **Malluchan** 3 months, 1 week ago

Selected Answer: C

This APIs use non-standard HTTP methods (LINK, UNLINK, LOCK, UNLOCK). CloudFront only forwards a fixed set of HTTP methods (GET, HEAD, OPTIONS, PUT, PATCH, POST, DELETE), and in practice non-standard methods can be blocked or return 403 when you put CloudFront in front of an ALB. Global Accelerator works at the network layer (TCP/UDP). It doesn't inspect or normalize HTTP methods, so it will forward your custom LINK/UNLINK/LOCK/UNLOCK traffic unchanged to the ALB. That avoids the CloudFront method limitation.

upvoted 1 times

 **fa6d93f** 3 months, 1 week ago

Selected Answer: C

Global Accelerator provides static Anycast IPs that route requests over the AWS global network backbone.

Improves latency and consistency for global users without needing multi-Region deployment.

Supports all TCP/UDP traffic, so non-standard REST methods are not a problem.

upvoted 2 times

 **princajen** 4 months, 1 week ago

Selected Answer: C

Need global performance without changing methods → Global Accelerator accelerates traffic while preserving all verbs.

CloudFront/API Gateway: method limitations / extra mapping; not suitable for LINK/UNLOCK/....

Multi-region: fixes latency but too much ops.

→ C gives the best latency/consistency with minimal operational overhead.

upvoted 1 times

 **fabriciolff** 1 year, 2 months ago

Selected Answer: C

C

upvoted 1 times

 **HelpnoseNse** 1 year, 6 months ago

Selected Answer: C

Not B. Because Gateway Edge-Optimized API Endpoint improve the performance by caching API responses. But (un)link the call is not supported by API Gateway so the rest will be passed to ALB anyway. So unlikely API gateway will cache and no benefit for performance improvement.

upvoted 2 times

 **titi_r** 1 year, 7 months ago

Selected Answer: C

Answer: C

AWS Global Accelerator is a service in which you create accelerators to improve the performance of your applications for local and global users.

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

When you create an ALB or NLB, you can optionally add an accelerator at the same time. Elastic Load Balancing and Global Accelerator work together to transparently add the accelerator for you. The accelerator is created in your account, with the load balancer as an endpoint. Using an accelerator provides static IP addresses and improves the availability and performance of your applications.

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.alb-accelerator.html>

upvoted 1 times

 **titi_r** 1 year, 7 months ago

Ans "B" is wrong, because API Gateway does NOT support non-standard REST methods. The supported methods are DELETE, GET, HEAD, OPTIONS, PATCH, POST, PUT, and ANY (which can substitute any of the other 7).

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-method-settings-method-request.html#setup-method-add-http-method> .

upvoted 4 times

 **dankositze** 1 year, 10 months ago

Selected Answer: D

A: No

B: No, API Gateway doesn't support LINK, UNLINK, LOCK, UNLOCK.

C: No, GA doesn't have the concept of "origin" - this is a CloudFront concept.

D: Yes, because this addresses the main concern which is latency.

upvoted 3 times

 **duriselvan** 2 years ago

b IS ANS

Minimal operational overhead: API Gateway edge-optimized endpoints offer several advantages:

Reduced latency: They leverage AWS's global network of edge locations, significantly reducing latency for users outside the United States.

Scalability: They automatically scale to handle traffic spikes, eliminating the need for manual intervention.

Security: They offer built-in security features, including access control and throttling, minimizing the need for additional configuration.

Non-standard methods compatibility: API Gateway supports a wide range of HTTP methods, including custom methods like LINK, UNLINK, LOCK, and UNLOCK, ensuring compatibility with the existing APIs.

Ease of configuration: Configuring API Gateway with ALB as the target is straightforward and requires minimal changes to the existing infrastructure.

upvoted 1 times

 **awsamar** 2 years ago

Selected Answer: B

Amazon CloudFront primarily supports standard HTTP/HTTPS request methods like GET, POST, PUT, DELETE, HEAD, OPTIONS, and PATCH. It does not natively support non-standard methods such as LINK and UNLINK, LOCK...etc
 HOWEVER>>>>
 If you need to use these non-standard methods, you have a couple of options:
 Custom Handling with Lambda@Edge
 API Gateway Integration: If you require more complex routing and method handling, integrating AWS API Gateway with CloudFront might be a more suitable solution. API Gateway provides robust support for various HTTP methods and can be set up to handle non-standard methods.

Clearly its B

upvoted 3 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C, GA is safest option.

upvoted 1 times

 **severlight** 2 years, 1 month ago

Selected Answer: C

there is no proper use case for API gateway here

upvoted 2 times

 **joleneinthebackyard** 2 years, 1 month ago

Selected Answer: C

A is invalid because cloudFront only support standard Rest Methods

B C D all technically feasible but let's consider "minimized operational overhead" requirement, it's must be C.

upvoted 2 times

 **chico2023** 2 years, 4 months 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 3 times

 **chico2023** 2 years, 4 months 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** 2 years, 4 months 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

 **vn_thanhung** 2 years, 4 months 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

 **Arnaud92** 2 years, 4 months 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 4 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.

Correct Answer: B*Community vote distribution*

B (100%)

 **easystoo** Highly Voted 2 years, 6 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 5 times

 **princajen** Most Recent 4 months, 1 week ago

Selected Answer: B
Reliability & scale: AWS IoT Core is a managed MQTT broker built for millions of devices; no server bottleneck.

Minimal changes: Use custom domain to keep `iot.example.com`, point to Data-ATS; define an IoT Rule to DynamoDB.

Why not A/C/D:

A: ALB isn't for raw MQTT; complex, stateful scaling problem.

C: Still a single EC2 broker → still fails under load.

D: Greengrass ≠ cloud MQTT ingress service.

upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 4 months, 2 weeks ago

Selected Answer: B
IoT Greengrass is designed for edge (on-premises/field) scenarios; it is not a replacement for a centralized, cloud-hosted MQTT broker.
upvoted 1 times

 **junta** 1 year, 9 months ago

Selected Answer: B
option B
upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B
Option B
upvoted 1 times

✉ **bur4an** 2 years, 3 months ago

I think this is repeat question.
upvoted 1 times

✉ **SK_Tyagi** 2 years, 4 months ago

Selected Answer: B

AWS service is the answer.
upvoted 3 times

✉ **lferrari** 2 years, 4 months ago

Selected Answer: B

IOT core for anything IOT
upvoted 2 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

IOT core for anything IOT
upvoted 4 times

✉ **pupsik** 2 years, 6 months ago

Selected Answer: B

Option C doesn't mention required auto-scaling group, hence eliminated.
upvoted 1 times

✉ **SkyZeroZx** 2 years, 6 months ago

Selected Answer: B

voting for B. IoT Core
upvoted 3 times

✉ **Maria2023** 2 years, 6 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 2 times

✉ **Daniel76** 1 year, 1 month ago

IoT core support availability whereas option c did not mention about auto scaling. With just one instance it might still fail to process when there's a surge in incoming data.

upvoted 1 times

✉ **chiaseed** 2 years, 6 months ago

Selected Answer: B

voting for B. IoT Core
upvoted 2 times

✉ **nexus2020** 2 years, 6 months ago

Selected Answer: B

IoT core, B
upvoted 1 times

Question #210

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.

Correct Answer: A*Community vote distribution*

A (81%)

D (19%)

 **EzKkk** 2 weeks, 3 days ago

I find this is a badly formatted question which doesn't have a good answer.

- A - Solution can't react to "upon request" event => wrong
- B - Storing keys in Parameter Store is not secure => wrong
- C - Solution can't rotate SSH keys => wrong
- D - Solution doesn't offer centrally managed key store => wrong

upvoted 1 times

 **princajen** 4 months, 1 week ago

Selected Answer: A

Secrets Manager gives encrypted storage + rotation hooks; Lambda generates per-instance keypairs and updates authorized_keys via SSM
→ <1 min downtime.

B/C/D miss either secure storage, correct rotation capability, or use the wrong service for SSH key management

upvoted 1 times

 **xerxersxu** 8 months, 2 weeks ago

Selected Answer: A

<https://aws.amazon.com/cn/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 1 times

 **pk0619** 1 year ago

Selected Answer: D

SSM RunCommand is the only solution that can actually replace the keys on EC2 instances.

upvoted 1 times

 **dankositze** 1 year, 4 months ago

Selected Answer: A

Not sure why you would need to "invoke an AWS Lambda function to generate new key pairs" when Secrets Manager natively supports automatic key rotation? Anyways, A seems to be the least worst answer.

upvoted 3 times

 **sat2008** 1 year, 4 months ago

Lambda is part of the key creation and rotation see the link

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 5 times

 **Maygam** 1 year, 6 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 3 times

✉ pk0619 1 year ago

this is a 5 years old solution, currently the answer should be either B or best D, also Lambda cannot replace the public keys on EC2 instances, you need SSM RunCommand for that.

upvoted 1 times

✉ CProgrammer 1 year, 6 months ago

@duriselvan ==> How did you arrive at "Automatic key rotation" from "key rotation policy that will, upon request

B. Parameter Store: While Parameter Store can store keys, it's not designed for automated key rotation. It would require manual configuration and orchestration.

C. AWS KMS: KMS is designed for managing encryption keys, not SSH key pairs.

It doesn't support the rotation of SSH key pairs on EC2 instances.

D. Fleet Manager: Fleet Manager, while facilitating management tasks on EC2 instances, doesn't intrinsically handle key rotation.

It would require integration with other services and custom scripts.

upvoted 2 times

✉ duriselvan 1 year, 6 months ago

C ans

Automatic key rotation: AWS KMS automatically rotates keys according to the configured schedule, eliminating the need for manual intervention and ensuring timely key updates.

Less than 1 minute downtime: AWS KMS allows for seamless key rotation with minimal downtime. The old key remains active until the new key is generated and propagated, ensuring uninterrupted access to instances.

Secure storage: AWS KMS provides a highly secure and encrypted environment for storing cryptographic keys, exceeding the security offered by Parameter Store.

Lambda function integration: The EventBridge rule can trigger a Lambda function to perform additional tasks during key rotation, such as updating user access controls or notifying administrators.

upvoted 3 times

✉ Jay_2pt0_1 1 year, 7 months ago

Torn between A and D. I don't like the do-it-yourself nature (Lambda) of A, but I understand what everyone is saying about the unique key requirement, which would seem to imply that D is wrong. Don't know tbh.

upvoted 1 times

✉ career360guru 1 year, 7 months ago

Selected Answer: A

Option A

upvoted 1 times

✉ severlight 1 year, 7 months ago

Selected Answer: A

A will work, don't overthink, you can request secret rotation in the Secrets manager, and secrets will be stored in a safe place

upvoted 2 times

✉ Sab 1 year, 8 months ago

Selected Answer: A

D is best option if we need to rotate for all Ec2 with same key pair. Since each EC2 to have a different Key pair, will be better to store in Secrets Manager and have that rotated using lambda.

upvoted 1 times

✉ wahaha2023 1 year, 10 months 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 3 times

✉ chico2023 1 year, 10 months 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

✉ chico2023 1 year, 10 months 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 year, 10 months ago

I am curious about how we can define a 1-minute Systems Manager maintenance window.

upvoted 2 times

 **vn_thanh tung** 1 year, 10 months ago

With D how to "keep the keys in a securely encrypted place" ? Should be A

upvoted 1 times

 **easystoo** 1 year, 11 months ago

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

upvoted 1 times

 **Just_Ninja** 1 year, 11 months 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** 1 year, 11 months ago

Selected Answer: D

Why A? Select D

upvoted 2 times

 **Just_Ninja** 1 year, 11 months 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 für Secrets and here we have for exmaple the secret manager with FIPS 140-2 Standard.

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.

Correct Answer: C

Community vote distribution

C (100%)

 **princajen** 4 months ago

Selected Answer: C

The best solution is C (Migration Evaluator agentless collector) because it provides automated inventory and utilization data directly from ESXi without installing agents on every VM. Options A and D require per-VM agents, which adds major overhead, and B is too manual. Since the question emphasizes "least operational overhead," the agentless collector is the right fit.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: C

C vs D

Migration Evaluator is suited for initial inventory collection, and it is Agentless so low overhead

In D, the Application Migration Service needs to install agent on thousands of VMs, so it is not suitable for initial inventory collection and is high Operational overhead

upvoted 1 times

 **igor12ghsj577** 1 year, 10 months ago

why to remove highly utilized servers from the list, these answers can be rejected immediately.

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C

upvoted 1 times

 **callmechoice** 2 years, 2 months ago

migration evaluator. I think C is correct

upvoted 4 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C no doubt

upvoted 1 times

 **SkyZeroZx** 2 years, 5 months 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 years, 6 months ago

Selected Answer: C

I was first thinking about D because it is stated that the company has little knowledge about VMWare. But option D introduces operational overhead

upvoted 1 times

✉  **pupsik** 2 years, 6 months ago

Selected Answer: C

C seems like a good choice:

<https://aws.amazon.com/migration-evaluator/features/>

upvoted 2 times

✉  **easytoo** 2 years, 6 months ago

C-C-C-C-C-

migration evaluator ftw

upvoted 1 times

✉  **easytoo** 2 years, 6 months ago

Question 210 is a-a-a-a-a-a-a-a

upvoted 1 times

✉  **yzrk** 2 years, 6 months 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

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.

Correct Answer: A

Community vote distribution

A (95%)	5%
---------	----

 **Just_Ninja**  2 years, 5 months 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 12 times

 **joleneinthebackyard**  2 years, 1 month ago

Selected Answer: A

"The company wants to protect the database from crashes" means keep the existing one and do something that can prevent crashes, not to migrate it to another in anywhere. -> B, C out

Choice between SQS and SNS is easy.

upvoted 6 times

 **princajen**  4 months ago

Selected Answer: A

SQS buffers bursty writes and a reserved concurrency cap on the SQS-triggered Lambda guarantees you never exceed the on-prem DB's connection limit. C (RDS Proxy) doesn't apply to on-prem databases, B is an unnecessary migration, and D mixes SNS with provisioned (not limited) concurrency, which doesn't protect the DB from spikes.

upvoted 1 times

 **eesa** 8 months, 1 week ago

Selected Answer: A

Amazon SQS decouples ingestion from processing, allowing for asynchronous data handling.

By placing data into an SQS queue, you can buffer incoming requests regardless of spikes in Lambda invocation.

You then create a separate Lambda consumer that reads messages from the queue and writes them to the database at a controlled rate.

Using reserved concurrency, you can limit the number of simultaneous Lambda executions to a number lower than the database's connection limit—protecting the database.

upvoted 1 times

 **bi11** 1 year, 6 months ago

Selected Answer: C

C,

Keyword: "supports a limited number of concurrent connections"

Creating an Amazon RDS Proxy DB instance and attaching it to the Amazon RDS DB instance can help manage the database connections efficiently and prevent the database from being overwhelmed by too many connections. The RDS Proxy can pool and share connections to the database, which can reduce the number of connections that each Lambda function invocation needs to establish. This can help to prevent the database from crashing when the number of Lambda function invocations is high.

Reconfiguring the Lambda function to write to the RDS Proxy DB instance instead of directly to the database can further help to protect the database from crashes. This is because the RDS Proxy can handle the connections to the database, reducing the load on the database and helping to ensure its stability.

upvoted 1 times

 **altonh** 11 months, 1 week ago

You need to first migrate your DB to Amazon RDS, which was never mentioned as one of the steps.

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just A

upvoted 1 times

 **pk0619** 1 year, 8 months ago

Selected Answer: A

You can use SQS to write data, however the phrase "reserved concurrency" is incorrect, Lambda has "provisioned concurrency"

upvoted 1 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: A

Option A: AWS Tutorial on How To

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-lambda-tutorial.html>

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

Option A

upvoted 2 times

 **ggrodsckiy** 2 years, 5 months ago

Correct A.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

Its an A

upvoted 1 times

 **javitech83** 2 years, 6 months ago

Selected Answer: A

correct is A as database is on-premises

upvoted 2 times

 **bhanus** 2 years, 6 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** 2 years, 6 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** 2 years, 6 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** 2 years, 6 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** 2 years, 6 months ago

Selected Answer: A

Correct answer is A

upvoted 1 times

👤 **easystoo** 2 years, 6 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** 2 years, 4 months ago

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

upvoted 3 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.

Correct Answer: B*Community vote distribution*

B (89%)

11%

 **easytoo**  2 years, 6 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 6 times

 **princajen**  4 months ago

Selected Answer: B

(Amazon Managed Grafana) because it's a managed service that preserves existing dashboards, handles HA automatically, and requires almost no maintenance. Option A requires recreating dashboards, C still leaves you managing EC2/patching, and D doesn't meet the <10-minute recovery requirement. Always pick the managed service when the question says "least operational overhead."

upvoted 1 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: B

The meaning of option B is to create a new Grafana workspace, configure the current CloudWatch data source to it, and then import the historical Grafana instances into the new Grafana workspace.

upvoted 1 times

 **bacharbhouri** 1 year, 7 months ago

Selected Answer: C

The company has invested time and effort to create dashboards that the company wants to preserve.

B is good but it won't preserve their dashboard

upvoted 2 times

 **bacharbhouri** 1 year, 7 months ago

I mean B, sorry. Moderator please change.

upvoted 3 times

 **surya_lolla** 2 years ago

Selected Answer: B

Option B is correct, however read this, <https://docs.aws.amazon.com/grafana/latest/userguide/AMG-workspace-content-migration.html>

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

gotta be a B

upvoted 1 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: B

Def B.

upvoted 1 times

 **psyx21** 2 years, 6 months ago

Selected Answer: B

Correct answer is B

upvoted 1 times

 **bhanus** 2 years, 6 months ago

Selected Answer: B

B is the answer <https://aws.amazon.com/grafana/>

upvoted 3 times

Question #214

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.

Correct Answer: B

Community vote distribution

B (100%)

 **joleneinthebackyard** Highly Voted 1 year, 8 months ago

Selected Answer: B

Wish all questions are clear like this.

A: Drop immediately at the first sentence

B: sounds good

C: host database in ec2 instance will never a choice. Plus SSM parameter store + lambda for password rotation is not as good as secret manager

D: Again, don't migrate one type of database to another
upvoted 6 times

 **611c008** Most Recent 1 year, 1 month ago

Selected Answer: B

C is wrong as system manager parm store does not support auto rotate password

upvoted 1 times

 **kejam** 1 year, 5 months ago

Selected Answer: B

Answer B

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/>
upvoted 2 times

 **career360guru** 1 year, 7 months ago

Selected Answer: B

Option B

upvoted 2 times

 **dkcloudguru** 1 year, 9 months 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** 1 year, 10 months 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** 1 year, 11 months 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** 1 year, 11 months ago

Selected Answer: B

ofc it's B

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: B

B for sure

upvoted 2 times

 **Christina666** 1 year, 11 months ago

Selected Answer: B

Secrets manager has built-in rotation feature

upvoted 1 times

 **SkyZeroZx** 2 years ago

Selected Answer: B

keyword = Secrets Manager.

Then B

upvoted 1 times

 **psyx21** 2 years ago

Selected Answer: B

Correct answer is B

upvoted 1 times

 **easytoo** 2 years ago

b-b-b-b-b-b-b-b

upvoted 1 times

 **bhanus** 2 years ago

B is the answer

upvoted 1 times

 **chiaseed** 2 years 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** 2 years ago

Selected Answer: B

least operation... rds + secret manager

upvoted 1 times

 **nexus2020** 2 years ago

Selected Answer: B

the LEAST operational overhead. So B is the easiest

upvoted 2 times

Question #215

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.

Correct Answer: BD*Community vote distribution*

BD (75%) BC (15%) 5%

 **NikkyDicky**  2 years, 5 months ago

Selected Answer: BD

BD

they need a (one) VPC, no need for TGW.
Use case for subnet sharing via RAM

upvoted 14 times

 **LuongTo** 1 year ago

why A out?

upvoted 1 times

 **KennethYY** 1 year ago

because deploy to "each account"
upvoted 1 times

 **princajen**  4 months ago

Selected Answer: BD

Put a single, centrally managed VPC in a shared services account and share subnets via AWS RAM so teams can deploy into those subnets without owning their own VPCs. Connect that VPC to on-prem with a Site-to-Site VPN (cheap and fits <50 Mbps). Avoid Direct Connect (E) because it's expensive for this bandwidth, and avoid Transit Gateway (C) and per-account VPCs (A) because they add unnecessary cost and complexity for this scenario.

upvoted 1 times

 **8693a49** 1 year, 4 months ago

Selected Answer: AC

They are designing an account structure. This means multiple accounts, implicitly multiple VPCs. So A will take care of account provisioning. (B is incorrect, subnets cannot be shared). To connect to on-prem, site-to-site VPN is sufficient and most cost-effective, and we also need to give access to it from all accounts, so we need a Transit Gateway. Therefore C is the other correct answer. (D is incorrect because it only works for one VPC, one account, and E is incorrect because is more expensive than VPN and not necessary)

upvoted 2 times

 **8693a49** 1 year, 4 months ago

Correction. VPC subnets can be shared, so BC would work, but the resulting architecture is a networking nightmare. I would not do that.

upvoted 3 times

 **0dc6cac** 6 months, 2 weeks ago

The question says "cost-effective", transit gateways + multiple site-to-site VPNs are not cheap. In most cases, B should be enough, so you only need one site-to-site connection

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

Transit gateways are not cost-effective
upvoted 1 times

- ✉ **helloworldabc** 1 year, 4 months ago
just BD
upvoted 1 times
- ✉ **gfhbox0083** 1 year, 5 months ago
B, D for sure.
No need for a TGW
upvoted 1 times
- ✉ **LuongTo** 1 year ago
why A out?
upvoted 1 times
- ✉ **Chris_W_1234** 2 months ago
A implies that each group gets their own VPC. A further implies that each account gets their own VPN "something", i.e. presumably more than one VPN connection to on-prem would exist. I.e. more expensive than a single VPN from a shared services account.
upvoted 1 times
- ✉ **bacharbhouri** 1 year, 7 months ago
Selected Answer: BE

Why is nobody considering Direct Connect, it is cheaper than Site to Site VPN.
upvoted 1 times
- ✉ **bacharbhouri** 1 year, 7 months ago
the ask here is for most cost effectively choice.
upvoted 1 times
- ✉ **YOUSSEFWAID** 1 year, 7 months ago
If you have one VPC why you need to share the subnets ?
upvoted 2 times
- ✉ **TonytheTiger** 1 year, 9 months ago
Selected Answer: BD
Option BC & NOT C - The MOST cost effective option: AWS Site-to-Site VPN connection pricing still applies in addition to AWS Transit Gateway VPN attachment pricing. So you will be additional cost with both option

<https://aws.amazon.com/transit-gateway/pricing/>
upvoted 2 times
- ✉ **ftaws** 1 year, 11 months ago
The problem did not say how many VPC. @@@
upvoted 2 times
- ✉ **pk0619** 1 year ago
there is just one VPC if you select B which makes D the right choice for second answer
upvoted 1 times
- ✉ **ayadmaawla** 2 years ago
Selected Answer: BC
B+C in my humble opinion. Reason for C is that this is a design for a company with "multiple teams" so it is only logical that these teams will want to have at some stage independent accounts from one another and different accounts within the same teams. Thinking about a single VPC would be a bit short sighted.
upvoted 3 times
- ✉ **career360guru** 2 years, 1 month ago
Selected Answer: BD
B and D is right choice.
upvoted 2 times
- ✉ **Ighoshino78** 2 years, 1 month ago
Selected Answer: AD
Most Cost Effective...
upvoted 1 times
- ✉ **nublit** 2 years, 1 month ago
Selected Answer: AD
You need to create a singe VPC and a single Account.
upvoted 1 times
- ✉ **SK_Tyagi** 2 years, 4 months ago
Selected Answer: BD
Direct Connect may be an overkill with 1GBPs

upvoted 3 times

 **kebmiockey** 2 years, 4 months ago

Other problem with VPN is 1.25 Gb limitation.

upvoted 1 times

 **ggrodschiy** 2 years, 5 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 3 times

 **Christina666** 2 years, 5 months ago

Selected Answer: BD

Tgw is for VPCs communication.

upvoted 1 times

 **SmileyCloud** 2 years, 5 months ago

Selected Answer: BC

BC. There are multiple teams and accounts.

upvoted 3 times

Question #216

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.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

Centrally managed egress, so C/D are out.
Both A and B are wrong, because

1. There isn't internet gateway.
2. "Modify all default routes to point to the ...". A firewall or "proxy's Auto Scaling group" don't have public IP, the default route must be pointing to the NAT gateway. And NAT gateway has a peer public IP configured on the IGW. The route should be: internet prefix of all the internal subnet-> NAT gateway -> firewall -> internet gateway, and reverse routing rules are also required.

Well, considering the persistent low quality of AWS Exam Questions, I vote B
upvoted 5 times

 **easystoo** Highly Voted 2 years ago

b-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 5 times

 **princajen** Most Recent 4 months ago

Selected Answer: B

It uses a centralized egress VPC with AWS Network Firewall (managed, horizontally scalable) and a NAT Gateway, attached to the existing Transit Gateway. All spoke VPCs route outbound through the firewall for org-wide, rule-based filtering. This meets the ≤25 Gbps/AZ load, minimizes operational overhead, and avoids the cost/complexity of running EC2 proxy fleets (A, D) or duplicating firewalls in 100+ accounts (C).

upvoted 1 times

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

Selected Answer: B

c,d in each AWS account. wrong
a: use third party solution, not as good as b (use aws service)
upvoted 2 times

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

Selected Answer: B

Option B
upvoted 1 times

✉  **rif** 1 year, 8 months ago

B.
<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-nat-gateway-with-firewall.html>
upvoted 4 times

✉  **duriselvan** 1 year, 9 months ago

<https://aws.amazon.com/blogs/security/hands-on-walkthrough-of-the-aws-network-firewall-flexible-rules-engine/>
upvoted 2 times

✉  **xav1er** 1 year, 10 months 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 year, 10 months ago

bro what?

upvoted 2 times

✉  **NikkyDicky** 1 year, 11 months ago

Selected Answer: B

B for sure
upvoted 1 times

✉  **Christina666** 1 year, 11 months ago

Selected Answer: B

centrally managed outbound traffic: tgw-> centralized VPC with network firewall with rules-> internet
upvoted 4 times

✉  **chiaseed** 2 years 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 3 times

✉  **SmileyCloud** 2 years 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 2 times

✉  **psyx21** 2 years ago

Selected Answer: B

Correct answer is B
upvoted 1 times

✉  **nexus2020** 2 years ago

Selected Answer: B

vote for B
upvoted 2 times

Question #217

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.

Correct Answer: D*Community vote distribution*

D (89%)	9%
---------	----

 **Maria2023**  2 years, 6 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 16 times

 **SK_Tyagi**  2 years, 4 months 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 6 times

 **princajen**  4 months ago

Selected Answer: D

Pick D because it cleanly satisfies all three requirements with AWS-native patterns: AWS WAF (with AWS Managed Rules) filters attacks, WAF logging to Kinesis Data Firehose ships rejected/request logs to the third-party auditor, and a Multi-AZ Auto Scaling group behind an ALB provides high availability. Options A and B misuse services (Inspector/CWL), and C lacks an explicit HA compute design.
upvoted 1 times

 **85b5b55** 7 months ago

Selected Answer: D

A and D look right. But D is the correct answer. As A is using Amazon Inspector, it doesn't support monitoring traffic flow.
upvoted 1 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: D

Compared to A, prioritize AWS Kinesis over third-party auditing applications
upvoted 1 times

✉ career360guru 2 years, 1 month ago

Selected Answer: B

D is good option but as the question does not mention about 3rd party auditing app it may not be possible to directly integrate it with Firehose. One may have to use http api to push the logs - as this is not mentioned I will go with Option B.

upvoted 1 times

✉ career360guru 2 years, 1 month ago

Oh Mistake, I want to change it to D as B does not support High Availability.

upvoted 2 times

✉ xav1er 2 years, 4 months ago

Selected Answer: D

It's D, makes most sense,

upvoted 2 times

✉ chico2023 2 years, 4 months 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 2 times

✉ ggrodskiy 2 years, 5 months ago

Correct D.

upvoted 1 times

✉ NikkyDicky 2 years, 5 months ago

Selected Answer: D

its a D

upvoted 1 times

✉ javitech83 2 years, 6 months ago

Selected Answer: D

ASG in Multiple AZ. WAF and WAF logs with kinesis

upvoted 1 times

✉ chikorita 2 years, 6 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

✉ Masonyeoh 2 years, 6 months ago

Selected Answer: D

Amazon inspector does NOT inspect traffic coming to an Application Load Balancer (ALB)

upvoted 3 times

✉ PhuocT 2 years, 6 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 4 times

✉ ozelliII 2 years, 6 months ago

Selected Answer: D

Inspector does not filter inbound traffic for attack signatures, this is what WAF is for

upvoted 2 times

✉ SmileyCloud 2 years, 6 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 years, 6 months ago

but you need logs of the reject request on WAF. So I think correct answer is D

upvoted 1 times

✉ SmileyCloud 2 years, 5 months ago

It's probably B. C and D are not correct, ALB can't send logs to Kinesis Fire Hose.

upvoted 1 times

 **easytoo** 2 years, 6 months ago

a-a-a-a-a-a-a
multi-az for HA
upvoted 1 times

 **easytoo** 2 years, 4 months ago

it's d-d-d-d-d-d--d-d
upvoted 1 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.

Correct Answer: B*Community vote distribution*

B (100%)

  **SkyZeroZx** Highly Voted 1 year, 5 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 11 times

  **Just_Ninja** Highly Voted 1 year, 5 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 6 times

  **rxhan** 1 year, 5 months ago

thanks Ninja
upvoted 2 times

  **princajen** Most Recent 4 months ago**Selected Answer: B**

Private API Gateway + Interface VPC Endpoint (PrivateLink) keeps calls entirely on the AWS network and blocks public internet access. Use an endpoint policy and an API resource policy to restrict to that VPC endpoint. A misuses VPN/API keys, C confuses auth with networking and adds TGW unnecessarily, and D (Global Accelerator) exposes a public edge which violates the "no public internet" requirement.
upvoted 1 times

  **shaaam80** 1 year ago**Selected Answer: B**

Answer B - VPC Interface endpoint to privately access services without data over internet.
upvoted 3 times

  **career360guru** 1 year, 1 month ago**Selected Answer: B**

Option B
upvoted 1 times

  **NikkyDicky** 1 year, 5 months ago**Selected Answer: B**

B for sure

upvoted 1 times

 **Alabi** 1 year, 6 months ago

Selected Answer: B

B for sure

upvoted 1 times

 **SmileyCloud** 1 year, 6 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

 **easytoo** 1 year, 6 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** 1 year, 6 months ago

I vote B

upvoted 1 times

 **nexus2020** 1 year, 6 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.

Correct Answer: D

Community vote distribution

D (83%)

B (17%)

 **Sweetedad**  2 years, 3 months 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 10 times

 **bhanus**  2 years, 6 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 6 times

 **princajen**  4 months ago

Selected Answer: D

AWS Config is purpose-built to track security group changes in real time against compliance rules and can directly send alerts through SNS. B (CloudTrail + CloudWatch) only tells you who changed what, not if it's compliant. A and C misuse SCPs, which don't track or alert on security group changes. For the exam, when you see "track + alert on compliance changes," think AWS Config first.

upvoted 1 times

 **ry1999** 1 year, 3 months ago

Selected Answer: B

B is faster

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: D

Both B and D works. But the question is asking for FASTEST.

For cloudTrail, you need: CloudTrail → CloudWatch Logs → CloudWatch Metric Filter → CloudWatch Alarm → SNS Notification

For aws Config, it natively support integration with SNS.

Hence we should choose D

upvoted 3 times

 **skipbaylessfor3** 1 year, 4 months ago

I'm leaning towards D, but looks what it says in this blog:

<https://aws.amazon.com/blogs/security/how-to-monitor-aws-account-configuration-changes-and-api-calls-to-amazon-ec2-security-groups/>

For the Config option, it says:

"The use of AWS Config in Method 1 allows for the configuration of a security group to be tracked along with other AWS resources. Changes to the security group's configuration are reported during the next Config compliance evaluation, typically within 10 minutes"

and for the CloudTrail option it says:

"The use of CloudTrail and CloudWatch Events in Method 2 allows for the near real-time detection of API calls that could change the configuration of a VPC security group"

So it seems clear cut to me that the answer is B, although if I hadn't seen this blog I would've picked D probably
upvoted 1 times

 **red_panda** 1 year, 7 months ago

Selected Answer: B

For me the answer is B.

Here we are talking about "tracking al changes" and "notify for non-compliant".

It's certainly a very ambiguous question that the folks at AWS could have spared us, but for me (and for chat-gpt) B is the answer :)
upvoted 3 times

 **9esh** 1 year, 9 months ago

D: AWS Config provides rules to detect non-compliant config

B: Can track all event however doesn't provide native support for rules to detect non-compliant changes

upvoted 1 times

 **dankositze** 1 year, 10 months ago

Selected Answer: B

In my opinion, the question asks for (1) a "system that tracks CHANGES" and (2) asks to "send alerts when the engineers make NONCOMPLIANT CHANGES," I would choose B since B satisfies the first condition and D does not.

B: implies that CloudTrail tracks all changes.

D: states that Config will only track noncompliant changes, but question is asking for all changes.

But overall this is just another poorly constructed and ambiguous question and answer, which seems to be the norm with these lol
upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just D

upvoted 1 times

 **fartosh** 1 year, 7 months ago

Actually, AWS Config cannot track *only* non-compliant changes, it always tracks all changes against monitored resources - that's by design. You set rules in AWS Config that indicate whether the change is compliant, but all the changes must be recorded.

<https://docs.aws.amazon.com/config/latest/developerguide/how-does-config-work.html#resource-tracking>

upvoted 1 times

 **duriselvan** 2 years ago

B is ans

<https://aws.amazon.com/blogs/security/how-to-monitor-aws-account-configuration-changes-and-api-calls-to-amazon-ec2-security-groups/>

Speed: Implementing CloudTrail and CloudWatch is faster than setting up AWS Organizations or using SCPs. You can do it in minutes without modifying the entire account structure or deploying additional resources.

Granularity: CloudTrail and CloudWatch offer fine-grained control over monitoring and alerting, allowing you to define specific rules for noncompliant security settings.

Flexibility: You can easily adapt the CloudWatch rules to different types of noncompliance and adjust the alerts to suit your notification needs.

Existing infrastructure: If the company already uses CloudTrail for logging, setting up CloudWatch rules is a natural extension without requiring significant changes.

upvoted 2 times

 **shaaam80** 2 years ago

Selected Answer: D

Answer D. AWS Config is perfect to track config changes. SNS for notification.

upvoted 4 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

B is better option than D. D only sends an SNS alert when there are non-compliant changes. It does not allow you to actually track each and every changes engineers make.

upvoted 2 times

 **Jay_2pt0_1** 2 years, 1 month ago

I thought so too, initially, but as others have said, B does not actually send the alert.

upvoted 2 times

 **ghadxx** 2 years, 4 months ago

It's D

<https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>

upvoted 2 times

 **ggrodskiy** 2 years, 5 months ago

Correct D.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: D

D works and faster

B would work with adding a CW alert, but D still better

upvoted 4 times

 **javitech83** 2 years, 6 months ago

Selected Answer: D

correct is D

upvoted 2 times

 **SkyZeroZx** 2 years, 6 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 5 times

Question #220

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.

Correct Answer: ACE

Community vote distribution

ACE (100%)

 **easytoo** Highly Voted 2 years 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 19 times

 **yorkicurke** Highly Voted 1 year, 8 months ago

Selected Answer: ACE

this link will explain it all. looks like this question was taken from here.

<https://repost.aws/knowledge-center/kinesis-readprovisionedthroughputexceeded>

upvoted 10 times

 **shaam80** Most Recent 1 year, 7 months ago

Selected Answer: ACE

Answer ACE

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: ACE

A, C, E Options

upvoted 1 times

 **totten** 1 year, 8 months ago

Selected Answer: ACE

Option (D) "Reshard the stream to reduce the number of shards" is generally not a recommended solution because it reduces the capacity of the stream, which might lead to more throttling issues. Reducing shards should only be considered if you're overprovisioned, and reducing capacity will not negatively impact your consumers.

Option (B) "Use the Kinesis Producer Library (KPL) and adjust the polling frequency" may not be directly related to solving the throttling issue. The KPL is primarily used for producing data into the Kinesis stream, not consuming it.

Option (F) "Configure the stream to use dynamic partitioning" can be beneficial for even distribution of data but is not directly related to

resolving throttling issues. Dynamic partitioning is more about balancing the data across shards and does not increase overall read capacity.

So, the most relevant actions to address the throttling issue are (A), (C), and (E).

upvoted 5 times

 **GoKhe** 1 year, 6 months ago

Nice way to explain the reasons other way round :-)

upvoted 1 times

 **ggrodsckiy** 1 year, 11 months ago

Correct ACE.

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: ACE

ACE it

upvoted 1 times

 **SkyZeroZx** 1 year, 11 months ago

Selected Answer: ACE

ACE is correct

upvoted 1 times

 **SmileyCloud** 2 years 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 3 times

 **psyx21** 2 years ago

Selected Answer: ACE

ACE is correct

upvoted 1 times

 **nexus2020** 2 years 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.

Correct Answer: B

Community vote distribution

B (100%)

 **Maria2023** Highly Voted 2 years 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 15 times

 **totten** Highly Voted 1 year, 8 months ago

Selected Answer: B

AWS Cost Explorer provides resource optimization recommendations, including rightsizing EC2 instances based on historical usage data. These recommendations are generated for each account in the organization's management account, so you can obtain insights for all accounts centrally.

Option A introduces complexity by requiring the company to install a third-party tool on all EC2 instances, and then manually develop and maintain a custom script for identifying underutilized instances.

Option C would require you to retrieve recommendations separately for each account within the organization, increasing the administrative overhead compared to a centralized management approach.

Option D, while using native AWS services for data collection, involves creating and maintaining additional AWS services, which is more complex than the straightforward combination of CloudWatch and AWS Cost Explorer.

upvoted 7 times

 **princajen** Most Recent 4 months ago

Selected Answer: B

Use Systems Manager to deploy the CloudWatch agent (so you have CPU + memory) and then pull org-wide rightsizing recommendations from Cost Explorer in the management account. It's the lowest-effort, native approach. A/D require custom tooling and pipelines; C duplicates work across every account instead of centralizing it.

upvoted 1 times

 **duriselvan** 1 year, 6 months ago

Let's analyze each option based on effort:

A. Marketplace tool:

Effort: High

Requires manual installation of a third-party tool on all instances.

Needs custom script development to identify underutilized instances.

Manual effort needed to reference pricing information for downsizing.

B. Cost Explorer in Org Management Account:

Effort: Low

Leverages existing tools (CloudWatch agent & Cost Explorer) already available.

Recommendations readily available in the management account.

Downsizing options directly available within Cost Explorer.

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: B

Option B

upvoted 1 times

 **SK_Tyagi** 1 year, 10 months 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** 1 year, 11 months ago

Selected Answer: B

its a B

upvoted 1 times

 **bhanus** 1 year, 12 months 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 3 times

 **SkyZeroZx** 2 years 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

 **easystoo** 2 years 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 2 times

 **SmileyCloud** 2 years 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** 2 years ago

Selected Answer: B

B - Management account is the key word

upvoted 1 times

 **nexus2020** 2 years 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.

Correct Answer: BDE

Community vote distribution

BDE (100%)

 **bjexamprep** Highly Voted 1 year, 10 months ago

Selected Answer: BDE

This is a bad question design.

The question is looking for a solution for "The network routes are not updated when the instance replacement occurs.", which means the ASG already has the capability to detect the failure node. With this assumption, there is NO need to install a CloudWatch agent on the EC2 instance, cause the CloudWatch agent in B is doing the same thing.

The correct solution is to use the ASG Lifecycle Hook to invoke the Lambda to update the route.

A better solution is to create a loadbalancer targeting the ASG, and update the route to point to the loadbalancer. With this solution, there is no need to update the route anymore.

upvoted 9 times

 **EzKkk** 2 weeks, 5 days ago

Agree, I'm so confused because I can't wrap my head around the question. The root of the problem can be easily solved using a simple load balancer. Maybe it would incur some addition cost but by far it's the most direct solution

upvoted 1 times

 **NikkyDicky** Highly Voted 2 years, 5 months ago

Selected Answer: BDE

CW agent->CW metric->CW alarm->Lambda action

upvoted 9 times

 **princajen** Most Recent 4 months ago

Selected Answer: BDE

Use CloudWatch agent to emit process metrics (not just EC2 status checks), alarm on failures and send to SNS (D), and trigger a Lambda to take the failed instance out of service and update the VPC routes to the new ASG instance (E). Options A/C don't detect app-level failure correctly, and F tries to use CloudFormation for runtime routing, which isn't appropriate.

upvoted 1 times

 **chris_spencer** 1 year, 2 months ago

Selected Answer: BDE

BDE.. but a professional should use ASG Lifecycle hooks <https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html>

upvoted 1 times

 **NoDoubkevo** 1 year, 3 months ago

you cannot update templates you can version them.

ADE

upvoted 1 times

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

why can't you update CloudFormation templates?

upvoted 1 times

✉ **shaaam80** 2 years ago

Answer - BDE

Install CW agent on all instances using CF template

Configure CW to send out metrics to SNS

Configure Lambda as SNS target to terminate instance and update n/w routes on the new instances

upvoted 1 times

✉ **career360guru** 2 years, 1 month ago

Selected Answer: BDE

B, D, E

upvoted 2 times

✉ **Piccaso** 2 years, 5 months ago

Selected Answer: BDE

A and F must be wrong.

upvoted 2 times

✉ **PhuocT** 2 years, 6 months ago

Selected Answer: BDE

B, D and E

upvoted 3 times

✉ **easytoo** 2 years, 6 months ago

b-d-e seems reasonable.

upvoted 2 times

✉ **SmileyCloud** 2 years, 6 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 4 times

✉ **james55** 2 years, 6 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.

Correct Answer: D

Community vote distribution

D (91%)	9%
---------	----

 **SmileyCloud** Highly Voted 1 year, 6 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 15 times

 **emiliocb4** 1 year, 6 months ago

NLB supports HTTPS so why excluding A?
 upvoted 1 times

 **SmileyCloud** 1 year, 5 months 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 9 times

 **ForDummies** 7 months, 1 week ago

But this ELB will be used to on-demand video application, so ALB is out. Also, ECS will use HTTPS, not ELB.
 upvoted 1 times

 **Hypercuber** Highly Voted 1 year, 5 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 5 times

 **career360guru** Most Recent 1 year, 1 month ago

Selected Answer: D

Option D
 upvoted 1 times

 **ggrodsckiy** 1 year, 5 months ago

Correct D.
 upvoted 1 times

 **nicecurls** 1 year, 5 months ago

Selected Answer: D

select D. for Fargate there is no Cluster Auto Scaling there.

upvoted 2 times

NikkyDicky 1 year, 5 months ago

Selected Answer: D

D

no NLB for ECS, no Cluster for Fargate

upvoted 2 times

vjp_training 1 year, 4 months 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 1 year, 6 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 1 year, 6 months ago

Selected Answer: D

<https://repost.aws/knowledge-center/ecs-fargate-service-auto-scaling>

upvoted 2 times

easystoo 1 year, 6 months ago

d-d-d-d-d-d-d

upvoted 1 times

james55 1 year, 6 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 1 year, 6 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 1 year, 6 months 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).

Correct Answer: A*Community vote distribution*

A (100%)

joleneinthedbackyard Highly Voted 1 year, 8 months ago**Selected Answer: A**

You want to look for "scan on push" solution, as scanning periodically is not enough, damage might have been done -> C, D is out, only A, B

A sounds complex, but B even worse, how can you put result in SQS? wording is so bad if they means sending message to SQS. Notifying by SES is a straight red flag that AWS exams like to use.

Only A makes sense.

upvoted 10 times

kz407 1 year, 3 months ago

Problem with this approach is, if you scan only what's pushed, and it has a zero-day vulnerability, you won't see it. Since you are scanning only when you are pushing, you won't detect the vulnerability ever. IMO, scanning periodically gives a better shot. Ideally it should be scanning both on push and periodically.

upvoted 3 times

kz407 Most Recent 1 year, 3 months ago**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html>

In a nutshell, 2 types of scans.

Basic: Scanned against CVE DB, "ON PUSH" or a manual scan. Don't see any way of notifying anywhere.
Enhanced: Ongoing scanning with Amazon Inspector, findings delivered via EventBridge notifications.

Closest answer would be A.

upvoted 2 times

shaaam80 1 year, 7 months ago**Selected Answer: A**

Answer A.

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: A

Option A

upvoted 2 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: A

A, but I think step function need to call Lambda to delete tag. there is not direct ecr integration

upvoted 3 times

 **SkyZeroZx** 2 years 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 2 times

 **Maria2023** 2 years 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** 2 years 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 2 times

 **SmileyCloud** 2 years 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** 2 years ago

Selected Answer: A

Use the building feature if you can, so scan on push. And A make more sense

upvoted 1 times

 **bhanus** 2 years 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** 2 years 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.

Correct Answer: B

Community vote distribution

B (100%)

 elanelans Highly Voted 2 years 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 14 times

 titi_r Most Recent 1 year, 2 months ago

Selected Answer: B

B - "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."

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 1 times

 shaaam80 1 year, 7 months ago

Answer B. Compute Savings plan covers EC2, Fargate & Lambda. Instance Savings plan only for EC2 instances.

upvoted 3 times

 career360guru 1 year, 7 months ago

Selected Answer: B

Option B

upvoted 1 times

 NikkyDicky 1 year, 11 months ago

Selected Answer: B

its a B

upvoted 1 times

 SkyZeroX 2 years 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 2 years ago

Selected Answer: B

B, magic keywords - Management account and Compute savings Plan.

upvoted 1 times

 **nexus2020** 2 years ago

Selected Answer: B

Compute Savings plan is made for this usage type

upvoted 1 times

 **bhanus** 2 years ago

Selected Answer: B

B- compute savings plans covers all ec2, fargate, lambda.

upvoted 1 times

Question #226

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.

Correct Answer: A

Community vote distribution

A (100%)

 **elanelans** Highly Voted  2 years, 6 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 10 times

 **85b5b55** Most Recent  10 months, 1 week ago

Selected Answer: A

AWS Budgets can help for daily tracking and notify through SNS.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: A

A: AWS Budgets + SNS = Easy budget (daily) tracking and alerts

B: Trusted Advisor is for recommendations, not daily budgets.

C: Control Tower is for governance, not budget alerts

D: Complex setup with no added value over AWS Budgets

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

Option A

upvoted 1 times

 **nicecurls** 2 years, 5 months ago

Selected Answer: A

ofc it's A <https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-professional-sap-c02/view/#>

upvoted 3 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

straight A

upvoted 2 times

 **SkyZeroZx** 2 years, 5 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 2 times

 **rxhan** 2 years, 5 months ago

you copy and paste other people answers

upvoted 7 times

 **easytoo** 2 years, 6 months ago

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

upvoted 1 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: A

This one is simple. A

upvoted 1 times

 **nexus2020** 2 years, 6 months ago

Selected Answer: A

A, simple one

upvoted 1 times

 **MoussaNoussa** 2 years, 6 months ago

A is the answer

upvoted 1 times

 **bhanus** 2 years, 6 months ago

Selected Answer: A

A is the answer

upvoted 1 times

Question #227

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.

Correct Answer: C*Community vote distribution*

C (95%)	5%
---------	----

 **chico2023** Highly Voted 1 year, 10 months 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 30 times

 **Jay_2pt0_1** 1 year, 6 months ago
Kudos to you for such a great explanation!
upvoted 2 times

 **kpcert** Most Recent 1 year ago

Selected Answer: C
Between A and C, I would choose C - Transfer Acceleration, as this issue is focusing on improving the upload performance across the region
upvoted 1 times

 **rohan0411** 1 year ago
Why not B?
upvoted 1 times

 **Monsterpuss** 6 months, 2 weeks ago
Because Cloudwatch is a CDN aimed at delivering out content, not uploading it.
upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: C
Option C. As the users in Europe only are facing this issue. A would improve upload performance overall for both US and Europe.
upvoted 3 times

 **Pupu86** 1 year, 7 months ago
I believe this question should rightfully be a multi-choice question where A and C are the answer together to solve this problem statement

<https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>
upvoted 2 times

 **skyhiker** 1 year, 10 months 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 year, 10 months ago
C would be the answer if the 's' was removed. Will go with C.

upvoted 1 times

✉ **RGR21** 1 year, 11 months 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.
<https://aws.amazon.com/pt/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

upvoted 1 times

✉ **ggrodsckiy** 1 year, 11 months ago

Correct C.

upvoted 1 times

✉ **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

C

would be good in combination with A, but better as a standalone choice

upvoted 1 times

✉ **Christina666** 1 year, 11 months ago

Selected Answer: C

upload performance-> transfer acceleration

upvoted 1 times

✉ **javitech83** 1 year, 12 months ago

Selected Answer: C

correct is C

upvoted 1 times

✉ **pupsik** 2 years ago

Selected Answer: A

Transfer Acceleration doesn't guarantee a significant increase in upload speed.

A multi-part upload on 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

✉ **SeemaDataReader** 1 year, 5 months ago

Reading carefully into the blog looks like the author did some maths wrong.

Multipart upload took 43s which is 40% faster than base of 72s

Transfer acceleration took 45s which is 38% faster than base of 72s.

So based on this multipart gives better performance

upvoted 1 times

✉ **shmoeee** 10 months, 2 weeks ago

Double check your math brother.

upvoted 1 times

✉ **YodaMaster** 1 year, 11 months 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 4 times

✉ **SkyZeroZx** 2 years ago

Selected Answer: C

C. <https://aws.amazon.com/s3/transfer-acceleration/>

upvoted 1 times

✉ **SmileyCloud** 2 years ago

Selected Answer: C

C. <https://aws.amazon.com/s3/transfer-acceleration/>

upvoted 2 times

✉ **MoussaNoussa** 2 years ago

C of course

upvoted 1 times

✉ **bhanus** 2 years 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

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.

Correct Answer: D*Community vote distribution*

D (84%)

Other

 **pupsik** Highly Voted 2 years, 6 months ago

Selected Answer: D

A looked good until "store session data in SQS".

upvoted 26 times

 **SkyZeroZx** Highly Voted 2 years, 6 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 16 times

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

Selected Answer: A

AWS Fargate removes all EC2 instance management, providing the lowest ongoing operational overhead.

It's fully serverless for containers, integrates directly with EFS for shared data, and uses managed, serverless services (EFS, SQS) for persistence.

EKS (as in D) still requires node management, Kubernetes configuration, and more operational effort, so it's not as lightweight as Fargate.

upvoted 1 times

 **Curious76** 6 months ago

Selected Answer: A

Why A is the best choice (least operational overhead):

ECS on Fargate:

Serverless compute engine for containers.

No infrastructure to manage (automatic scaling, patching, etc.).

Lowest operational overhead compared to EC2 or self-managed Kubernetes.

Amazon EFS:

Fully managed, scalable file storage accessible by multiple containers.

Great for sharing data between tiers and across availability zones.

Session persistence using SQS:

This may sound odd, but SQS can be used as a lightweight buffer or to manage ephemeral session metadata in stateless apps.

However, in production, something like DynamoDB or ElastiCache is often better. But the question emphasizes "least operational overhead", and SQS is fully managed and scalable.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: D

By exclusion of the other options, the least worst answer is D.

upvoted 3 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: D

B,D can do it all.

Multiple EC2 accesses a single storage using EFS and EBS, with priority given to EFS file storage.

DynamoDB can also be used for session storage.

<https://docs.aws.amazon.com/aws-sdk-php/v2/guide/feature-dynamodb-session-handler.html>

upvoted 1 times

 **43c89f4** 1 year, 8 months ago

one of the poor Question... so answer we give poor... its D. because i cant choose ABC

upvoted 4 times

 **ayadmawla** 2 years ago

Selected Answer: B

I think that the issue of multi-attach EBS in one AZ is dealt with by the manner in which it is explained. It is the EC2 that are distributed in Multi-AZ not the EBS. Just my pov.

upvoted 4 times

 **career360guru** 2 years, 1 month ago

Selected Answer: D

Option D, Though C is also possible but Multi-attach EBS has higher operational overhead.

upvoted 2 times

 **covabix879** 2 years, 2 months ago

Selected Answer: D

Due to operational efficiency D is better choice compared to B.

upvoted 1 times

 **task_7** 2 years, 2 months ago

Selected Answer: D

deployments carry ReplicaSets

DynamoDB table for session data

upvoted 1 times

 **rsn** 2 years, 3 months ago

Selected Answer: C

There is a requirement for fault tolerance. I feel 'C' satisfies that as it has replicaset.

upvoted 1 times

 **skyhiker** 2 years, 4 months 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** 2 years, 3 months 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 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: D

D - best of the worst

upvoted 7 times

 **YodaMaster** 2 years, 5 months ago

Selected Answer: D

A looked good until "store session data in SQS".
upvoted 2 times

 **Henrytml** 2 years, 6 months ago

A looked good until "store session data in SQS".
upvoted 3 times

 **javitech83** 2 years, 6 months ago

Selected Answer: D

A looked good until "store session data in SQS".
upvoted 2 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.

Correct Answer: C*Community vote distribution*

C (58%)

B (39%)

✉  **SmileyCloud**  2 years, 6 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 17 times

✉  **yorkicurke** 2 years, 1 month ago

the following link maybe helpful for some;
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html#CHAP_Target.S3.Limitations
upvoted 3 times

✉  **Ganshank**  2 years, 4 months 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 14 times

✉  **Malluchan**  3 months, 1 week ago

Selected Answer: C

Native SQL Server replication (transactional replication, Always On, or log shipping depending on your environment) lets you keep the source fully operational while you replicate changes to the AWS target. That minimizes the cutover window and supports near-zero downtime cutover
upvoted 1 times

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

Selected Answer: C

C is correct because using SQL Server's native high availability and replication tools allows near-real-time synchronization to Amazon RDS for SQL Server.
This approach enables a quick cutover with minimal downtime and avoids extra migration steps or intermediate data loads required by the other options.
upvoted 1 times

✉  **Kaps443** 6 months, 2 weeks ago

Selected Answer: C

Uses native replication; minimal downtime; direct migration
upvoted 2 times

✉  **0b43291** 1 year, 1 month ago

Selected Answer: C

By using native database high availability tools and replication methods, you can achieve near-zero downtime during the migration process. The other options may not provide the same level of seamless data replication and minimal downtime as the native SQL Server replication tools.

Option 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.

While AWS DMS can be used for migrations, it introduces additional complexity compared to native SQL Server replication tools. Staging data in Amazon S3 and then loading into the target RDS instance can cause downtime during the final cutover. Native replication tools can directly replicate data to the target RDS instance without an intermediate storage solution.

upvoted 5 times

 **jefnmet** 1 year, 4 months ago

B look correct to me

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just C

upvoted 1 times

 **8693a49** 1 year, 4 months ago

Selected Answer: B

B is the AWS way of doing a DB migration. C might work and could be better in some cases, but because the DBs are legacy you might run into compatibility issues or limitations with the tooling. If the databases are very large you really want to use B because you need to ship the bulk of the data with Snowball.

upvoted 1 times

 **CAIAsia** 1 year, 5 months ago

Selected Answer: C

C. Correct, Near-Zero Downtime.

A. In-Place Upgrade and Migration to Aurora: This involves multiple steps and the potential for increased downtime during the cutover process.

Schema Conversion: Depending on the complexity of the legacy system, converting schemas and ensuring compatibility with Amazon Aurora can be challenging and time-consuming.

B. Intermediate Storage in Amazon S3: Adds complexity

Two-Step Process: First replicating to Amazon S3 and then loading into Amazon RDS adds additional steps and potential points of failure.

upvoted 1 times

 **grandcanyon** 1 year, 5 months ago

Selected Answer: B

In option C - "Connect the source system to an Amazon RDS for Microsoft SQL Server DB instance", should be target, not source

upvoted 2 times

 **trungtd** 1 year, 6 months ago

Selected Answer: C

Use AWS Database Migration Service (AWS DMS) to "rehost" the database????

How you can "rehost" database with DMS

upvoted 1 times

 **michele_scar** 1 year, 7 months ago

Selected Answer: B

DMS should be the better service for this use case

upvoted 2 times

 **titi_r** 1 year, 7 months ago

Selected Answer: C

Answer: C.

upvoted 1 times

 **BrijMohan08** 1 year, 8 months ago

Selected Answer: A

AWS Application Migration Service (MGN) is a highly automated lift-and-shift (rehost) solution that simplifies the migration of applications to AWS. It supports near-zero downtime migrations by continuously replicating the source servers to AWS.

Repointing the applications to Amazon Aurora Serverless satisfies the migration to the modern data architecture.

upvoted 2 times

 **svenkata18** 1 year, 9 months ago

Why not A as the question the it should rearchitected from legacy

upvoted 1 times

 **JOKERO** 1 year, 9 months ago

Native database high availability (HA) tools include the Always On or distributed availability group clusters in Microsoft SQL Server and Oracle's Data Guard replications. This approach requires a major effort to set up across extended, cross-site HA clusters, and might cause some performance degradation because of the longer latency to achieve fully synchronous active/active deployments. However, this method provides the closest to near-zero downtime during the cutover.

upvoted 4 times

 **ftaws** 1 year, 11 months ago

What is "native database high availability tools"????

upvoted 1 times

Question #230

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.

Correct Answer: CD

Community vote distribution

CD (42%)	BD (39%)	Other
----------	----------	-------

 **SkyZeroZx** Highly Voted 2 years, 5 months 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 17 times

 **helloworldabc** 1 year, 4 months ago

just CD

upvoted 1 times

 **xav1er** Highly Voted 2 years, 3 months 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 9 times

 **Malluchan** Most Recent 3 months, 1 week ago

Selected Answer: AD

A - Use Amazon VPC sharing (AWS RAM) to put provider workloads and consumer workloads into the same VPC subnets/AZs without creating peering or extra hops.

D - Interface endpoints provide regional and zonal DNS names. If a consumer resolves to the endpoint IP in the same AZ (use the zone-specific DNS name), traffic stays AZ-local and avoids inter-AZ transfer.

upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 4 months, 2 weeks ago

Selected Answer: CD

Choose C and D because they keep traffic in the same Availability Zone. Disabling NLB cross-zone load balancing (C) and using the AZ-specific PrivateLink endpoint DNS (D) stop requests from crossing AZs, which is what drives up data-transfer costs.

upvoted 1 times

 **youonebe** 1 year, 1 month ago

Selected Answer: CD

Normally when data leaves AZ to another, there is a cost associated
upvoted 2 times

sam2ng 1 year, 1 month ago

This is why C is correct:

"For ALB and CLB, there is no cross-AZ data transfer charges within the same VPC. But for NLB, if the client and target are in one AZ, but the NLB is in another AZ, there will be a zone-in and zone-out which is \$0.02."

upvoted 3 times

JoeTromundo 1 year, 2 months ago

Selected Answer: CD

B is not an option: While placing resources in the same organization might simplify management, it does not inherently reduce data transfer charges. Data transfer costs between AWS Organizations accounts are typically not impacted by being in the SAME OR DIFFERENT organizations, especially when using PrivateLink.

upvoted 2 times

vip2 1 year, 5 months ago

Selected Answer: CD

C D is correct one

For C, Cross-zone load balancing can distribute traffic across multiple AZs, which increases data transfer costs between AZs. Disabling cross-zone load balancing ensures that traffic remains within the same AZ, reducing the associated data transfer charges. This is particularly important for applications using AWS PrivateLink, as it will help keep data transfers within the same AZ as much as possible.

upvoted 2 times

michele_scar 1 year, 7 months ago

Selected Answer: CD

B is useless because if you place the resource in the same org but in different AZs you will pay the same as different org in different AZs. So B is uncorrect (like A and E).

Remains C and D as a solution that should reduce costs.

upvoted 4 times

seetpt 1 year, 7 months ago

Selected Answer: BD

BD for me

upvoted 3 times

4555894 1 year, 8 months ago

B - allows data transfer between linked accounts to be free of charge.

D - ensures traffic stays within the same AZ as much as possible, minimizing inter-AZ data transfer costs.

CD - Save money.

upvoted 2 times

VerRi 1 year, 9 months ago

Selected Answer: BD

"The company manages two organisations in AWS Organizations," which means they have one organisation for service providers and one more for consumers.

A. Since applications are created in the provider organisation, sharing the subnet with other accounts within the same organisation has no effect.

B. Combining provider and consumer into one organisation is the first move for Option D.

C. Cross-zone load balancing does not change the amount of data traffic passing through the NLB, it affects how that traffic is distributed across the targets.

D. AZ-specific endpoint helps to reduce data transfer charges because it keeps the traffic in a single AZ and is designed for intra-regional communication within the same account or organization.

E. WTF

upvoted 5 times

Dgix 1 year, 9 months ago

Selected Answer: BD

It's B and D.

A. Sharing subnets does not directly reduce data transfer charges.

C. Turning off cross-zone load balancing does not impact data transfer costs between VPC endpoints and service consumers.

E. A Savings Plan reduces costs for compute usage, not specifically for data transfer charges.

upvoted 6 times

mav3r1ck 1 year, 9 months ago

Turning off cross-zone load balancing can reduce inter-AZ data transfer costs. With cross-zone load balancing disabled, a Network Load Balancer (NLB) only routes requests to targets in the same Availability Zone as the load balancer node that received the request. This setup reduces the data transferred across Availability Zones, thereby reducing costs.

upvoted 3 times

ajeeshb 1 year, 9 months ago

Selected Answer: CD

Answer: C, D
upvoted 4 times

 **marszalekm** 1 year, 10 months ago

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html> "Can share with only AWS accounts in its own organization."
ec2:Subnet
upvoted 2 times

 **Wardove** 1 year, 10 months ago

Selected Answer: CD

Answer is CD
D) Obvious option, This approach minimizes data transfer costs by ensuring that traffic between service consumers and service providers stays within the same Availability Zone
C) Only after setting up your NLB, you can create a VPC Endpoint Service (VPC-E) that is powered by AWS PrivateLink. Cross-zone lb feature is optional for NLB since 2018 so, turning off cross-zone load balancing can help ensure that data does not unnecessarily cross Availability Zones, thereby once again reducing data transfer costs
<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html>

B) Incorrect: putting the workloads into 1 org - would not make any effect on billing neither, unless you change the topology profoundly and move away the VPCE solution - but we are not talking about Re-architecting, we are looking to provide guidelines
A) Incorrect: RAM can be used only within 1 organization
E) Incorrect: there is no such flavor of Saving plans, AWS provides 3 Compute, EC Instance and SageMaker Saving plans
upvoted 7 times

 **JOKERO** 1 year, 9 months ago

You can also share with specific AWS accounts by account ID, regardless of whether the account is part of an organization.
upvoted 1 times

 **LazyAutonomy** 1 year, 11 months ago

Selected Answer: BD

Holy bageezus, never seen a discussion thread so divided.

@NikkyDicky is spot on - cross zone traffic is indeed where the money is going. I think we all know that.

A - appears incorrect, we cannot share subnets between accounts in different AWS Orgs. Even if you could, or even if you chose A+B, it would be impractical to assume all other workloads could be deployed in service provider subnets. Would probably run out of IPs. And even if the subnets were huge and we didn't run out of IPs, there is no mechanism in A to guide developers deploying their workloads to reduce or prevent cross-AZ traffic. You could share the subnets and deploy all provider/consumer workloads in the same set of subnets and still end up with the same huge bill :-)

upvoted 6 times

 **LazyAutonomy** 1 year, 11 months ago

B - appears correct. @Just_Ninja's explanation nails it. If you use Organizations and you create accounts, then in each member account, the logical identifiers for each availability zone (e.g. "eu-central-1a") are guaranteed to map to the same AZ Physical ID (e.g. "euc1-az3") for all accounts within the Organization. In other words, it's likely that AZ "eu-central-1a" for accounts in OrgABC is not the same as AZ "eu-central-1a" for accounts in OrgXYZ. That's a problem if you're trying to eliminate unnecessary cross-zone traffic. Without this, you could instruct developers to use AZ-specific DNS names and still end up with the same huge bill :-)

upvoted 1 times

 **LazyAutonomy** 1 year, 11 months ago

C - appears incorrect, but the reason has nothing to do with "compromising high availability". As pointed out by @elmoh, cross-zone load balancing isn't enabled by default in NLBs anyway. See <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/network-load-balancers.html#cross-zone-load-balancing>. Even if cross-zone load balancing was enabled by default in NLBs, this option doesn't cover the Gateway Load Balancer VPC endpoint service use case.

upvoted 2 times

Question #231

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.

Correct Answer: A

Community vote distribution

A (96%)	4%
---------	----

 **SkyZeroZx** Highly Voted  1 year, 12 months ago

Selected Answer: A

File Gateway == SMB , NFS
 Volumes Gateway == iSCSI
 Tape Gateway = VTL
 upvoted 33 times

 **SIJUTHOMASP** Most Recent  12 months ago

Selected Answer: A

Guys, options B and C are exactly same. :)
 upvoted 1 times

 **duriselvan** 1 year, 6 months ago

Ans D
 he most cost-effective solution for moving the backups to S3 is D. Deploy an AWS Storage Gateway volume gateway, create an SMB file share, and automate data copies to S3.

Here's why:

Cost-effectiveness: Volume gateways use Amazon EBS volumes for local storage, which is typically more cost-effective than Amazon FSx for Windows File Server for storing large amounts of data. Additionally, this approach avoids the need for additional backups within Amazon FSx, further reducing costs.

Direct Connect utilization: Leveraging the existing Direct Connect connection optimizes network bandwidth for transferring data to S3, minimizing latency and potential data transfer charges.

Automated backups: Automating copies of the nightly exports to S3 ensures reliable backups and minimizes manual intervention.
 upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: A

Option A
 upvoted 2 times

 **yorkicurke** 1 year, 7 months ago

Selected Answer: A

if you read the end of the following link's paragraph, its right there in documentation;
https://aws.amazon.com/storagegateway/features/#Gateway_Types
 under "Amazon S3 File Gateway"

Customers can use Amazon S3 File Gateway to back up on-premises file data as objects in Amazon S3 (including Microsoft SQL Server and Oracle databases and logs), and for hybrid cloud workflows using data generated by on-premises applications for processing by AWS services such as machine learning or big data analytics.

upvoted 3 times

✉ **NolaHOla** 1 year, 7 months ago

But the answer A never mentions S3 file gateway?

upvoted 2 times

✉ **SK_Tyagi** 1 year, 10 months ago

Selected Answer: A

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

upvoted 1 times

✉ **rafael796** 1 year, 10 months ago

Selected Answer: A

file gateway = most cheap

upvoted 1 times

✉ **NikkyDicky** 1 year, 11 months ago

Selected Answer: A

A - SMB mount = file gw

upvoted 2 times

✉ **RockyLeon** 2 years 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** 2 years 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 2 times

✉ **Maria2023** 2 years 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** 2 years ago

Selected Answer: A

It's A (file gateway). Volume gateway is iSCSI.

upvoted 2 times

✉ **Jackhemo** 2 years 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

✉ **easytoo** 2 years 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** 2 years 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

 **bjexamprep** 1 year, 6 months ago

The backend of storage gateway is actually S3 storage, which means both volume gateway and file gateway share the same cost for storage.

And the gateway cost is the same according to aws pricing: <https://aws.amazon.com/storagegateway/pricing/>. so where did you get the "D is Block level, for sure will cost more"?

upvoted 1 times

 **bhanus** 2 years 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

 **gd1** 2 years ago

Volume will iSCSI so hat is out. Therefor A is correct

upvoted 1 times

 **Jackhemo** 2 years ago

Use olabiba.ai. It is better.

upvoted 1 times

 **PhuocT** 2 years 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 2 times

 **bhanus** 1 year, 12 months ago

I might be wrong with my theory. Going with A

upvoted 1 times

Question #232

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.

Correct Answer: B

Community vote distribution

B (100%)

 **Pupu86** Highly Voted 2 years, 1 month ago

Selected Answer: B

In fact site to site VPN would be more affordable than deploying a Direct Connect leased line. However, AWS also wants to market their product by stating that there is a need to increase throughput (site to site only can achieve max of 1.25Gbps) and consistent user experience (AWS Direct Connect > Site-to-Site VPN) so B would be a better choice.

upvoted 9 times

 **gfhbox0083** Most Recent 1 year, 5 months ago

B, for sure.
For a consistent network experience
upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: B
<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html>
upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B
Option B may not be most cost-effective best option in terms of performance.
upvoted 3 times

 **joleneinthebackyard** 2 years, 1 month ago

Anyone can explain that why Site to Site VPN not valid?
upvoted 1 times

 **fartosh** 1 year, 7 months ago

The company wants to increase bandwidth throughput, which is gained by establishing Direct Connect.
upvoted 2 times

 **Gabehcoud** 2 years, 4 months 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 years, 5 months ago

Selected Answer: B
B.
Cant be D because TGW doesn't support transitive connections, so if users connect to a VPN it invalidates this option.
A and C are skipable on the first phrase.
upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B no doubt
upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: B

direct connect + vpc = direct connect gw + TGW. so B
upvoted 3 times

 **rxhan** 2 years, 5 months ago

Mr. copy and paste
upvoted 3 times

 **Maria2023** 2 years, 6 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** 2 years, 6 months ago

Selected Answer: B

B. No need for D and S2S VPN.
upvoted 1 times

 **aragon_saa** 2 years, 6 months ago

BBBBBBBBBBBB?
upvoted 1 times

 **nexus2020** 2 years, 6 months ago

Selected Answer: B

direct connect + vpc = direct connect gw + TGW. so B
upvoted 3 times

Question #233

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.

Correct Answer: D

Community vote distribution

D (100%)

 **bhanus** Highly Voted 2 years, 6 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 6 times

 **duriselvan** Most Recent 2 years ago

A is ans

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.

Here's why:

Cross-account roles: Provide a secure and managed way for users or services in one AWS account to access resources in another account.
Least privilege access: Configure the cross-account role with the minimum permissions needed to stop or terminate resources in the member accounts, minimizing potential security risks.

Centralized control: Maintaining user credentials and access in the management account simplifies centralized management and auditing.
upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just D

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: D

Option D

upvoted 2 times

 **skyhiker** 2 years, 4 months 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 years, 5 months ago

Selected Answer: D

its a D

upvoted 2 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: D

One user is sufficient and you need cross-account role.

upvoted 4 times

 **MoussaNoussa** 2 years, 6 months ago

D - Cross account role should be created in destination(member) account. The role has trust entity to master account.
upvoted 2 times

 **bhanus** 2 years, 6 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 3 times

Question #234

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.

Correct Answer: D

Community vote distribution

D (100%)

 **TonytheTiger** 1 year, 3 months ago

Selected Answer: D

The steps to do on How To -

<https://aws.amazon.com/blogs/storage/recovering-network-file-shares-with-aws-elastic-disaster-recovery-and-aws-datasync/>
upvoted 1 times

 **shaaam80** 1 year, 7 months ago

Selected Answer: D

Answer D

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: D

Option D

upvoted 1 times

 **SK_Tyagi** 1 year, 10 months ago

Selected Answer: D

FSX for Windows and Elastic Disaster Recovery

upvoted 4 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: D

its a D

upvoted 1 times

 **SmileyCloud** 2 years ago

Selected Answer: D

You need FSx, not EFS and def not S3.

upvoted 2 times

 **PhuocT** 2 years ago

Selected Answer: D

D is the answer

upvoted 1 times

 **Alabi** 2 years ago

Selected Answer: D

D for sure
B is wrong because you cannot use EFS for Windows EC2 Servers
upvoted 1 times

 **MoussaNoussa** 2 years ago

D is the right answer
upvoted 1 times

 **bhanus** 2 years 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 4 times

Question #235

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.

Correct Answer: ACF*Community vote distribution*

ACF (93%)

7%

 **aviathor** Highly Voted 1 year, 4 months 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 13 times

 **duriselvan** Most Recent 1 year ago

- C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.
- D. Ensure the cluster is launched across multiple Availability Zones.
- F. Replace Amazon EFS with Amazon FSx for Lustre.

upvoted 2 times

 **srv321** 1 year ago

Selected Answer: ACF

Going to ACF ,looks logical
upvoted 1 times

 **career360guru** 1 year, 1 month ago

Selected Answer: ACF

A, C, F
upvoted 2 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: ACF

ACF for performance
upvoted 1 times

 **bhanus** 1 year, 6 months ago

Selected Answer: ACF

@MODERATOR - Please remove my previous comment. I agree with ACF. Thank you MoussaNoussa for clarifying
upvoted 1 times

 **javitech83** 1 year, 6 months ago

Selected Answer: ACF

ACF is the correct answer

upvoted 1 times

 **SkyZeroZx** 1 year, 6 months ago

Selected Answer: ACF

A, C and F

upvoted 1 times

 **SkyZeroZx** 1 year, 6 months ago

- B) Not is correct because ENI not more performance in this case with HPC Cluster
- D) sonds good but not is good option because performance is required in same AZ is the cluster placement group strategy more adecuate
- E) replace EFS by EBS not is apropiate for performance

upvoted 1 times

 **SmileyCloud** 1 year, 6 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 3 times

 **PhuocT** 1 year, 6 months ago

Selected Answer: ACF

A, C and F

upvoted 1 times

 **ozelllll** 1 year, 6 months ago

Selected Answer: ACF

ACF is the correct answer

upvoted 1 times

 **easytoo** 1 year, 6 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 2 times

 **nexus2020** 1 year, 6 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** 1 year, 6 months ago

ACF is the right answer

upvoted 2 times

 **bhanus** 1 year, 6 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

 **MoussaNoussa** 1 year, 6 months ago

performance is the main goal. so running HPC in the same AZ is the right choice here

upvoted 5 times

✉  **bhanus** 1 year, 6 months ago

Thank you @ MoussaNoussa for clarifying. Agreed.

upvoted 1 times

✉  **bhanus** 1 year, 6 months ago

changing my vote to ACF as per below suggestion

upvoted 1 times

Question #236

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.

Correct Answer: A*Community vote distribution*

A (84%)

B (16%)

 **duriselvan** Highly Voted 1 year, 6 months ago

The most suitable solution for applying standardized tags across the organization with specific values for each OU is 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 for each OU. Attach the tag policies to the OUs.

Here's why:

Enforce tag standardization: An SCP applied to the entire organization denies resource creation unless the required tags are present, ensuring consistent tagging across all accounts.

OU-specific tags: Tag policies attached to each OU define the specific tag values for that OU, allowing customization without compromising overall standardization.

Granular control: Attaching tag policies to OUs instead of the management account provides more granular control and flexibility for managing tags within each OU.

upvoted 8 times

 **Maria2023** Highly Voted 2 years 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 6 times

 **duriselvan** Most Recent 1 year, 6 months ago

A is ans

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: A

Option A

upvoted 1 times

 **nicecurls** 1 year, 11 months ago

Selected Answer: A

FOR EACH OU's

upvoted 2 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: A

it's an A

upvoted 1 times

 **dkx** 1 year, 11 months 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** 1 year, 11 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 4 times

✉️ **santi1975** 1 year, 11 months ago

Sorry, I mean cannot be B, and the correct answer is A!
upvoted 2 times

✉️ **43c89f4** 1 year, 1 month ago

The Question mentions "Each of the company's OUs will have unique tag values." the values list will change for OU's

My answer is A

upvoted 2 times

✉️ **Piccaso** 1 year, 11 months ago

Selected Answer: A
C and D must be wrong, because of "allow ... "
B is weird.
upvoted 1 times

✉️ **SkyZeroZx** 1 year, 12 months 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

✉️ **SmileyCloud** 2 years 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 3 times

✉️ **bhanus** 2 years 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** 2 years ago

I think it's A
upvoted 2 times

✉️ **gd1** 2 years ago

GPT 4. 0 says A - I agree. Values per OU
upvoted 2 times

✉️ **easytoo** 2 years ago

b-b-b-b-b
upvoted 1 times

✉️ **MoussaNoussa** 2 years ago

option A is the right answer, we need a have a list of allowed tag values per OU
upvoted 1 times

✉️ **bhanus** 2 years 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** 1 year, 12 months 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

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.

Correct Answer: C*Community vote distribution*

C (88%)

12%

 **SK_Tyagi**  2 years, 4 months ago

Selected Answer: C

Option B is missing the Data Transformation to be done by Lambda
upvoted 8 times

 **softarts**  2 years, 4 months ago

Selected Answer: C

C, because it said new design and obviously IoT is what aws recommend.
upvoted 6 times

 **Soliner_Bilgi_Teknolojileri**  4 months, 2 weeks ago

Selected Answer: C

C is correct because using a managed, highly available AWS streaming service (such as Amazon MSK or Kinesis) removes the single point of failure from the on-premises Kafka server.
With MQTT data ingested directly into AWS IoT Core, then streamed to the managed service for transformation and stored in Amazon S3, the solution is multi-AZ, automatically scalable, and prevents data loss even if a broker or node fails.
upvoted 1 times

 **Linuslin** 1 year, 4 months ago

Must be C.
<https://aws.amazon.com/tw/blogs/iot/building-an-iot-solution-to-securely-transmit-mqtt-messages-under-private-networks/>
upvoted 1 times

 **8693a49** 1 year, 4 months ago

Selected Answer: C

Option B could also work. The key why it is not correct is because it says there is a single broker, so it will not be HA, therefore it won't prevent the crashing problem. So C is the correct option.
upvoted 1 times

 **tmlong18** 1 year, 11 months ago

Selected Answer: C

MSK can't transforms the data
upvoted 5 times

 **duriselvan** 2 years ago

b ANS
B. Amazon MSK with NLB:

Pros:
Highly available and managed Kafka service.

Scalable to accommodate increasing data volume.
NLB automatically distributes sensor data across healthy brokers.
Cons:
Requires migration from on-premises Kafka server.
Potential cost increase for managed service.

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C.

upvoted 1 times

 **duriselvan** 2 years, 3 months ago

C :Anshttps://docs.aws.amazon.com/lambda/latest/dg/services-kinesisfirehose.html

upvoted 2 times

 **chico2023** 2 years, 4 months 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 3 times

 **andy7t** 2 years, 5 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 2 times

 **Just_Ninja** 2 years, 5 months ago

Selected Answer: B

It's B,

because MSK can handle the lightweight MQTT protocol.

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

its a C

mqtt->IoT core

upvoted 1 times

 **javitech83** 2 years, 6 months ago

Selected Answer: C

IoT perfect for MQTT. Option D could have the same problem as on-premises

upvoted 2 times

 **SmileyCloud** 2 years, 6 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 3 times

 **bhanus** 2 years, 6 months ago

Selected Answer: C

MODERATOR - please remove my previous comment. Looks is C is correct answer

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: C

IOT core is designed to handle this. and NLB does not support MQTT.

upvoted 1 times

Question #238

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.

Correct Answer: ABD

Community vote distribution

ABD (100%)

 **bhanus** Highly Voted 2 years 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 8 times

 **TonytheTiger** Most Recent 1 year, 3 months ago

Selected Answer: ABD

AWS Backup Plan - <https://docs.aws.amazon.com/aws-backup/latest/devguide/about-backup-plans.html>

Backup Copy across AWS Regions - <https://docs.aws.amazon.com/aws-backup/latest/devguide/cross-region-backup.html>

Backup across AWS regions video - <https://www.youtube.com/watch?v=qMN18Lpj3PE>

upvoted 2 times

 **0dc6cac** 6 months, 2 weeks ago

Legend

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: ABD

Options A B D

upvoted 2 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: ABD

its ABD

upvoted 2 times

 **SkyZeroZx** 1 year, 12 months ago

Selected Answer: ABD

ABD. You don't need Lambda for cross-region backup. You don't need RDS snaps.

upvoted 2 times

SmileyCloud 2 years ago

Selected Answer: ABD

ABD. You don't need Lambda for cross-region backup. You don't need RDS snaps.

upvoted 4 times

easytoo 2 years ago

a-b-d...a-b-d

upvoted 1 times

MoussaNoussa 2 years ago

ABD is the correct answer

upvoted 2 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.

Correct Answer: B

Community vote distribution

B (95%) 5%

 **shaaam80** Highly Voted 2 years ago

Selected Answer: B

Answer B.

Option A might be close enough, near-real time, which is Firehose, but the target is RDS but the ask is for Datawarehouse (Redshift)
upvoted 8 times

 **Win007** Most Recent 1 year, 6 months ago

Dis the right Answer

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just B

upvoted 1 times

 **bjexamprep** 1 year, 8 months ago

Selected Answer: D

Kinesis client is a library. Users need to write an application with the Kinesis Client Library to use it.

Both A and B states “analyze the data with Kinesis clients” without mentioning how the application is written and deployed. So, both A and B are out, cause the deployment model is the key of the question to satisfy the requirement.

C has an incorrect statement “analyze the data from Amazon SQS with Kinesis”

D is a feasible solution.

upvoted 1 times

 **jopaca1216** 1 year, 5 months ago

SQS is not near real time

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just B

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: B

Correct answer is B.

upvoted 1 times

 **tmlong18** 1 year, 11 months ago

Selected Answer: B

'parallel'
upvoted 1 times

✉ **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B
upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B for sure
upvoted 1 times

✉ **SmileyCloud** 2 years, 6 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 4 times

✉ **easytoo** 2 years, 6 months ago

b=b=b=b=b=b
upvoted 1 times

✉ **nexus2020** 2 years, 6 months ago

Selected Answer: B

B is the one for real time
upvoted 1 times

✉ **MoussaNoussa** 2 years, 6 months ago

Answer B is the right one
upvoted 2 times

✉ **bhanus** 2 years, 6 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 years, 6 months 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** 2 years, 6 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 2 times

Question #240

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.

Correct Answer: BCE*Community vote distribution*

BCE (94%)

6%

✉  **shaaam80** Highly Voted 1 year ago

Selected Answer: BCE

not sure how these answers are generated, poor quality!

Correct answer - BCE

Hot standby, DynamoDB Global tables, Route53 failover routing policy.

upvoted 5 times

✉  **career360guru** Most Recent 1 year, 1 month ago

Selected Answer: BCE

B, C and E

upvoted 2 times

✉  **career360guru** 1 year, 1 month ago

Selected Answer: BCE

FDE is incorrect.

BCE are right options

upvoted 1 times

✉  **NikkyDicky** 1 year, 5 months ago

Selected Answer: BCE

BCE for sure

upvoted 2 times

✉  **Piccaso** 1 year, 5 months 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** 1 year, 5 months ago

Selected Answer: BCE

BCE is correct

upvoted 1 times

✉  **javitech83** 1 year, 6 months ago

Selected Answer: BCE

BCE is correct

upvoted 1 times

✉  **SmileyCloud** 1 year, 6 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** 1 year, 6 months ago

Sorry BCE.

upvoted 3 times

✉  **SkyZeroZx** 1 year, 6 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** 1 year, 6 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** 1 year, 6 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** 1 year, 6 months ago

Selected Answer: BCE

B, C and E

upvoted 1 times

✉  **PhuocT** 1 year, 6 months ago

B, C and E

upvoted 1 times

✉  **nexus2020** 1 year, 6 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** 1 year, 6 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.

Correct Answer: B

Community vote distribution

B (86%)

11%

 **career360guru** Highly Voted 2 years, 1 month ago

Selected Answer: B

Option B is correct. Feeltwise Option C requires edge agent to collect the data --> Higher operational overhead to migrate as this will need changes in customer application customer has today.

upvoted 9 times

 **SK_Tyagi** Highly Voted 2 years, 4 months 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 7 times

 **TonytheTiger** Most Recent 1 year, 8 months ago

Selected Answer: C

Option C: How To

<https://aws.amazon.com/blogs/iot/best-practices-for-ingesting-data-from-devices-using-aws-iot-core-and-or-amazon-kinesis/>
upvoted 1 times

 **TonytheTiger** 1 year, 8 months ago

Sorry " Option B NOT C "

upvoted 1 times

 **sunny** 1 year, 11 months ago

Selected Answer: C

ans is C

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just B

upvoted 2 times

 **learnwithaniket** 1 year, 11 months ago

Selected Answer: D

Answer is D.

AWS Lookout - Automatically detect anomalies within metrics and identify their root causes.

<https://aws.amazon.com/lookout-for-metrics/>

upvoted 1 times

 **Jay_2pt0_1** 2 years ago

Agree with @duriselvan - Fleetwise is made for this and Glue has machine learning modules

upvoted 1 times

 **duriSelvan** 2 years ago

C ans :-

AWS IoT FleetWise: This managed service simplifies vehicle data collection and management, reducing operational overhead compared to other options.

Kinesis data stream: This serverless stream allows processing data in real-time, eliminating the need for custom code.

Kinesis Data Firehose: This service automatically stores data in S3, reducing manual intervention.

Glue machine learning transforms: These built-in features enable anomaly detection directly within Glue, eliminating the need for separate ML models and infrastructure

upvoted 3 times

 **shaaam80** 2 years ago

Selected Answer: B

Answer B. Straightforward

C might sound like a good option with Fleetwise, but Glue for anomaly detection?? Also talks about Kinesis integration with Fleetwise not sure.

Fleetwise also needs an Edge agent to communicate with AWS IoT Fleetwise

upvoted 6 times

 **yorkicurke** 2 years, 1 month ago

Selected Answer: B

its a B...oye! :)

upvoted 2 times

 **totten** 2 years, 2 months ago

Selected Answer: B

Here's why option B is the best choice:

Simplicity: This solution leverages AWS IoT Core and Amazon Kinesis Data Firehose, which are fully managed services, making it a simple and low-overhead option.

Real-time Data Streaming: AWS IoT Core efficiently receives the vehicle data using the MQTT protocol, and Kinesis Data Firehose streams the data to Amazon S3. This supports data streaming in real-time.

Easy Anomaly Detection: Amazon Kinesis Data Analytics can easily be set up to process the streaming data in real-time to detect anomalies.

Scalability: This architecture is designed to handle a growing number of vehicles and high data volumes, ensuring scalability without operational overhead.

Data Storage: Data is reliably stored in Amazon S3, eliminating concerns about on-premises storage limitations.

upvoted 3 times

 **chico2023** 2 years, 4 months ago

Selected Answer: B

I agree with everyone. Even olabiba agrees. It's B.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

it's a B

C - there is no Fleetwise to Kinesis integration

upvoted 2 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: B

A - too complex

B - It's B. You use IoT Core, 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** 2 years, 6 months ago

C-C-C-C-C-C

upvoted 1 times

 **SkyZeroZx** 2 years, 6 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** 2 years, 6 months ago

Selected Answer: B

Olabiba says 'B'.
upvoted 1 times

 **gd1** 2 years, 6 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

Question #242

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.

Correct Answer: D

Community vote distribution

D (94%)	6%
---------	----

 **SmileyCloud**  2 years 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 15 times

 **yuliaqwerty**  1 year, 6 months ago

D <https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/>
 upvoted 1 times

 **Pupu86** 1 year, 7 months ago

Using lambda to trigger a scan is retrospectively ineffective as Azure can do so with DevOps Organization advanced security (which does code scanning) and provide you an option to remediate if targets are found.
 upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: D
 D is right option.
 upvoted 1 times

 **joleneinthebackyard** 1 year, 8 months ago

Selected Answer: D
 Macie only does S3 -> C is out
 Scheduled or nightly script will only detect the problem after a while so damage might has already done --> A, B is out
 Plus KMS doesn't do secrets
 D looks valid technically
 upvoted 2 times

 **ggrodsckiy** 1 year, 11 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/macie/latest/user/what-is-macie.html>: <https://docs.aws.amazon.com/codecommit/latest/userguide/data-protection.html> <https://aws.amazon.com/blogs/aws/category/amazon-macie/>: <https://aws.amazon.com/blogs/aws/category/amazon-macie/>
 upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: D

D - <https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/>
upvoted 2 times

□ **River007** 2 years ago

D can resolve the code that already commit to codecommit
upvoted 1 times

□ **RockyLeon** 1 year, 12 months ago

D says Codecommit trigger to scan new code submissions....
how already commit code will scan ?
upvoted 1 times

□ **RockyLeon** 1 year, 12 months ago

whereas question did not ask for existing code
upvoted 1 times

□ **SkyZeroZx** 2 years 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** 2 years 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 2 times

□ **gd1** 2 years ago

Selected Answer: D

Need auto-disable and D does it
upvoted 1 times

□ **Alabi** 2 years 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** 2 years 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 submission.

only D would prevent it from happening by doing a check BEFORE it get submitted.

upvoted 4 times

□ **MoussaNoussa** 2 years ago

option D is the correct one of course
upvoted 3 times

□ **bhanus** 2 years 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** 1 year, 12 months ago

change it to D as it would prevent it from happening by doing a check BEFORE it get submitted.
upvoted 1 times

Question #243

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.

Correct Answer: AC*Community vote distribution*

AC (72%)	AB (17%)	6%
----------	----------	----

 **joleneinthebackyard**  2 years, 1 month ago

Selected Answer: AC

For those who struggle on why A but not D as they are almost identical like I did:
 A: Create an S3 access point for each application in THE AWS account
 D: Create an S3 access point for each application in EACH AWS account

Not sure if this is technical or English exam.

upvoted 20 times

 **a54b16f** 1 year, 10 months ago

A: in the AWS account that owns the S3 bucket

upvoted 1 times

 **vip2**  1 year, 5 months ago

Selected Answer: AC

see details step in below link where 'Create an Amazon S3 gateway endpoint in your VPC'

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 4 times

 **sse69** 1 year, 7 months ago

Selected Answer: AC

<https://repost.aws/knowledge-center/s3-access-bucket-restricted-to-vpc>

upvoted 2 times

 **fartosh** 1 year, 7 months ago

The linked post describes the scenario of creating an S3 access point in the data lake account (answer A) and a gateway VPC endpoint in the application's account (answer C).

upvoted 2 times

 **red_panda** 1 year, 7 months ago

Selected Answer: AC

A and C in my opinion. Interface Endpoint is for EC2 generally, when we need a private IP. Gateway Endpoint is suitable in 95% cases when there are DynamoDB and S3 secure connectivity.

upvoted 1 times

 **BrijMohan08** 1 year, 8 months ago

Selected Answer: AC

A & C

Why not B?

Interface endpoints are used for services that require a private IP address within the VPC, such as Amazon EC2, Amazon ECS, or Amazon SNS.

Gateway endpoints, on the other hand, are used for services that are accessed using their public endpoint, such as Amazon S3 and Amazon DynamoDB.

Since the scenario involves accessing an S3 bucket, a gateway endpoint is the appropriate choice, not an interface endpoint.

upvoted 2 times

 trap 1 year, 8 months ago

Correct:A,B

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 1 times

 VerRi 1 year, 9 months ago**Selected Answer: AB**

Gateway Endpoint only allows resources within the VPC to connect to S3.

It is not possible to provide the gateway endpoint across many AWS accounts

upvoted 2 times

 kz407 1 year, 9 months ago**Selected Answer: AB**I don't think C can achieve the requirement. At least according to this <https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>. Here's why.

"100's of AWS Accounts" hints about possibility of cross region access. Gateway Endpoints can't allow access from VPCs in other regions. Gateway endpoint is to access from own VPC.

upvoted 2 times

 Dgix 1 year, 9 months ago**Selected Answer: AB**

It's A+B. A sets up S3 Access Points, one for each accessing application, in the data lake account (the S3 account) which are configured with policies giving each application least-privilege access. B then sets up PrivateLink access (==interface endpoints) in each of the application accounts.

C is out because gateway endpoints can't take policies.

D is less efficient than A+B

E is too simplistic - one gateway endpoint is not enough..

upvoted 3 times

 Dgix 1 year, 9 months ago**Selected Answer: AB**

A is valid, but C can't be configured for fine-grained access since it involves a gateway endpoint. Therefore: B as this is possible with a PrivateLink (==interface endpoint)

upvoted 1 times

 blackgamer 2 years ago

Answer is A & B.

C is not suitable based on AWS Gateway endpoints documentation -

"Endpoint connections cannot be extended out of a VPC. Resources on the other side of a VPN connection, VPC peering connection, transit gateway, or AWS Direct Connect connection in your VPC cannot use a gateway endpoint to communicate with Amazon S3."

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

upvoted 3 times

 zhooon 1 year, 10 months agoWith a gateway endpoint, you can access Amazon S3 from your VPC (<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>)

upvoted 1 times

 career360guru 2 years, 1 month ago**Selected Answer: AC**

A & C are right.

upvoted 1 times

 Sab 2 years, 1 month ago**Selected Answer: AC**<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 3 times

 Mehrannn 1 year, 11 months ago

considering this blog post, do you agree with A&B or A&C?

upvoted 2 times

✉ KCjoe 2 years, 2 months ago

Selected Answer: AB

Answer is AB, because gateway VPC does not have access to S3 access point.

And interface VPC endpoint allows access to S3 access point.

Note from ChatGPT:

As of my last knowledge update in September 2021, Gateway VPC Endpoints for Amazon S3 do not support direct access to S3 access points. Gateway VPC Endpoints are designed to provide private connectivity from your Amazon Virtual Private Cloud (VPC) to S3, but they do not inherently support access to S3 access points.

upvoted 2 times

✉ totten 2 years, 2 months ago

Selected Answer: AC

A. By creating an S3 access point for each application in the AWS account that owns the S3 bucket and configuring it to be accessible only from the application's VPC, you ensure that each application has the minimum necessary permissions and can access the data lake securely.

C. Creating a gateway endpoint for Amazon S3 in each application's VPC and configuring the endpoint policy to allow access to an S3 access point ensures that traffic from each VPC is directed through the S3 access point and adheres to the security requirements. Specifying the route table that is used to access the access point is an essential part of the configuration.

This combination of steps helps you meet your security and access requirements by using S3 access points and VPC endpoints for each application. It ensures that the data lake is accessed securely and that access permissions are correctly configured.

upvoted 1 times

✉ Gabehcoud 2 years, 3 months 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 2 years, 4 months 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 2 years, 3 months ago

interface endpoint is completely private, you are wrong interface endpoint is public

upvoted 1 times

✉ vn_thanh tung 2 years, 3 months 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 years, 3 months ago

thanks, got it

upvoted 1 times

Question #244

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.

Correct Answer: B

Community vote distribution

B (100%)

 **bhanus** Highly Voted 2 years 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 17 times

 **adelynlllllllll** Most Recent 1 year, 5 months ago

B:

Why do they answer the solution backwards. it does no follow the workflow, it is hard to put the picture together. but , anyway.

upvoted 4 times

 **career360guru** 1 year, 7 months ago

Selected Answer: B

B is right answer as KDF supports Splunk integration.

upvoted 1 times

 **career360guru** 1 year, 7 months ago

and Requirement is Near Real time.

upvoted 1 times

 **joleneinthebackyard** 1 year, 8 months ago

Selected Answer: B

Monitoring solution -> VPC flow logs

Near real time analysis -> Firehose

Firehose also can have spunk as destination -> eye on B

A: giving access key normally a secondary considered option

C: too complex to get logs while we have vpc flow logs

D: same

upvoted 3 times

✉  **ggrodskiy** 1 year, 11 months ago

correct B.

upvoted 1 times

✉  **NikkyDicky** 1 year, 11 months ago

Selected Answer: B

its a B

upvoted 1 times

✉  **Christina666** 1 year, 11 months 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** 1 year, 12 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 2 times

✉  **SmileyCloud** 2 years 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** 2 years ago

Selected Answer: B

B is answer, I think

upvoted 1 times

✉  **ozelllll** 2 years ago

Selected Answer: B

B. <https://docs.aws.amazon.com/firehose/latest/dev/vpc-splunk-tutorial.html>

upvoted 2 times

✉  **gd1** 2 years 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 4 times

Question #245

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.

Correct Answer: BDE*Community vote distribution*

BDE (86%)

10%

 **SmileyCloud**  2 years 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 9 times

 **Arnaud92** 1 year, 10 months 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 2 times

 **SkyZeroZx**  1 year, 11 months ago

Selected Answer: BDE

- Remember SCP Only deny not allow (in definition)
 upvoted 8 times

 **Soliner_Bilgi_Teknolojileri**  4 months, 1 week ago

Selected Answer: BDE

- A. CUR to S3: Adds extra complexity. Finance can already view consolidated costs directly in the management account via Cost Explorer. Not needed.
 C. SCP with "allow only US regions": SCPs work on explicit deny, not allow lists. Deny is the right approach.
 F. IAM role in each account: Operationally heavy (25+ accounts to manage). Centralized role in management account (E) is much more efficient.
 upvoted 1 times

 **red_panda** 1 year, 1 month ago

Selected Answer: BDE

Answer is BDE without any doubt!

upvoted 2 times

 **Wardove** 1 year, 4 months ago

Selected Answer: BDE

Not C because there is no word about default SCP removal.

FullAWSAccess - without an explicit deny SCP would not suffice the requirement

upvoted 3 times

 **veyisceylan** 1 year, 4 months ago

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

Notes

An Allow statement in an SCP permits the Resource element to only have a "*" entry.

An Allow statement in an SCP can't have a Condition element at all.

Therefore Option C is not possible

upvoted 1 times

 **GoKhe** 1 year, 6 months ago

BCE and it aligns with what ChatGpt thinks

upvoted 1 times

 **duriselvan** 1 year, 6 months ago

ABD -ANS

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.

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 2 times

 **shaaam80** 1 year, 7 months ago

Selected Answer: BDE

Answer - BDE

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: BDE

Explicit Deny is more strict than Explicit Allow - As member account can add allow creation of resources in other regions.

upvoted 6 times

 **NikkyDicky** 1 year, 11 months 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

 **Tofu13** 1 year, 7 months ago

Not exactly overwritten. If you allow the creation in certain regions in the SCP, all member accounts are allowed to create instances in the region. But each member account can add IAM policies to allow to create them in different regions as well, unless there is an explicit deny. Therefore only D works.

upvoted 2 times

 **Christina666** 1 year, 11 months 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** 1 year, 12 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 1 times

 **javitech83** 1 year, 12 months ago

Selected Answer: BDE

correct answer is BDE

upvoted 1 times

✉️  **easytoo** 2 years ago

b-c-e...b-c-e

upvoted 1 times

✉️  **nexus2020** 2 years 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** 2 years ago

B, D an E

upvoted 1 times

Question #246

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.

Correct Answer: B

Community vote distribution

B (100%)

 **bhanus**  2 years, 6 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 7 times

 **Christina666**  2 years, 5 months 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 5 times

 **albert_kuo**  9 months, 3 weeks ago

Selected Answer: B

D is incorrect. OrganizationAccountAccessRole will have AdministratorAccess privilege.
 upvoted 1 times

 **duriselvan** 2 years ago

D Ans
 D. STS AssumeRole with OrganizationAccountAccessRole in Member Account:

Pros:

Follows best practices for cross-account access using temporary credentials.
 Minimizes complexity by leveraging the pre-existing OrganizationAccountAccessRole.

Cons:

Security team needs access to each member account to assume the role.
 Therefore, option D, using AWS STS to call the AssumeRole API for the OrganizationAccountAccessRole in each member account from the security account, is the most secure and efficient solution. This approach leverages existing IAM roles, minimizes configuration overhead, and adheres to best practices for cross-account access using temporary credentials.

upvoted 1 times

 **0c118eb** 2 years ago

OrganizationAccountAccessRole by default has AdministratorAccess IAM policy attached. The security team should only get Read Only.
 Best practice for accounts within an organization is B.
 upvoted 3 times

 **helloworldabc** 1 year, 4 months ago

just B

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B

upvoted 1 times

 **ggrodsckiy** 2 years, 5 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

its a b

upvoted 2 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: B

B - You need a role.

upvoted 1 times

 **easytoo** 2 years, 6 months ago

b-b-b-b-b-b-b

upvoted 1 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: B

B is classic usage of Cross Account Role

upvoted 1 times

 **Jackhemo** 2 years, 6 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 2 times

 **PhuocT** 2 years, 6 months ago

B is the answer

upvoted 1 times

 **gd1** 2 years, 6 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** 2 years, 6 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

Question #247

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.

Correct Answer: B*Community vote distribution*

B (90%) 10%

 **Christina666**  2 years, 5 months ago

Selected Answer: B

hundreds of VPCs-> TGW
then we only have B and C
C: create TGW in each account, wrong
upvoted 5 times

 **sergza888**  9 months, 4 weeks ago

Selected Answer: A

there are a lot of unknowns (IS there AWS organization so we can use Ram to share TGW or if these VPC's are in the same region). If we think about sharing there are supposed be AWS organizations and RAM
upvoted 1 times

 **mns0173** 1 year, 7 months ago

With hundreds of VPCs you will inevitably face CIDR overlapping conflict so better to use Transit Gateway
upvoted 1 times

 **teo2157** 1 year, 7 months ago

Selected Answer: A

There's a key information that is not mentioned in the question, if the VPCs are in the same region or in different regions, as we're talking of hundreds of AWS accounts the answer will be VPC peering as a single transit gateway doesn't support different regions so A. If all VPCs are in the same region, the answer would be transit gateway so B. Saying that I go for A
upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just B
upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B
upvoted 1 times

 **joleneinthebackyard** 2 years, 1 month ago

Selected Answer: B

"hundreds of AWS account" - think of transit gateway, VPC peering, PrivateLink should be out
option C: add transit gateway to each account -> out
upvoted 4 times

 **ggrodsckiy** 2 years, 5 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

b for sure

upvoted 1 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: B

B - Hub and spoke is based on transit GW

upvoted 2 times

 **easytoo** 2 years, 6 months ago

b-b-b-b-b-b-b

upvoted 2 times

 **PhuocT** 2 years, 6 months ago

yep, it's B

upvoted 1 times

 **Alabi** 2 years, 6 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 3 times

 **gd1** 2 years, 6 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** 2 years, 6 months ago

B is correct because we have hundreds of vpcs and default quota for peering peer vpc is = 50

upvoted 1 times

 **bhanus** 2 years, 6 months ago

Selected Answer: B

SHould be B

upvoted 1 times

Question #248

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.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

Option B provides the most operational efficiency to prevent the weekly spike in failed login attempts. Here's why:

AWS WAF (Web Application Firewall) with a rate-based rule allows you to monitor and block traffic based on the rate of requests from different IP addresses.

The rate-based rule can help identify and block the excessive login attempts originating from a large number of IP addresses that change weekly.

By blocking traffic at the ALB level using AWS WAF, the traffic doesn't reach the application, reducing the load on your authentication service.

The rate-based rule can automatically adjust to changing patterns of attack without manual updates, providing an efficient solution. AWS WAF is designed for web application protection and allows you to create flexible rules to mitigate various types of attacks, making it a suitable choice for handling this scenario.

upvoted 7 times

 **85b5b55** Most Recent 7 months, 1 week ago

Selected Answer: B

IP rate-based Rule.

upvoted 1 times

 **career360guru** 1 year, 1 month ago

Selected Answer: B

Using WAF with ALB is most operationally efficient. This narrows the choices down to B and D. As IP address keeps changing B is most efficient.

upvoted 3 times

 **joleneinthebackyard** 1 year, 1 month ago

Selected Answer: B

The application should be used by users "around the world" so policies that IP based are not suitable, as you have to update set of new IPs each week.

Option B has valid actions, as WAF webACL has rate-based rule and Block Action.

upvoted 2 times

 **ggrodsckiy** 1 year, 5 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: B

easyu B

upvoted 1 times

 **Christina666** 1 year, 5 months ago

Selected Answer: B

B, if login hit at a certain ratio, block this IP

upvoted 1 times

 **SkyZeroZx** 1 year, 5 months ago

Selected Answer: B

B and not D because of "500 different IP addresses that change each week"

upvoted 2 times

 **SmileyCloud** 1 year, 6 months ago

Selected Answer: B

B and not D because of "500 different IP addresses that change each week"

upvoted 3 times

 **easytoo** 1 year, 6 months ago

b-b-b-b-b-b

upvoted 1 times

 **PhuocT** 1 year, 6 months ago

yep, it's B

upvoted 1 times

 **elanelans** 1 year, 6 months ago

Selected Answer: B

B Is Correct.

Since IP address keeps changing, WAF can't block on IP/CIDR.

upvoted 2 times

 **bhanus** 1 year, 6 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.

Correct Answer: A*Community vote distribution*

A (100%)

 **0b43291** 1 year, 1 month ago

Selected Answer: A

Register the customer-owned block of IP addresses in the company's AWS account: This allows the company to use their existing IP addresses within AWS, ensuring customers don't need to update firewall allow lists.

Create Elastic IP addresses from the address pool: Elastic IP addresses are static IPv4 addresses for dynamic cloud computing. Creating them from the customer-owned pool allows assigning these IP addresses to AWS resources.

Assign the Elastic IP addresses to an AWS Transfer for SFTP endpoint: AWS Transfer for SFTP enables secure SFTP file transfers. Assigning customer-owned Elastic IP addresses to the endpoint maintains existing IP addresses for customers.

Use AWS Transfer to store files in Amazon S3: AWS Transfer for SFTP integrates with Amazon S3, allowing ingested files to be stored directly in S3 buckets, eliminating the need to manage file storage infrastructure and reducing operational overhead.

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

Option A is the only possible option.

upvoted 2 times

 **joleneinthebackyard** 2 years, 1 month ago

Selected Answer: A

Option A is valid

Option D: S3 doesn't have support for SFTP option -> out

B, C: using EC2 to host FTP (not SFTP) while there is a native solution in option A -> out

upvoted 2 times

 **Simon523** 2 years, 4 months ago

Selected Answer: A

should use AWS Transfer for SFTP

upvoted 4 times

 **breadops** 2 years, 5 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/storage/use-ip-whitelisting-to-secure-your-aws-transfer-for-sftp-servers/>

upvoted 2 times

 **ggrodsckiy** 2 years, 5 months ago

Correct A.

upvoted 1 times

 **nicecurls** 2 years, 5 months ago

Selected Answer: A

it's A

upvoted 1 times

 **Piccaso** 2 years, 5 months ago

Selected Answer: A

D is too manual

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

its an A

upvoted 1 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: A

A - AWS Managed SFTP

upvoted 2 times

 **nexus2020** 2 years, 6 months ago

Selected Answer: A

AWS Transfer for SFTP, fully managed service, no operational overhead

upvoted 2 times

 **Alabi** 2 years, 6 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** 2 years, 6 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 2 times

 **MoussaNoussa** 2 years, 6 months ago

A is the right answer

upvoted 1 times

Question #250

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.

Correct Answer: A

Community vote distribution

A (100%)

 **Malluchan** 2 months, 3 weeks ago

Selected Answer: A

Cluster = Speed (low latency, high throughput)
Partition = Scale (big data, fault isolation across partitions)
Spread = Safety (max fault tolerance, small # of critical nodes)
upvoted 2 times

 **bhanus** 1 year ago

Selected Answer: A

Cluster that would place them in same Az.
upvoted 1 times

 **43c89f4** 1 year, 1 month ago

typical cluster placement group use case
upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: A

A is the only option.
upvoted 4 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: A

easy A
upvoted 1 times

 **SmileyCloud** 2 years ago

Selected Answer: A

A - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>
upvoted 4 times

 **Alabi** 2 years ago

Selected Answer: A

A for sure
upvoted 1 times

 **gd1** 2 years 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 2 times

 **elanelans** 2 years 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** 2 years 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 4 times

Question #251

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.

Correct Answer: D

Community vote distribution

D (97%)

✉  **shree2023**  2 years 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 15 times

✉  **kejam**  1 year, 5 months ago

Selected Answer: D

Answer D
<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-aws-waf.html>

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

✉  **duriselvan** 1 year, 6 months ago

c ANS
 C. WAF with IP Filtering and Resource Policy:

Pros:
 Simple and cost-effective solution.
 WAF rules and resource policy restrict access.
 Cons:
 IP filtering might not be effective if partners use dynamic IP addresses.
 Resource policy request limit applies to all methods, not just POST.
 upvoted 1 times

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

Selected Answer: D

Option D
 upvoted 1 times

✉  **xav1er** 1 year, 10 months 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

 **grodskiy** 1 year, 11 months ago

Correct D.

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: D

D fits

upvoted 1 times

 **Christina666** 1 year, 11 months 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** 2 years 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 3 times

 **easystoo** 2 years ago

d-d-d-d-d-d

upvoted 1 times

 **SkyZeroZx** 2 years 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** 2 years 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

 **Alabi** 2 years 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** 2 years 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 2 times

Question #252

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.

Correct Answer: C

Community vote distribution

C (100%)

 **elanelans** Highly Voted 2 years, 6 months ago

Selected Answer: C

C achieves the Goal.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

upvoted 7 times

 **aka1177** Most Recent 1 month ago

Selected Answer: C

recommended architecture:

Aurora PostgreSQL

↓

Activity Streams (DAS)

↓

Amazon Kinesis Data Streams

↓

Kinesis Data Firehose → S3 / Splunk / OpenSearch / SIEM

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: C

For those who think the correct option is B: "The Aurora DB cluster sends activities to an Amazon Kinesis data stream in near real time." It does NOT send to EventBridge.

https://docs.aws.amazon.com/pt_br/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.html

upvoted 1 times

 **thotwielder** 1 year, 11 months ago

C seems correct. but why not B?

upvoted 1 times

 **duriselvan** 2 years ago

B is ans :

Here's why this solution is the most suitable:

Direct integration: Database activity streams natively integrate with EventBridge, streamlining the process of capturing and routing events.

Rich event filtering: EventBridge offers powerful filtering capabilities, allowing the database team to selectively monitor specific events or patterns of interest.

Flexible delivery: EventBridge can trigger various targets, including Lambda functions, which provide the ability to process and store events in S3 for further analysis.

Serverless architecture: Lambda functions eliminate the need to manage servers, reducing operational overhead and scaling automatically to handle event volume.

Cost-effective storage: S3 offers durable and cost-effective storage for long-term analysis of database activity logs.

upvoted 2 times

 **helloworldabc** 1 year, 4 months ago

just C

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C

upvoted 1 times

 **ggrodsckiy** 2 years, 5 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

its a C

upvoted 1 times

 **SmileyCloud** 2 years, 6 months ago

C - Correct. <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

upvoted 2 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: C

C achieves the Goal.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

upvoted 1 times

 **shree2023** 2 years, 6 months ago

Selected Answer: C

C indeed

upvoted 1 times

 **gd1** 2 years, 6 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 4 times

 **MoussaNoussa** 2 years, 6 months ago

C is the right answer

upvoted 1 times

 **bhanus** 2 years, 6 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.

Correct Answer: C

Community vote distribution

C (97%)

 **bhanus** Highly Voted 2 years, 6 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 11 times

 **nexus2020** Highly Voted 2 years, 6 months ago

Selected Answer: C

16large = 64CPU,
4Large = 16 CPU
8Large = 32 CPU
 $\frac{1}{4}$ usage of 64 = 16CPU
 $\frac{1}{4}$ of 12 EC2 = 3 instance, so C is a better choice.

upvoted 8 times

 **rajkanch** Most Recent 1 year, 11 months ago

In regards with Efficiency vs. Headroom: I would choose D over C because there will be less headroom during peak loads.

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just C

upvoted 1 times

 **duriselvan** 2 years ago

SORRY c ANS
r6g.8xlarge

Upfront cost
0.00 USD
Monthly cost
1,248.01 USD
Total 12 months cost
14,976.12 USD

r6g.4xlarge

624.00 USD

Total 12 months cost

7,488.00 USD

<https://calculator.aws/#/estimate>

upvoted 1 times

✉ **duriselvan** 2 years ago

I would suggest that option B is the most cost-effective solution that meets the requirements. It uses m6g.4xlarge instances, which are general purpose instances powered by Arm-based AWS Graviton2 processors. These instances offer a balance of compute, memory, and networking resources, and deliver up to 40% better price performance than comparable current generation x86-based instances⁵. This option can also reduce the number of instances needed to meet the demand, as each m6g.4xlarge instance has 16 vCPUs and 64 GiB of memory, which is equivalent to one quarter of the resources of an r6g.16xlarge instance. This option can also leverage the existing Network Load Balancer and CloudWatch metrics to monitor and distribute the traffic across the instances.

upvoted 2 times

✉ **duriselvan** 2 years ago

Option D, using r6g.8xlarge instances with a minimum capacity of 2, a desired capacity of 2, and a maximum capacity of 6, is the most cost-effective solution for this scenario. Here's why:

Cost reduction: Lower instance size and smaller fleet size significantly reduce cost compared to the current configuration.

Balanced memory and cost: R6g.8xlarge still provides sufficient memory for current demand while being cheaper than r6g.16xlarge.

Scalability for peak demand: Doubling the capacity up to 6 instances can cater to potential player spikes while remaining within a controlled budget.

upvoted 1 times

✉ **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C

upvoted 1 times

✉ **severlight** 2 years, 1 month ago

Selected Answer: C

see Maria2023's answer

upvoted 1 times

✉ **chico2023** 2 years, 4 months 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 years, 5 months ago

Correct C.

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C I guess. weird question

upvoted 1 times

✉ **SmileyCloud** 2 years, 6 months ago

Selected Answer: C

C makes most sense.

upvoted 1 times

✉ **Maria2023** 2 years, 6 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 4 times

✉ **LuongTo** 1 year ago

but the auto scaling group have to maintain maximum capability to meet the current setup = ¼ of (12 * r6g.16xlarge) = (3 * r6g.16xlarge) or (12 * r6g.4xlarge). Does comparison on "non-peak" make any sense?

upvoted 1 times

✉ **shree2023** 2 years, 6 months ago

Selected Answer: C

Memory optimized and cost optimized
upvoted 1 times

Alabi 2 years, 6 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 2 years, 6 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

✉ **Just_Ninja** 2 years, 5 months ago

I now switch to D, because it's an expedited workload.
upvoted 1 times

✉ **rxhan** 2 years, 5 months ago

looool
upvoted 2 times

✉ **ggrodsckiy** 2 years, 5 months ago

Correct D.
upvoted 1 times

✉ **achillesatan** 2 years, 5 months 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** 2 years, 5 months ago

what about caching?
upvoted 1 times

✉ **goodard** 1 year, 5 months ago

Saving plans are not applicable to dynamodb. <https://aws.amazon.com/savingsplans/>
upvoted 1 times

✉ **rrrrrrrr1** 2 years, 5 months ago

Isn't DAX extremely expensive? Weird question.
upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: D
its a D
upvoted 1 times

✉ **Christina666** 2 years, 5 months ago

Selected Answer: D
DAX + Provision Capacity + Auto Scaling meets the need
upvoted 1 times

✉ **SmileyCloud** 2 years, 6 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 4 times

✉ **nexus2020** 2 years, 6 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** 2 years, 6 months ago

Selected Answer: D
DAX + Provision Capacity + Auto Scaling meets the need
upvoted 2 times

✉ **gd1** 2 years, 6 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** 2 years, 6 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/80440-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 2 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.

Correct Answer: AC

Community vote distribution

AC (61%)	BD (19%)	7%	7%
----------	----------	----	----

 **magmichal05** Highly Voted 1 year, 8 months ago

Selected Answer: AC

When you associate a Network Load Balancer with an endpoint service, the Network Load Balancer forwards requests to the registered target. The requests are forwarded as if the target was registered by IP address. In this case, the source IP addresses are the private IP addresses of the load balancer nodes. If you have access to the Amazon VPC endpoint service, then verify that:

The Inbound security group rules of the Network Load Balancer's targets allow communication from the private IP address of the Network Load Balancer nodes

The rules within the network ACL associated with the Network Load Balancer's targets allow communication from the private IP address of the Network Load Balancer nodes

<https://repost.aws/knowledge-center/security-network-acl-vpc-endpoint>

upvoted 14 times

 **red_panda** Highly Voted 1 year, 1 month ago

Selected Answer: AC

A and C.

The flow is:

Application -> NLB -> Logging Monitor Tool.

So we need to check NACL of NLB subnets (in and out from applications client and in and out to EC2 subnet) and Security group (Statefull, so only ingress) of EC2 Instances of Logging Monitor Tool.

upvoted 6 times

 **Blair77** Most Recent 2 months, 3 weeks ago

Selected Answer: DE

After analyzing the question carefully and considering recent AWS updates (especially the support for security groups on Network Load Balancers (NLBs) introduced in August 2023), the best answer combination is:

- D. Check the security group for the 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.

upvoted 1 times

 **loreant** 6 months, 2 weeks ago

Selected Answer: BC

Option A is incorrect because it focuses on communication between the NLB subnets and the logging service subnets, which is not the primary path for PrivateLink traffic.

upvoted 1 times

 **Longc** 8 months, 3 weeks ago

Selected Answer: CE

To resolve connectivity issues between clients using VPC endpoints and the logging service:

NLB Security Group (Option E):

The NLB must allow traffic from the subnets where the client's interface endpoints reside. Since clients connect via PrivateLink, the NLB's security group must permit ingress from the CIDR blocks of the client's interface endpoint subnets.

EC2 Security Group (Option C):

The EC2 instances hosting the logging service must allow traffic from the NLB's subnets. The NLB forwards traffic to the EC2 instances, and their security group must permit ingress from the NLB's subnet CIDRs (or the NLB's security group).

upvoted 2 times

 **esa** 9 months, 2 weeks ago

Selected Answer: BE

B.- Network ACLs operate at the subnet level and could be blocking traffic between:

The interface endpoints (created in each AWS account) and the logging service's subnets.

The logging service subnets and the interface endpoint subnets.

AWS PrivateLink uses interface endpoints, and the NACL must allow inbound/outbound traffic between the interface endpoint subnets and the EC2 instances running the logging service.

E.-The interface endpoint in each AWS account connects to the NLB.

If the NLB security group does not allow ingress from the interface endpoint subnets, traffic from the clients will be dropped.

upvoted 1 times

 **titi_r** 1 year, 1 month ago

Selected Answer: AC

A and C.

<https://repost.aws/knowledge-center/security-network-acl-vpc-endpoint>

upvoted 2 times

 **BrijMohan08** 1 year, 1 month ago

Selected Answer: BD

B. Network Access Control Lists (NACLs) act as a firewall at the subnet level. To ensure communication between the interface endpoint subnets and the logging service subnets running on EC2 instances, the NACLs attached to both subnets should be configured to allow the necessary traffic.

D. Security groups act as virtual firewalls at the instance level. To allow clients to submit logs to the logging service running on EC2 instances, the security group associated with the EC2 instances should be configured to allow ingress traffic from the clients' IP addresses or security groups.

upvoted 2 times

 **altonh** 10 months ago

The EC2 will not receive the interface endpoint IP but the NLB's IP instead.

upvoted 1 times

 **chelbsik** 1 year, 4 months ago

Selected Answer: CE

CE: we only need to allow access from client -> NLB -> application

upvoted 3 times

 **Mehrannn** 1 year, 5 months ago

Selected Answer: BD

B&D are correct answers. Rational:

EC2s and NLB are both in one subnet, so the NACL is associated with one subnet and there is no NACL which controls EC2 and NLB communication --> A is not Valid, C is not Valid.

Security groups are attached to EC2s --> E is not Valid

upvoted 1 times

 **7f6aef3** 1 year, 1 month ago

The logging service running on EC2 instances with a Network Load Balancer (NLB) are deployed in different subnets.

upvoted 1 times

 **duriselvan** 1 year, 6 months ago

guys .pls B,E ans

e:-

The Inbound security group rules of the Network Load Balancer's targets allow communication from the private IP address of the Network Load Balancer nodes

upvoted 1 times

 **duriselvan** 1 year, 6 months ago

CE is ans

The clients are trying to connect to the logging service through the NLB.

The NLB needs to forward the requests to the EC2 instances running the logging service.

Therefore, both the NLB and the EC2 instances need to have security group rules allowing inbound traffic from each other's subnets.

upvoted 2 times

 **ayadmawla** 1 year, 6 months ago

Selected Answer: AC

Link below seems to confirm it. The focus is on the Provider VPC so the question wasn't really that clear.

<https://repost.aws/knowledge-center/security-network-acl-vpc-endpoint>

upvoted 3 times

 **career360guru** 1 year, 7 months ago

Selected Answer: AC

A and C

upvoted 1 times

 **severlight** 1 year, 7 months ago

Selected Answer: AC

see magmichal05's answer

upvoted 1 times

 **dpatra** 1 year, 8 months ago

Selected Answer: BE

B is pretty clear plus E is valid as well since AWS has introduced support for associating security groups with Network Load Balancers (NLBs).

upvoted 1 times

 **Certified101** 1 year, 8 months ago

Selected Answer: AC

AC - NLB needs to be allowed to the instances otherwise targets are unhealthy

upvoted 1 times

Question #256

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.

Correct Answer: B

Community vote distribution

B (100%)

 **gd1** [Highly Voted] 2 years 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 15 times

 **Oznerol96_** [Most Recent] 1 year, 3 months ago

Selected Answer: B

100% B

upvoted 1 times

 **GoKhe** 1 year, 6 months ago

Bucket key would have been an option here but it is not in the answers.

upvoted 4 times

 **career360guru** 1 year, 7 months ago

Selected Answer: B

Option B

upvoted 1 times

 **shizhan** 1 year, 10 months 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 2 times

 **Just_Ninja** 1 year, 11 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 2 times

 **ggrodschi** 1 year, 11 months ago

Correct B.

upvoted 2 times

 **nicecurls** 1 year, 11 months ago

Selected Answer: B

this is B

upvoted 1 times

  **NikkyDicky** 1 year, 11 months ago**Selected Answer: B**

B for sure

upvoted 1 times

  **SmileyCloud** 2 years 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 2 times

  **Maria2023** 2 years 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 2 times

  **Alabi** 2 years 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 4 times

  **i_am_robot** 2 years 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** 2 years ago

B, SSE-S3 does not incur additional costs.

upvoted 2 times

  **shree2023** 2 years 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.

Correct Answer: BD

Community vote distribution

BD (100%)

 **SmileyCloud** Highly Voted 2 years 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 7 times

 **duriselvan** Most Recent 1 year, 6 months ago

D. Add an Amazon SQS queue and reprocessing logic between Amazon S3 and the Lambda functions. This decouples photo upload from processing, prevents Lambda overload, and offers retry capabilities.
A. Evaluate and adjust the RCUs for the DynamoDB tables. This ensures sufficient read capacity for application state retrieval without overspending on unused capacity.
upvoted 2 times

 **career360guru** 1 year, 7 months ago

Selected Answer: BD

option B and D
upvoted 2 times

 **ggrodsckiy** 1 year, 11 months ago

Correct BD
upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: BD

BD for sure
upvoted 1 times

 **gd1** 2 years ago

Selected Answer: BD

SQS and write to DDB.
upvoted 2 times

 **i_am_robot** 2 years 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 2 times

 **PhuocT** 2 years ago

Selected Answer: BD

B and D, I think

upvoted 1 times

 **shree2023** 2 years ago

Selected Answer: BD

WCU & SQS will solve the issue

upvoted 1 times

 **bhanus** 2 years 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 4 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.

Correct Answer: D

Community vote distribution

D (92%) 8%

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

Selected Answer: D

The solution described in Option D leverages AWS Amplify to create a serverless and scalable architecture for media file uploads. Amplify provides an easier development experience and supports integration with Amazon S3 for file storage and Amazon Cognito for user authentication. Hosting the website through Amazon CloudFront ensures low-latency access for users across the United States and Canada. This solution minimizes operational overhead and accelerates application development.

This blogpost contains a description of a similar use case:

<https://aws.amazon.com/ru/blogs/compute/lifting-and-shifting-a-web-application-to-aws-serverless-part-2/>

upvoted 11 times

 **rrrrrrrrr1** Highly Voted 1 year, 5 months ago

Why not C?

upvoted 5 times

 **career360guru** Most Recent 1 year, 1 month ago

Selected Answer: D

Option D

upvoted 1 times

 **nharaz** 1 year, 2 months ago

Selected Answer: D

Option D (using AWS Amplify, CloudFront, S3, and Cognito) seems like the best choice. It provides a streamlined development process while ensuring scalability, reliability, and user authentication.

upvoted 4 times

 **ggrodsckiy** 1 year, 5 months ago

Correct D.

upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: D

its a D

upvoted 2 times

 **Christina666** 1 year, 5 months 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 4 times

 SmileyCloud 1 year, 6 months agoD - <https://aws.amazon.com/amplify/>

upvoted 2 times

 nexus2020 1 year, 6 months ago**Selected Answer: D**

LEAST operational overhead

upvoted 2 times

 Alabi 1 year, 6 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 1 year, 6 months ago**Selected Answer: D**

Think the key here is this requirement "accelerate application development." Which is one of the things Amplify does

upvoted 2 times

 PhuocT 1 year, 6 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 1 year, 6 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 1 year, 6 months ago**Selected Answer: A**

A is least operational overhead.

D is lot of work upfront

upvoted 3 times

 bhanus 1 year, 6 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.

Correct Answer: B

Community vote distribution

B (100%)

 **bhanus** Highly Voted 1 year, 6 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 7 times

 **career360guru** Most Recent 1 year, 1 month ago

Selected Answer: B

Option B

upvoted 2 times

 **totten** 1 year, 2 months ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html>

upvoted 1 times

 **ggrodsckiy** 1 year, 5 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: B

easy B

upvoted 1 times

 **SmileyCloud** 1 year, 6 months ago

Selected Answer: B

B - custom logs

upvoted 1 times

 **gd1** 1 year, 6 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 3 times

 **shree2023** 1 year, 6 months ago

B is correct indeed

upvoted 1 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.

Correct Answer: C

Community vote distribution

C (96%)	4%
---------	----

 **gd1** Highly Voted 2 years 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 8 times

 **duriselvan** Most Recent 1 year, 6 months ago

C : ans <https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-cors.html>

upvoted 3 times

 **career360guru** 1 year, 7 months ago

Selected Answer: C

Option C

upvoted 1 times

 **severlight** 1 year, 7 months ago

Selected Answer: C

we call API Gateway endpoint from a different origin, API Gateway should be able to verify that request comes from the verified origin, hence you should enable CORS in API Gateway and add your website origin to the list of verified origins.

upvoted 4 times

 **ggrodsckiy** 1 year, 11 months ago

Correct C.

upvoted 1 times

 **rrrrrrrrrr1** 1 year, 11 months 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 2 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

eaasy C

upvoted 1 times

 **javitech83** 1 year, 12 months ago

Selected Answer: C

C is correct

upvoted 1 times

 **SmileyCloud** 2 years ago

Selected Answer: C

C - use case -> <https://repost.aws/knowledge-center/api-gateway-cors-errors>

upvoted 3 times

 **Alabi** 2 years 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 4 times

 **Maria2023** 2 years ago

Selected Answer: A

I vote for A since I was not able to 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** 1 year, 12 months 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

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.

Correct Answer: ACE*Community vote distribution*

ACE (100%)

  **gd1** Highly Voted 1 year, 6 months ago**Selected Answer: ACE**

Yes ACE - A for a new Management account: C for SSO; E for permissions to IAM
upvoted 14 times

  **SkyZeroZx** Highly Voted 1 year, 6 months 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 6 times

  **salazar35** Most Recent 1 year, 1 month ago**Selected Answer: ACE**

ACE make sense.
upvoted 1 times

  **career360guru** 1 year, 1 month ago**Selected Answer: ACE**

A C and E options.
upvoted 1 times

  **ggrodsckiy** 1 year, 5 months ago

Correct ACE.
upvoted 1 times

  **Piccaso** 1 year, 5 months ago**Selected Answer: ACE**

D must be wrong.
upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: ACE

ACE IT!

upvoted 2 times

 **YodaMaster** 1 year, 5 months ago

Selected Answer: ACE

this question scored an ACE

upvoted 1 times

 **SmileyCloud** 1 year, 6 months ago

Selected Answer: ACE

ACE - Management account, AWS SSO with Azure AD and permission sets

upvoted 1 times

 **SkyZeroZx** 1 year, 6 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** 1 year, 6 months ago

Selected Answer: ACE

A, C and E

upvoted 1 times

 **MoussaNoussa** 1 year, 6 months ago

ACE is the right answer

upvoted 1 times

 **psyx21** 1 year, 6 months ago

Selected Answer: ACE

Correct Answer is ACE

upvoted 1 times

Question #262

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.

Correct Answer: B*Community vote distribution*

B (85%)

C (15%)

 **nexus2020**  2 years, 6 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 20 times

 **SKS**  1 year, 8 months ago
 option D seems most cost effective solution
 upvoted 1 times

 **SKS** 1 year, 8 months ago
 This option provides more control over the infrastructure and can accommodate the varying resource requirements of different applications. By utilizing EC2 Auto Scaling and Application Load Balancers, you can efficiently manage resources based on demand. Purchasing Reserved Instances can provide cost savings over the long term.
 upvoted 1 times

 **helloworldabc** 1 year, 4 months ago
 just B
 upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: C

Go with C as it provides standard deployment process for each App.
 One can right size each App using appropriate EC2 sizing for each Application and I feel this approach can be as cost effective as using option B (ECS).
 upvoted 2 times

 **ele** 1 year, 10 months ago

Selected Answer: B

B is the answer.
 Elastic Beanstalk is a PaaS offering by AWS, which automates the deployment and scaling of web applications. It abstracts the underlying infrastructure, making it easier to manage, but it may have some limitations in terms of customization.
 EC2, on the other hand, is an infrastructure as a service (IaaS) offering that provides more control over the virtual servers running your

applications.

With EC2, you have the flexibility to customize the infrastructure to your exact needs, but it requires more manual management. In general, if you require more control and customization, EC2 may be more cost-effective in the long run.

upvoted 1 times

 **ele** 1 year, 11 months ago

Selected Answer: C

Between B & C, I'll go with C .

Both options are using EC2, the cost will be the same. Additional requirement is "standardizing by using a single deployment methodology" , and this is about Beanstalk.

upvoted 4 times

 **duriselvan** 2 years ago

C: ans

The most cost-effective solution is 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.

Here's why:

Cost efficiency:

Elastic Beanstalk: Provides managed application deployment and scaling, reducing operational overhead and potential configuration errors.

Auto Scaling: Ensures that resources are available only when needed, minimizing idle costs.

Reserved Instances: Purchasing 3-year Reserved Instances can offer significant discounts compared to on-demand instances.

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B

upvoted 1 times

 **yorkicurke** 2 years, 2 months ago

Selected Answer: B

Many of you have already explain the reasons why other options are not a good fit. but i will explain optionD bit further.

D-> Wrong

Not only for using Custom Metric but Co-hosting all applications on a single EC2 instance cluster means that the resources (CPU, memory, storage) of the instances would need to be shared among all the applications. This lead to resource contention and inefficient resource allocation, especially when some applications have peak memory requirements of up to 2.5 GB. It may result in underutilization of resources for applications with low usage and performance issues during peak processing times.

upvoted 4 times

 **softarts** 2 years, 4 months ago

Selected Answer: B

B 100% sure

upvoted 1 times

 **ggrodsckiy** 2 years, 5 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months 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 2 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: B

B is correct.

upvoted 1 times

 **Alabi** 2 years, 6 months ago

Selected Answer: B

B for sure

upvoted 1 times

 **shree2023** 2 years, 6 months ago

Selected Answer: B

A is incorrect due to lambda 15mins constraint

B is Correct

upvoted 1 times

 **psyx21** 2 years, 6 months ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

Question #263

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.

Correct Answer: B*Community vote distribution*

B (52%)

D (47%)

 **aviathor** Highly Voted 2 years, 4 months 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 29 times

 **sashenka** 1 year, 2 months ago

One does not need the cluster to read the data. MRFS enables storing persistent data in Amazon S3. This means data remains available even after an EMR cluster is terminated, allowing for cost savings and data reuse across multiple clusters.

upvoted 3 times

 **javitech83** Highly Voted 2 years, 6 months 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 16 times

 **sashenka** 1 year, 2 months ago

One chooses the usage commitment when purchasing a Compute Savings Plan. So, one can base it on the fact that the on-demand nodes will only need to run for a min amount of time. In this case for 6 hrs a day.

upvoted 1 times

 **a178080** Most Recent 3 months, 3 weeks ago

Selected Answer: B

I was first voted for D since I wasn't sure terminating entire Cluster is a good option or even valid. here is why B is better option: Since the data is stored in EMRFS (which uses Amazon S3), you can safely terminate the entire cluster after job completion without losing data. And this is different than terminating primary nodes which are essential for cluster management and run critical services like YARN ResourceManager and HDFS NameNode.

Configure your entire cluster to automatically terminate after a specified idle period. This ensures you don't pay for resources when the cluster is not processing data.

it

upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 4 months, 1 week ago

Selected Answer: B

The key point here is "Amazon EMR cluster that is using the EMR File System (EMRFS)", the EMR File System use S3 as persistent storage, so once the cluster finished the processing of data, the data is ready for the users but the cluster is no longer needed and it can be terminated without any issue.

upvoted 1 times

 **teo2157** 1 year, 6 months ago

Changing my mind to B as the process is business critical and you shouldn't use spot instances for any critical processing but the cluster can be terminated as the data is in S3 once it's processed.

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just D

upvoted 1 times

 **seetpt** 1 year, 7 months ago

Selected Answer: D

D for me

upvoted 1 times

 **43c89f4** 1 year, 8 months ago

B - we should not terminate the cluster.

D - once task is done can terminate the node.

so my answer is D

upvoted 1 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: D

Option D: How To / Use Case

<https://aws.amazon.com/blogs/big-data/strategies-for-reducing-your-amazon-emr-costs/>

upvoted 2 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 Metrics 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.

Correct Answer: C

Community vote distribution

C (100%)

 **AMohanty** Highly Voted 2 years, 4 months ago

Isn't NAT Gateway AWS managed
Why do we need to check if NAT GW is healthy ?
upvoted 10 times

 **bhanus** Highly Voted 2 years, 6 months ago

Selected Answer: C
I go with C
A is incorrect because you don't need 3 nat gateways
B does not make sense to replace ALB
D - you cannot assign elastic ip to ALB
upvoted 7 times

 **gd1** 2 years, 6 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 3 times

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

Selected Answer: C
A would have been the best answer if resilient internet access for private instances is the goal here.

However, the question already states that "the company's security team is bringing only one IP address from its internal IP address range to the cloud". Therefore, C becomes the only suitable answer.

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: C
Option C is best. As there is only one IP address that can be used Option A = 3 NAT gateways are not needed.
upvoted 3 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

This question is little unclear. It does not state whether the communication between on-premise system and AWS is out bond or in bound in nature. If it is outbound then C makes sense.

upvoted 5 times

 **Daniel76** 1 year, 4 months ago

The design should "gives the application the ability to communicate with the on-premises systems", so it is outbound.

upvoted 1 times

 **alonis2201** 2 years, 1 month ago

also think about B option to assign an IP address to NLB

upvoted 2 times

 **ggrodskiy** 2 years, 5 months ago

Correct C.

upvoted 1 times

 **study_aws1** 2 years, 5 months 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 2 times

 **chikorita** 2 years, 4 months 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 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C makes some sense

upvoted 1 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: C

C - single NAT if only one Elastic IP is available.

upvoted 2 times

 **Alabi** 2 years, 6 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 3 times

 **shree2023** 2 years, 6 months ago

Selected Answer: C

C is the answer single NAT is needed

upvoted 1 times

 **PhuocT** 2 years, 6 months ago

I think it's C.

upvoted 1 times

 **psyx21** 2 years, 6 months 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.

Correct Answer: BEF

Community vote distribution

BEF (89%) 5%

 **SmileyCloud**  1 year, 6 months ago

Selected Answer: BEF

B - Remove
E - Invite
F - Verify
<https://repost.aws/knowledge-center/organizations-move-accounts>
upvoted 19 times

 **Khannas** 1 year, 4 months ago

Excellent Explanation
upvoted 5 times

 **yorkicurke**  1 year, 2 months ago

no one talked about;
"All accounts are set up with all the required information so that each account can be operated as a standalone account."
Wouldnt that make Option B invalid?
can some one clarify that plz.
upvoted 1 times

 **shaaam80** 1 year ago

You can remove an account from your organization only if the account is configured with the information required to operate as a standalone account.
upvoted 1 times

 **joleneinthebackyard** 1 year, 1 month ago

No, it's to confirm that B is valid. Removing accounts from organization effectively makes them standalone accounts. The statement you cited, says that they have all info, permissions.. to operate as standalone account thus make B feasible.
upvoted 2 times

 **khksoma** 1 year, 5 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,ands%20services%20continue%20to%20operate>.
upvoted 2 times

 **ggrodsckiy** 1 year, 5 months ago

correct BEF.
upvoted 1 times

✉ **Jonalb** 1 year, 5 months ago

Selected Answer: BEF

its BEF

upvoted 2 times

✉ **NikkyDicky** 1 year, 5 months ago

Selected Answer: BEF

its BEF

upvoted 1 times

✉ **nexus2020** 1 year, 6 months ago

Selected Answer: BEF

remove from org, invite from org, verify from individual. BEF

upvoted 2 times

✉ **gd1** 1 year, 6 months ago

Selected Answer: BEF

GPT 4.0 corrected BEF are the answers. A is not feasible.

upvoted 3 times

✉ **gd1** 1 year, 6 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** 1 year, 6 months ago

GPT corrected BEF are the answers.

upvoted 2 times

✉ **i_am_robot** 1 year, 6 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** 1 year, 6 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 3 times

✉ **PhuocT** 1 year, 6 months ago

B, E, and F, I think

upvoted 1 times

✉ **Jackhemo** 1 year, 6 months ago

Selected Answer: BDE

olabiba.ai says BDE

upvoted 1 times

✉ **rxhan** 1 year, 5 months ago

olabiba.ai is wrong

upvoted 1 times

✉ **bhanus** 1 year, 6 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 3 times

 **psyx21** 1 year, 6 months ago

Selected Answer: BDE

Correct Answer is BDE

upvoted 1 times

Question #266

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.

Correct Answer: C

Community vote distribution

C (97%)

 **i_am_robot**  2 years, 6 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 19 times

 **874def1**  8 months, 1 week ago

Selected Answer: C

If you are tempted to go with D - remember that S3 event notifications can ONLY be sent to :
SQS, Lambda, SNS Topic, Event Bridge.

You cannot DIRECTLY invoke a Step function as part of the S3 notification. You can use Event bridge to do that. But that is not mentioned here.

upvoted 2 times

 **Peaches35** 12 months ago

Selected Answer: C

Option B would add unnecessary latency by running the detection logic every time an image is fetched from the origin
upvoted 2 times

 **0b43291** 1 year, 1 month ago

Selected Answer: B

By using a Lambda@Edge function triggered by an origin-response event, you can inspect and process the images as soon as they are retrieved from the S3 bucket, before they are cached and served to the end-users. This allows you to detect and handle corrupted images with minimal latency, ensuring a better user experience in the web application.

Option C (S3 event notification invoking a Lambda function) would introduce additional latency, as the Lambda function would run after the image has been ingested into the S3 bucket, and the detection logic would not be integrated with the serving process.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Ignore this. You want to detect before serving. So C is correct

upvoted 2 times

 **duriselvan** 1 year, 10 months ago

<https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html>

Using AWS Lambda with Amazon S3

PDF

RSS

You can use Lambda to process event notifications from Amazon Simple Storage Service. Amazon S3 can send an event to a Lambda function when an object is created or deleted. You configure notification settings on a bucket, and grant Amazon S3 permission to invoke a function on the function's resource-based permissions policy.

upvoted 1 times

✉  **duriselvan** 2 years ago

Lambda@Edge triggered by origin-response event:

Pros:

Detects corrupted images closer to the origin, minimizing impact.

Avoids processing overhead for valid images.

Cons:

Corrupted images might still be partially downloaded by users before detection.

upvoted 1 times

✉  **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C

upvoted 1 times

✉  **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

its a C

upvoted 2 times

✉  **pupsik** 2 years, 6 months ago

Selected Answer: C

Take care of corrupted images as soon as they get uploaded to S3

upvoted 2 times

✉  **gd1** 2 years, 6 months ago

Selected Answer: C

D is for more complex and multiple sets of Lambda.

upvoted 1 times

✉  **shree2023** 2 years, 6 months ago

Selected Answer: C

A&B is too late, D is unnecessary

C is correct

upvoted 3 times

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

How is A&B too late if they are done at the edge before the upload?

upvoted 1 times

✉  **PhuocT** 2 years, 6 months ago

C is correct.

upvoted 1 times

✉  **psyx21** 2 years, 6 months ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #267

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.

Correct Answer: D*Community vote distribution*

D (95%)	5%
---------	----

 **Alabi** Highly Voted 2 years 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 7 times

 **d401c0d** Most Recent 10 months, 3 weeks ago

Selected Answer: D

D – CodeDeploy agent is already installed, so use AMI instead.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: D

Option D

upvoted 1 times

 **severlight** 1 year, 7 months ago

Selected Answer: D

CodeDeploy deployment group should be associated with ASG

upvoted 1 times

 **Ganshank** 1 year, 10 months 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 3 times

 **aviathor** 1 year, 10 months 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 2 times

✉ **aviathor** 1 year, 10 months 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 3 times

✉ **Simon523** 1 year, 10 months 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 2 times

✉ **rxhan** 1 year, 11 months ago

Selected Answer: D

Bake AMI with agent already installed
upvoted 1 times

✉ **achillesatan** 1 year, 11 months ago

Selected Answer: C

D is not correct since it is considering about the code change.
upvoted 1 times

✉ **rxhan** 1 year, 11 months ago

CodeBuild cant create a new AMI?
upvoted 1 times

✉ **NikkyDicky** 1 year, 11 months ago

Selected Answer: D

It's a D
upvoted 1 times

✉ **SmileyCloud** 2 years ago

D - correct. You want the agent baked in the AMI.
upvoted 3 times

✉ **gd1** 2 years 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** 2 years ago

Selected Answer: D

Correct Answer is D
upvoted 2 times

Question #268

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.

Correct Answer: B*Community vote distribution*

B (93%)	7%
---------	----

 **SK_Tyagi** Highly Voted 2 years, 4 months 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 12 times

 **kejam** 1 year, 11 months ago

Agreed

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg-from-instance.html#create-asg-from-instance-console>

upvoted 1 times

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

Selected Answer: B

B is the correct choice.

It introduces an Auto Scaling group to handle automatic instance replacement.

Uses a launch template for new instances.

Keeps the existing ALB to minimize downtime.

Allows attaching existing instances to the ASG.

upvoted 1 times

 **goodard** 1 year, 4 months ago

Selected Answer: D

B and D are similar but

B is wrong since you cannot add ec2 instances to autoscaling group. You can only add ec2 to ALB target group.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

You are wrong. Don't misguide others here with wrong argument.

You can attach EC2 to ASG for sure

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-detach-attach-instances.html>

just simply google `attach ec2 to asg` and you will find the doc above. I don't understand why ppl just make random wrong assumptions and misguide others while it only take a few seconds to verify on google/chatgpt

upvoted 9 times

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

Just B

upvoted 2 times

✉ **career360guru** 2 years, 1 month ago

Selected Answer: B

B is correct answer.

upvoted 2 times

✉ **Ustad** 2 years, 1 month ago

Selected Answer: D

why should we attach the current one, why not leaving it to the ASG?

upvoted 1 times

✉ **yorkicurke** 2 years, 1 month ago

if you read @SK_Tyagi , i think he made a fair point. :)

upvoted 2 times

✉ **carpa_jo** 1 year, 12 months ago

Is ALB even capable of automatically registering existing EC2 instances with an ASG? I don't think so.

upvoted 1 times

✉ **DavScout** 2 years, 2 months ago

Does it require Attaching the existing EC2 instances to the Auto Scaling group? Why is D incorrect or Why B is a better response than D?

upvoted 1 times

✉ **ggrodsckiy** 2 years, 5 months ago

Correct B

upvoted 1 times

✉ **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

its a B

upvoted 1 times

✉ **SmileyCloud** 2 years, 6 months ago

Selected Answer: B

B - correct. Attach the EC2s

upvoted 1 times

✉ **SkyZeroZx** 2 years, 6 months ago

Selected Answer: B

New AS Group - assign to existing ALB and attach EC2s to new Scaling group.

upvoted 1 times

✉ **gd1** 2 years, 6 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** 2 years, 6 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 4 times

✉ **psyx21** 2 years, 6 months ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

Question #269

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.

Correct Answer: C*Community vote distribution*

C (84%)

Other

 **bhanus** Highly Voted 2 years, 6 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 5 times

 **Peaches35** 12 months ago

Option A, as described, scopes the developers' IAM permissions to allow them to launch VPC resources only with CloudFormation. This means that developers would be restricted from creating resources outside of the approved CloudFormation templates. So it is still valid

upvoted 1 times

 **Chris_W_1234** Most Recent 2 months ago

Selected Answer: C

I originally wanted to vote for A, as C, as written, does restrict developers to creating VPCs and EC2 instances. However, the question does state that "Developers can configure VPCs and launch Amazon EC2 instances in a single AWS Region." You can read this as that these two activities are the *only* activities developers do, which means that C would *not* unduly limit their daily work.

upvoted 1 times

 **tama1984** 4 months, 3 weeks ago

Selected Answer: A

The question is asking to not limit too much developers' job. Maybe it's just the wording of C, but C says "to allow access only to AWS Service Catalog." Developers can't work by using only AWS Service Catalog.

upvoted 2 times

 **Deztroyer88** 9 months, 2 weeks ago

Selected Answer: C

S3 interface endpoints are not free, but gateway endpoints are free.

upvoted 2 times

 **Peaches35** 12 months ago

Selected Answer: A

Service Control Policies (SCPs): Enforcing SCPs ensures that developers cannot launch unapproved EC2 instance types, which helps control costs.

AWS CloudFormation: Providing a CloudFormation template for an approved VPC configuration with S3 interface endpoints ensures that data transfer between EC2 instances and S3 does not incur NAT gateway charges, reducing data transfer costs.

IAM Permissions: Scoping IAM permissions to allow developers to launch VPC resources only with CloudFormation ensures compliance with the approved architectural patterns without affecting the speed of development.

upvoted 1 times

 **hamimelon** 1 year, 2 months ago

A. Interface endpoints are cheaper than Gateway endpoints if the resources are in the same region. The question specifically said one region.

upvoted 1 times

 **tungnguyenne** 1 year, 4 months ago

Selected Answer: D

D is correct and least affects the speed at which the developers can perform their tasks

C denies the developers access to any AWS services except AWS Service Catalog, therefore it would limit access to all other services.

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just C

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

C is least disruptive option for Developers productivity.

upvoted 3 times

 **Sweetedadad** 2 years, 3 months ago

Why not D?

upvoted 2 times

 **jwyeung** 5 months, 2 weeks ago

Because it is reactive instead of preventive

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

C works

upvoted 2 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: C

C - let the devs choose what they want but they still adhere to standards. Service catalog does that.

upvoted 3 times

 **SkyZeroZx** 2 years, 6 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 3 times

 **gd1** 2 years, 6 months ago

Selected Answer: C

C is correct. Service catalog solves all issues.

upvoted 1 times

 **psyx21** 2 years, 6 months 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.

Correct Answer: C

Community vote distribution

C (100%)

 **AI8282** 5 months, 1 week ago

Selected Answer: C

For those of you stuck on the fact that you need Orgs enabled to use SCPs or ControlTower and there is no orgs yet, enabling ControlTower creates an org if one doesn't exist.

upvoted 2 times

 **career360guru** 1 year, 1 month ago

Selected Answer: C

B is incorrect as it is too difficult to maintain. C is correct answer.

upvoted 3 times

 **Gabehcoud** 1 year, 4 months ago

my bad, "attach a policy to each user" its a tedious tasks. ignore my previous message.

upvoted 2 times

 **Gabehcoud** 1 year, 4 months ago

can someone please detail why the answer cannot be B?

upvoted 1 times

 **joleneinthebackyard** 1 year, 1 month ago

For this type of question (organization and policy for many accounts), we avoid options that require actions on each account/user. There's always better option to set policies at one place.

upvoted 4 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: C

its a C

upvoted 1 times

 **SmileyCloud** 1 year, 6 months ago

Selected Answer: C

AWS Org, Control Tower and SCPs.

upvoted 4 times

 **Alabi** 1 year, 6 months ago

Selected Answer: C

C for sure

upvoted 1 times

 **gd1** 1 year, 6 months ago

Selected Answer: C

Control Tower with SCP (deny) solves the issues

upvoted 2 times

 **bhanus** 1 year, 6 months ago

Selected Answer: C

C is the answer

upvoted 1 times

 **psyx21** 1 year, 6 months ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

Question #271

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.

Correct Answer: C

Community vote distribution

C (85%)

A (15%)

 **shaaam80** 1 year, 7 months ago

Selected Answer: C

Answer - C
S3 for Web hosting,
Appsync for DB API services
SQS DLQ for Failed orders
upvoted 4 times

 **career360guru** 1 year, 7 months ago

Selected Answer: C

SQS Dead letter Queue is key
upvoted 3 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

C
A would work with Lambda/SQS vs ECS/SQS
upvoted 2 times

 **SkyZeroZx** 1 year, 12 months ago

Selected Answer: C

S3 + Appsync DB API (Manged service) and SQS and Deal letter queue for failed orders
upvoted 1 times

 **SmileyCloud** 2 years ago

Selected Answer: C

C - You don't use "Amazon SQS long polling for retaining failed orders"
upvoted 2 times

 **Alabi** 2 years 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 3 times

 **nexus2020** 2 years ago

Selected Answer: C

C is a good answer, but is it the cheapest? hard to tell

upvoted 2 times

✉️ **Maria2023** 2 years 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 4 times

✉️ **fartosh** 1 year ago

SQS long polling does not solve "retaining failed orders" - it's dead-letter queue's responsibility.

upvoted 1 times

✉️ **pdboi3355** 1 year ago

From AppSync page - Access data from multiple sources with a single request. Instantly create APIs for your databases. Combine APIs into a single Merged API

upvoted 2 times

✉️ **gd1** 2 years ago

Selected Answer: C

S3 + Appsync DB API (Manged service) and SQS and Deal letter queue for failed orders

upvoted 3 times

✉️ **MoussaNoussa** 2 years ago

Correct Answer is C

upvoted 1 times

✉️ **psyx21** 2 years ago

Selected Answer: C

Correct Answer is C

upvoted 2 times

Question #272

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.

Correct Answer: B

Community vote distribution

B (94%)	6%
---------	----

 **gd1** Highly Voted 2 years ago

Selected Answer: B

B- Aurora provides the minimum RTO and RPO (1 min)
upvoted 8 times

 **vjp_training** Highly Voted 1 year, 10 months 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 6 times

 **Soliner_Bilgi_Teknolojileri** Most Recent 4 months, 1 week ago

Selected Answer: B

Aurora Global Database provides cross-Region disaster recovery with the lowest RTO (<1 minute) and RPO (<1 second). Other options are either limited to a single Region, rely on slower asynchronous replication, or require manual failover, which cannot meet the strict requirements.
upvoted 1 times

 **bidboom** 7 months ago

Selected Answer: B

Its B sure.
upvoted 1 times

 **Dgix** 1 year, 3 months ago

Selected Answer: B

B. Not the cheapest, but the other ones are either not cross-regional or can't handle the RTO/RPO.
upvoted 1 times

 **Russ99** 1 year, 3 months ago

Selected Answer: B

Amazon's documentation states that for Multi-AZ deployments, the typical RTO for failing over to the standby is 60-120 seconds. For read replicas, since the lag is typically larger, the RTO is often cited as around 5-10 minutes under normal conditions.
upvoted 1 times

 **GaryQian** 1 year, 6 months ago

Selected Answer: B

The question doesn't mention cost, so usually it will be the best performance choice. In this case is B
upvoted 3 times

 **career360guru** 1 year, 7 months ago

Selected Answer: B

B is right answer
upvoted 2 times

 **AMohanty** 1 year, 7 months ago

A

RDS Read Replica is more cost effective and can be promoted as Primary within 5 mins
upvoted 2 times

 nicksss 1 year, 7 months ago

Selected Answer: A

Why not A? Promoting a read replica will still meet the RTO of 5 minutes while being cheaper than using aurora.
upvoted 2 times

 softarts 1 year, 10 months 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 2 times

 NikkyDicky 1 year, 11 months ago

Selected Answer: B

B for Baurora
upvoted 5 times

 shree2023 2 years ago

Selected Answer: B

B global database is correct
upvoted 2 times

 bhanus 2 years ago

Selected Answer: B

B Aurora is the right choice
upvoted 1 times

 psyx21 2 years ago

Selected Answer: B

Correct Answer is B
upvoted 1 times

Question #273

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.

Correct Answer: D

Community vote distribution

D (100%)

 **shaaam80** 1 year ago

Answer - D
Always SCPs for OUs to confine accounts from using services
upvoted 2 times

 **career360guru** 1 year, 1 month ago

Selected Answer: D
D for sure
upvoted 1 times

 **joleneinthebackyard** 1 year, 1 month ago

Selected Answer: D
Cant be anything else than D
upvoted 1 times

 **ggrodsckiy** 1 year, 5 months ago

Correct D.
upvoted 1 times

 **Don2021** 1 year, 5 months 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 2 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: D
easy D
upvoted 1 times

 **SmileyCloud** 1 year, 6 months ago

Selected Answer: D
D - Correct. SCPs applied to OU.
upvoted 2 times

 **shree2023** 1 year, 6 months ago

Selected Answer: D
D is correct
upvoted 1 times

 **gd1** 1 year, 6 months ago

Selected Answer: D
OU and SCP to have Tags and regions denied
upvoted 1 times

 **psyx21** 1 year, 6 months ago

Selected Answer: D

Correct Answer is D

upvoted 1 times

Question #274

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.

Correct Answer: D*Community vote distribution*

D (79%)	14%	7%
---------	-----	----

 **rxhan** Highly Voted 2 years, 5 months ago

Script is never AWS answers
upvoted 9 times

 **Sin_Dan** Most Recent 1 year, 2 months ago

Selected Answer: A
Option D impacts the application's normal workflow. It will block access to the objects from the internet irrespective of whether the user is authorised or not.
upvoted 1 times

 **Phil___** 1 year, 6 months ago

Selected Answer: D
Not C due to the following:

C. Script for Private ACL (Potentially Disruptive):

Setting a private ACL on all objects might disrupt existing download mechanisms that rely on signed URLs.

upvoted 1 times

 **goodard** 1 year, 4 months ago

Also running script is only temporary solution since files uploaded after script it executed can still be publicly accessible. So D is better selection.
upvoted 1 times

 **kejam** 1 year, 11 months ago

Selected Answer: D
Answer: D
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-presigned-url.html>
upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: D
Public Block access
upvoted 2 times

 **rif** 2 years, 2 months ago

D.
IgnorePulicAcls : Setting this option to TRUE causes Amazon S3 to ignore all public ACLs on a bucket and any objects that it contains. This setting enables you to safely block public access granted by ACLs while still allowing PUT Object calls that include a public ACL (as opposed to BlockPublicAcls, which rejects PUT Object calls that include a public ACL). Enabling this setting doesn't affect the persistence of any existing ACLs and doesn't prevent new public ACLs from being set.
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html>
upvoted 4 times

 **ggrodsckiy** 2 years, 5 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 3 times

NikkyDicky 2 years, 5 months ago

Selected Answer: D

its a D

upvoted 1 times

SmileyCloud 2 years, 6 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 2 years, 6 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 IgnorePublicAcIs 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

easytoo 2 years, 6 months ago

d-d-d-d-d-d

upvoted 1 times

nexus2020 2 years, 6 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 2 times

joleneinthebackyard 2 years, 2 months ago

Then you know to choose D since "running a script" never be the answer in aws exam

upvoted 2 times

shree2023 2 years, 6 months ago

Selected Answer: C

C indeed

upvoted 1 times

gd1 2 years, 6 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 2 years, 6 months ago

Selected Answer: D

D - Block Public Access feature in Amazon S3 to set the IgnorePublicAcIs

upvoted 2 times

psyx21 2 years, 6 months 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.

Correct Answer: ACE*Community vote distribution*

ACE (97%)

 **SmileyCloud**  2 years 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 17 times

 **TonytheTiger**  1 year, 3 months ago

Selected Answer: ACE

Option E - <https://aws.amazon.com/blogs/database/migrating-oracle-databases-with-near-zero-downtime-using-aws-dms/>

Option A - <https://docs.aws.amazon.com/dms/latest/sbs/chap-oracle-postgresql.migration-process.database-schema-conversion.html>
upvoted 2 times

 **duriselvan** 1 year, 6 months ago

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.
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.

upvoted 1 times

 **shaaam80** 1 year, 7 months ago

Selected Answer: ACE

Answer - ACE
Create target DB and use SCT for Schema conversion
VPC peering and Open DB access ports via SGs
AWS DMS to fully load + CDC
upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: ACE

A, C, E right options

upvoted 1 times

 **joleneinthebackyard** 1 year, 8 months ago

Selected Answer: ACE

Choices are between A vs B, C vs D, E vs F.

B: SCT cannot create RDS

D: When you see making database publicly accessible, you don't need to read more

F: only perform on changed data while E also do the full load

upvoted 1 times

 **ggrodsckiy** 1 year, 11 months ago

Correct ACE.

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: ACE

ACE it

upvoted 1 times

 **SkyZeroZx** 2 years ago

Selected Answer: ACE

ACE are correct

B is incorrect because SCT cannot create RDS instance

upvoted 1 times

 **Maria2023** 2 years ago

Selected Answer: ACE

<https://docs.aws.amazon.com/dms/latest/sbs/chap-oracle-postgresql.migration-process.data-migration.html>

upvoted 1 times

 **shree2023** 2 years ago

Selected Answer: ACE

ACE is correct

upvoted 1 times

 **gd1** 2 years ago

Selected Answer: ACE

A. Use SCT; C- Peering; E - DMS with full and change

upvoted 1 times

 **PhuocT** 2 years ago

A, C and E

upvoted 1 times

 **jubileu84** 2 years ago

Correct Answer is ACE

upvoted 1 times

 **bhanus** 2 years ago

Selected Answer: ACE

ACE are correct

B is incorrect because SCT cannot create RDS instance

upvoted 3 times

 **MoussaNoussa** 2 years ago

Correct Answer is ACE

upvoted 3 times

 **psyx21** 2 years ago

Selected Answer: BEF

Correct Answer is BEF

upvoted 1 times

Question #276

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.

Correct Answer: D*Community vote distribution*

D (88%) 12%

 **SkyZeroZx**  1 year, 12 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 17 times

 **7f6aef3**  1 year, 1 month ago

ANS: D

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-dead-letter-queue.html>

upvoted 1 times

 **ram8** 1 year, 5 months ago

C is the ans,

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.

in the question, we have SQS standard queue. hence ans is C

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

upvoted 1 times

 **ram8** 1 year, 5 months ago

sry typo its "D"

upvoted 1 times

 **duriselvan** 1 year, 6 months ago

ANS c

Configure a new SQS FIFO queue as a dead-letter queue to isolate the faulty messages.

Fault isolation: A dead-letter queue (DLQ) provides a dedicated location for storing messages that cannot be processed successfully. This isolates the faulty message from the main queue, allowing subsequent messages to be processed without interruption.

FIFO processing: Since the faulty message is causing an error on the backend, it's crucial to retain the original order of messages. A FIFO queue preserves the order in which messages were received, ensuring proper processing order after resolving the issue with the faulty message.

Message analysis: Placing the faulty message in the DLQ facilitates further analysis to identify the cause of the error and update the backend to handle such messages in the future.

upvoted 2 times

 **career360guru** 1 year, 7 months ago

Selected Answer: D

Option D is most logical right answer.

This question description looks little confusing. Why in a standard SQS one faulty message can block other message processing. It must be a FIFO queue. Processing logic should continue reading other arriving messages that are not faulty. One faulty message may keep failing after every 30 sec of visibility timeout.

upvoted 4 times

en 1 year, 7 months ago

Selected Answer: C

It is C. In an ordering system, it is important to receive the orders in order, so FIFO. Both C and D are new SQS queues - doesn't matter what the original was.

upvoted 2 times

joleneinthebackyard 1 year, 8 months ago

Selected Answer: D

Somehow I read the option D as create a new queue (to replace the current one) and so confused of what's going on. Wording for this exam is really disaster.

upvoted 4 times

ggrodsckiy 1 year, 11 months ago

Correct D.

upvoted 1 times

Nikkidyky 1 year, 11 months ago

Selected Answer: D

it's a D

upvoted 2 times

rxhan 1 year, 11 months 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 3 times

Jonalb 2 years 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 2 times

Jonalb 2 years ago

Selected Answer: C

C

its a C

upvoted 1 times

SmileyCloud 2 years 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

SkyZeroZx 2 years ago

Selected Answer: D

D dead letter queu

upvoted 2 times

shree2023 2 years ago

Selected Answer: D

D indeed

C incorrect FIFO will slow down the process

upvoted 3 times

gd1 2 years 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 3 times

i_am_robot 2 years 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 2 times

Question #277

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".

Correct Answer: ABC*Community vote distribution*

ABC (89%) 4%

 **Maria2023**  2 years, 6 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 6 times

 **youonebe**  1 year, 1 month ago

Selected Answer: ABC

abc-abc-abc

upvoted 1 times

 **liquen14** 1 year, 9 months ago

Selected Answer: AB

I think that ABC makes the most sense here but look what I found reading this: <https://docs.aws.amazon.com/step-functions/latest/dg/concepts-error-handling.html>

"A retry or catch on States.ALL won't catch States.Runtime errors."

Really does this need to be so convoluted? Do we need to be tested in such nitty-gritty details? :-)

upvoted 1 times

 **liquen14** 1 year, 9 months ago

Correcting my poor English grammar:

"Really, does this need to be so convoluted? Do we need to be tested in such nitty-gritty details?"

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: ABC

A, B, C - Right answers

upvoted 2 times

 **joleneinthebackyard** 2 years, 2 months ago

Selected Answer: ABC

I love how this question formulated, wish all SAP question can be of this type. With only knowing SES is not for notification, you can rule out D and E. We have to choose three among A B C F, which easily can narrow down to choose between C and F as they are similar. Then yeah, State.ALL vs State.Runtime determines it, A B C it is 😅

upvoted 3 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: ABC

simple as ABC

upvoted 1 times

 **javitech83** 2 years, 6 months ago

Selected Answer: ABC

ABC is the right answer

upvoted 1 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: ABC

ABC

D, E - SES - not good

F - States.runtime, doesn't catch all errors

upvoted 2 times

 **gd1** 2 years, 6 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 3 times

 **shree2023** 2 years, 6 months ago

Selected Answer: ABC

ABC is correct

upvoted 1 times

 **gd1** 2 years, 6 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** 2 years, 6 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 2 times

 **PhuocT** 2 years, 6 months ago

A, B and C

upvoted 1 times

 **bhanus** 2 years, 6 months ago

Selected Answer: ABC

ABC are right

DE are incorrect because SES cannot be used here. SES can be good fir for Bulk/Marketing emails

F is incorrect because the error type "States.Runtime" doesn't catch all types of errors. The ques asks "notifications are sent for all types of failures "

upvoted 2 times

 **MoussaNoussa** 2 years, 6 months ago

ABC is the right answer

upvoted 2 times

 **psyx21** 2 years, 6 months 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.

Correct Answer: B

Community vote distribution

B (100%)

 **bhanus** Highly Voted 1 year, 6 months ago

Selected Answer: B

Outbound resolver endpoints will let you query your on-prem DNS
Inbound resolver endpoints will let your on-prem DNS server to query the AWS VPC DNS server
upvoted 13 times

 **gd1** 1 year, 6 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 4 times

 **career360guru** Most Recent 1 year, 1 month ago

Selected Answer: B

A is incorrect. B is right answer.
upvoted 1 times

 **SK_Tyagi** 1 year, 4 months ago

Selected Answer: B

bhanus explanation spot on
upvoted 1 times

 **ggrodsckiy** 1 year, 5 months ago

Correct B.
upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: B

B for sure
upvoted 1 times

 **Jonalb** 1 year, 6 months ago

Selected Answer: B

b
its a B
upvoted 1 times

 **SmileyCloud** 1 year, 6 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** 1 year, 6 months ago

Selected Answer: B

B is correct

upvoted 1 times

 **bhanus** 1 year, 6 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** 1 year, 6 months 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.

Correct Answer: C

Community vote distribution

C (100%)

 **gd1** Highly Voted 2 years 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 8 times

 **nexus2020** Highly Voted 2 years 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 5 times

 **0dc6cac** 6 months, 2 weeks ago

they are talking about creating route tables for the TGW attachments, not the TGW itself....so each TGW-VPC attachment would have its own RT

upvoted 1 times

 **career360guru** Most Recent 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

 **shaaam80** 1 year, 7 months ago

Selected Answer: C

Answer C.

Since TGW is responsible for VPCs communicating with each other, there should be default routes for each VPC attachment on the TGW route table limiting access to VPCs

upvoted 4 times

 **ggrodsckiy** 1 year, 11 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

it's a C

upvoted 1 times

 **SmileyCloud** 2 years ago

Selected Answer: C

C - Correct. Static routes on TGW.

upvoted 2 times

 **shree2023** 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

 **MoussaNoussa** 2 years ago

C is the right answer

upvoted 1 times

 **psyx21** 2 years ago

Selected Answer: C

Correct Answer is C

upvoted 2 times

Question #280

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.

Correct Answer: C

Community vote distribution

C (91%)	9%
---------	----

 **AI8282** 5 months ago

Selected Answer: B

I hate this question so much. It blatantly says LEAST development effort. Spinning up a Ec2 instance is way easier than configuring appstream. Linux clients have a ton of ways they can connect to Remote Desktop without problems. C is by far the better answer though over time but purely just only for DEVELOPMENT B is better.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option C uses Amazon AppStream 2.0, a service that allows you to host and manage desktop applications in the cloud. You can create an image of your Windows-based desktop application, and provision an On-Demand fleet with dynamic Fleet Auto Scaling policies for running the image. This way, employees can access the application by starting browser-based AppStream 2.0 streaming sessions. AppStream 2.0 also allows you to implement authentication using user pools, which is a simplified way of managing access compared to Active Directory or setting up virtual desktops for every employee.

upvoted 4 times

 **trungtd** 1 year, 6 months ago

Selected Answer: C

typical use case of appstream

upvoted 3 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C. B is possible but it needs RDP connectivity to Windows server and so will be more complex than C

upvoted 2 times

 **chico2023** 2 years, 4 months ago

Selected Answer: C

Answer: C - Don't even think in any other option. It's AppStream what they need to provision.

upvoted 2 times

 **ggrodsckiy** 2 years, 5 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

it's C, so Linux desktops can access via browser
upvoted 3 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: C

C - Correct. AppStream is what is Citrix XenDesktop.
upvoted 1 times

 **nexus2020** 2 years, 6 months ago

Selected Answer: C

Amazon Cognito identity pools does not support AD. however WorkSpace is a right choise forthis use case though.
upvoted 2 times

 **Alabi** 2 years, 6 months ago

Selected Answer: C

C for sure
upvoted 1 times

 **shree2023** 2 years, 6 months ago

Selected Answer: C

C is correct answer
upvoted 1 times

 **gd1** 2 years, 6 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 4 times

 **PhuocT** 2 years, 6 months ago

C seems correct answer.
upvoted 1 times

 **bhanus** 2 years, 6 months ago

Selected Answer: C

C
Use appstream
upvoted 1 times

 **psyx21** 2 years, 6 months ago

Selected Answer: B

Correct Answer is B
upvoted 1 times

 **Alabi** 2 years, 6 months ago

Stop putting wrong answers in every question
upvoted 23 times

Question #281

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.

Correct Answer: B*Community vote distribution*

B (96%)	4%
---------	----

 **Alabi** Highly Voted 2 years, 6 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 6 times

 **sarlos** Most Recent 1 year, 7 months ago

Why not D , Is it because it is expensive?

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Yeah, you don't wanna build a Redshift cluster for it. You store data in S3, and use Athena to query it, so you just pay for the query you run rather than paying for the whole Redshift cluster

upvoted 2 times

 **helloworldabc** 1 year, 4 months ago

just B

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: B

Option B - Athena can connect to your data stored in Amazon S3 using the AWS Glue Data Catalog to store metadata such as table and column names. After the connection is made, your databases, tables, and views appear in Athena's query editor.

<https://docs.aws.amazon.com/athena/latest/ug/data-sources-glue.html>

upvoted 2 times

 **kejam** 1 year, 11 months ago

Selected Answer: C

The question doesn't provide enough info to calculate the answer. We need to know how large the emr cluster is, how many queries, and how many TBs/PBs of data per query per day. However I'm leaning towards...

Answer C: Store data in EMR File System (EMRFS). Use Presto in Amazon EMR to query data.

EMRFS is an implementation of HDFS that all Amazon EMR clusters use for reading and writing regular files from Amazon EMR directly to Amazon S3.

The company could switch to EMRFS and continue to use Presto which comes included in EMR and turn off the clusters when not in use while the data persists in EMRFS(S3).

EMR comes in many flavors with different price points (EC2, Serverless) and is geared more towards daily data pipelines like this company

is running.

Regarding B: Athena is serverless and great for ad-hoc queries, but it is not cheap.

upvoted 1 times

 **CProgrammer** 2 years ago

significantly more expensive to store data in Redshift compared to S3 HOWEVER

<https://docs.aws.amazon.com/redshift/latest/gsg/data-lake.html> You can use Amazon Redshift Spectrum to query data in Amazon S3 files without having to load the data into Amazon Redshift tables. Athena: While cost-effective for occasional ad-hoc queries, Athena's serverless architecture may not be as performant for frequent, resource-intensive queries [Queries scan large amounts of data]

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

B is most cost effective. A Redshift Spectrum can be a good option but then it needs Redshift cluster which may be more expensive. One information missing in the question is many queries/sec. If there are large number queries/sec then A can be better choice.

upvoted 3 times

 **ggrodsckiy** 2 years, 5 months ago

Correct B

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

it's a B

upvoted 2 times

 **SkyZeroZx** 2 years, 5 months ago

Selected Answer: B

Clasic ServerLess

S3 Datalake

Glue for ETL

Athena for Query

upvoted 4 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: B

B - S3 , GDC and Athena for sure is the cheapest.

upvoted 1 times

 **shree2023** 2 years, 6 months ago

Selected Answer: B

B is most cost effective

upvoted 1 times

 **gd1** 2 years, 6 months ago

Selected Answer: B

S3 with Glue and Athena will do the trick

upvoted 1 times

 **PhuocT** 2 years, 6 months ago

Selected Answer: B

B could be the answer

upvoted 1 times

 **bhanus** 2 years, 6 months ago

Selected Answer: B

B is the answer

upvoted 1 times

 **psyx21** 2 years, 6 months ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

Question #282

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.

Correct Answer: C*Community vote distribution*

C (89%)

11%

 **TonytheTiger** 1 year, 3 months ago

Selected Answer: C

Option C: Expanding use of tag policies in AWS Organization

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies-getting-started.html
upvoted 2 times

 **career360guru** 1 year, 7 months ago

Selected Answer: C

Option C

upvoted 2 times

 **ggrodsckiy** 1 year, 11 months ago

Correct C.

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: C

C of course

upvoted 2 times

 **hexie** 1 year, 11 months 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 2 times

 **SmileyCloud** 2 years ago

Selected Answer: C

C - Apply tags and prevent future untagged resources to be created with SCPs.

upvoted 2 times

 **SkyZeroZx** 2 years ago

Selected Answer: C

C , adicionally use SCP for denied not create resource without tag in the future

upvoted 1 times

 **Maria2023** 2 years 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 3 times

 **shree2023** 2 years ago

Selected Answer: C

C is correct.

A only takes care of existing resources not future resources

upvoted 2 times

 **gd1** 2 years 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** 2 years ago

C makes sense, using SCP

upvoted 1 times

 **bhanus** 2 years ago

Selected Answer: C

C is correct use SCPs

upvoted 1 times

 **MoussaNoussa** 2 years ago

C is the right answer

upvoted 1 times

 **Don2021** 2 years ago

Why not C, C will take care of existing and SCP will ensure future resources are tagged

upvoted 3 times

 **psyx21** 2 years ago

Selected Answer: A

Correct Answer is A

upvoted 1 times

 **Ustad** 1 year, 7 months ago

wrong answer. you need the scp for future resources.

upvoted 2 times

Question #283

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.

Correct Answer: AC*Community vote distribution*

AC (87%)

8%

 **Christina666** Highly Voted 2 years, 5 months 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 12 times

 **cachac** Highly Voted 2 years, 1 month ago

Selected Answer: AC

AC:

"The company must send the data privately" = Interface endpoints

Gateway endpoints, do not allow access from on premises.

upvoted 6 times

 **JoeTromundo** Most Recent 1 year, 2 months ago

Selected Answer: AC

Why not A and D: "Currently, gateway VPC endpoints for Amazon S3 do not support accessing resources in a different Region, in a different VPC, or from an on-premises data center (environment outside of AWS)."

upvoted 2 times

 **gfhbox0083** 1 year, 5 months ago

Selected Answer: AC

A, C for sure.

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

 **LazyAutonomy** 1 year, 11 months ago

Selected Answer: AC

Really, really awful question. Agree that the answer they're looking for is AC. However, technically, this element of B if done in isolation will also work and might actually be better: "Set up an AWS Direct Connect connection with a public VIF between the on-premises environment and the private VPC". Just because you're accessing S3 using its public IPs, doesn't mean you're routing over the "public internet". Plus, accessing S3 via its regular public prefixes means no mucking around with `--endpoint-url https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com` command line options. Your devs can just use S3 normally with normal DNS hostnames. If they forget then the traffic will route via the internet - oops. So B+anything-else is technically also correct, and arguably preferable.

upvoted 4 times

 **eboehm** 2 weeks, 3 days ago

true however, you cant connect a public vif to a VPC

upvoted 1 times

 **LazyAutonomy** 1 year, 11 months ago

And yes, I know that technically a public VIF has nothing to do with nor are they attached to VPCs, but the core tenet of B is to "use public VIF", i.e. public peering. So, if I was faced with this situation in real life, I'd consider that. The downside of the public VIF approach is missing out on VPC endpoint policies. Maybe the optimal solution is to deploy EC2 forward proxies in a VPC with an S3 gateway endpoint?

upvoted 3 times

 **duriselvan** 2 years ago

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.

This creates a dedicated, private connection between the on-premises systems and the AWS VPC, ensuring data remains secure and isolated from the public internet. The private VIF further enhances security by preventing access to the S3 buckets from the public internet.

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.

This establishes connectivity between the private VPC and the VPCs containing the S3 buckets, enabling private data transfer without crossing the public internet. Peering allows resources in both VPCs to communicate directly, maintaining data security and privacy.

upvoted 1 times

 **ayadmaawla** 2 years ago

S3 doesn't live in a customer VPC. It's a public service. So you either connect to it over the Internet or through a VPC Gateway endpoint or Interface Endpoint depending on the setup.

upvoted 3 times

 **career360guru** 2 years, 1 month ago

Selected Answer: AC

S3 Gateway endpoint is for access inside VPC and not from on-premise.

upvoted 6 times

 **enk** 2 years, 1 month ago

Selected Answer: CE

C: needs to be an endpoint

E: Company does NOT have a dedicated network connection so DX answers are out, so peer the VPC's.

upvoted 3 times

 **cmoreira** 2 years, 3 months 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 4 times

 **ggrodsckiy** 2 years, 5 months ago

Correct AC.

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: AC

AC of course. see links below

upvoted 1 times

 **pupsik** 2 years, 6 months ago

Selected Answer: AC

AC - links provided by other members provide very good explanation.

upvoted 1 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: AC

AC - detailed steps under use case 2 -> <https://repost.aws/knowledge-center/s3-bucket-access-direct-connect>

upvoted 4 times

 **NETeng01** 2 years, 6 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** 2 years, 6 months ago

Thank you. Perfect explanation

upvoted 1 times

 **Mekala** 2 years, 6 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** 2 years, 6 months ago

Selected Answer: AC

Seems AC

upvoted 1 times

 **gd1** 2 years, 6 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

Question #284

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 RCUs and WCUs.
- 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.

Correct Answer: C*Community vote distribution*

C (67%)	B (26%)	7%
---------	---------	----

 **saggy4** Highly Voted 1 year, 10 months ago

Selected Answer: B

The correct answer is B: On Demand
Autoscaling with the current RCU and WCU will not make sense since it is defined for peak loads
upvoted 10 times

 **titi_r** 1 year, 8 months ago
"C" is correct, because the question states a "

You can use auto scaling to adjust your table's provisioned capacity automatically in response to traffic changes. Provisioned mode is a good option if any of the following are true:
- You have PREDICTABLE application traffic.

On-demand mode is a good option if any of the following are true:
- You have unpredictable application traffic.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html#HowItWorks.OnDemand>
upvoted 1 times

 **helloworldabc** 1 year, 4 months ago
just C
upvoted 1 times

 **career360guru** Highly Voted 2 years, 1 month ago

Selected Answer: C

Question itself is bit unclear as it does not state difference in load for peak vs non-peak. Choice of most cost-effective depends on this between Reserved vs on-demands vs autoscaling. Overall autoscaling looks safest option.
upvoted 7 times

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

Selected Answer: C

For known workload and need to scale during low time, auto scaling is a no brain-er
upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 4 months, 1 week ago

Selected Answer: B

The most cost-effective solution is B, on-demand capacity, because it automatically scales with traffic, requires no management, and charges only for actual usage, unlike provisioned or reserved capacity which waste money during off-peak hours.
upvoted 1 times

 **sammyhaj** 1 year ago

Selected Answer: C

On demand is \$\$\$
provisioned all the time is \$\$\$
but autoscaling works with provisioned to scale write and read when needed
upvoted 1 times

0b43291 1 year, 1 month ago

Selected Answer: B

If your workload has predictable peak periods and relatively stable traffic patterns during off-peak times, as in the case of the quick-service restaurant scenario, on-demand capacity mode may be more cost-effective and require less operational overhead than Auto Scaling.

Option C (Enabling DynamoDB auto scaling) can help manage capacity during peak periods, but it still requires provisioned capacity and may not be as cost-effective as on-demand capacity mode for workloads with predictable peak periods.

upvoted 1 times

vip2 1 year, 5 months ago

Selected Answer: C

C is correct one
DynamoDB auto-scaling for predictable
DynamoDB on-demand for un-predictable
upvoted 2 times

mark_232323 1 year, 5 months ago

Selected Answer: C

By implementing DynamoDB Auto Scaling, you can achieve the following benefits:

Cost savings: During non-peak hours, the provisioned capacity will automatically scale down, reducing the cost of provisioned throughput.
Consistent performance: During peak hours, the provisioned capacity will automatically scale up to handle the increased workload, ensuring consistent performance.

Reduced operational overhead: Auto Scaling eliminates the need for manual capacity management, reducing the operational burden on the IT staff.

upvoted 3 times

michele_scar 1 year, 7 months ago

Selected Answer: B

If you know that the peak is in the 4hour you can use autoscaling.
BUT, if you want to reduce operation IT, and if the peak goes higher in other moment, on-demand is the way
upvoted 2 times

titi_r 1 year, 8 months ago

"C" is correct, because the question states "a predictable module".

You can use auto scaling to adjust your table's provisioned capacity automatically in response to traffic changes. Provisioned mode is a good option if any of the following are true:

- You have PREDICTABLE application traffic.

On-demand mode is a good option if any of the following are true:

- You have unpredictable application traffic.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html#HowItWorks.OnDemand> and

upvoted 2 times

Russ99 1 year, 9 months ago

Selected Answer: C

C is the correct answer. On Demand is out since it is only fully used for 4 hours daily
upvoted 2 times

kejam 1 year, 11 months ago

Selected Answer: C

Answer C:
<https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/>
upvoted 2 times

duriselvan 2 years ago

B ia ans
<https://dynobase.dev/dynamodb-on-demand-vs-provisioned-scaling/>
upvoted 1 times

Arnaud92 2 years, 4 months 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 4 times

ayadmawla 2 years ago

You are right but if you reserve the capacity based on the peak requirement, you only use that capacity for 4 / 24 hours per day. Whilst if you provision to guarantee availability and auto-scale to that level you will save 20 hours of low usage. As @career360guru said, we will need more information as to what that balance of 72% savings on 4 hours would be when compared to provisioned+auto-scaled means for the savings on 20 hours (per day).

upvoted 1 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: C

its C for predictable scaling

upvoted 3 times

 **SkyZeroZx** 2 years, 5 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 5 times

 **SmileyCloud** 2 years, 6 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 5 times

Question #285

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.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Alabi**  2 years 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 8 times

✉  **NikkyDicky**  1 year, 11 months ago

Selected Answer: C

C. websockets ==realtime

upvoted 6 times

✉  **kejam**  1 year, 5 months ago

Selected Answer: C

Answer C:

<https://docs.aws.amazon.com/appsync/latest/devguide/aws-appsync-real-time-data.html>

upvoted 3 times

✉  **SmileyCloud** 2 years ago

Selected Answer: C

C - Correct. <https://advancedweb.hu/real-time-data-with-appsync-subscriptions/>

upvoted 1 times

✉  **shree2023** 2 years ago

Selected Answer: C

C is correct others are not real time and cost effective

upvoted 2 times

✉  **gd1** 2 years 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 3 times

✉  **psyx21** 2 years 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.

Correct Answer: B

Community vote distribution

B (95%)	5%
---------	----

 **SmileyCloud**  2 years, 6 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 5 times

 **softarts** 2 years, 4 months 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

 **CProgrammer**  2 years ago

@duriselvan "the" access point
 which one bro.. all of them ? ==>
 hundreds of AWS accounts centrally in an organization in AWS Organizations. company recently started to allow product teams to create and manage their own S3 access points in their accounts.
 regarding Minimal impact? was that constraint perhaps from some other question ?
 MOST operationally efficient way to enforce this requirement
 Lastly Resource policies inherently apply to actions performed on a specific resource. To control the creation of a resource like an access point, a broader policy mechanism is needed.
 upvoted 1 times

 **durielvan** 2 years ago

A. Set the S3 access point resource policy to deny the s3>CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

Here's why:

Granularity: Enforcing the restriction within the access point resource policy itself offers the most granular control. It applies directly to the access point creation action, preventing unauthorized configuration at the source.

Centralized management: Implementing the policy at the access point level allows for centralized management and avoids the need to manage individual IAM policies in each account. This simplifies operation and reduces maintenance overhead.

Minimal impact: This approach doesn't require additional infrastructure or services like Service Control Policies (SCPs) or CloudFormation StackSets, minimizing setup and complexity.

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

As customer is using Organizations B is right.

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B. SCP for scale

upvoted 3 times

 **SkyZeroZx** 2 years, 6 months ago

Selected Answer: B

B is correct SCP at Org level

upvoted 3 times

 **shree2023** 2 years, 6 months ago

Selected Answer: B

B is correct SCP at Org level

upvoted 3 times

 **gd1** 2 years, 6 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** 2 years, 6 months ago

Selected Answer: B

B

when the question mention AWS Organizations, use SCP always the good choice.

upvoted 2 times

 **MoussaNoussa** 2 years, 6 months ago

of course answer B

upvoted 1 times

 **Don2021** 2 years, 6 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

Question #287

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.

Correct Answer: B

Community vote distribution

B (100%)

 **gd1** Highly Voted 2 years 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 10 times

 **duriselvan** Most Recent 1 year, 6 months ago

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 3 times

 **career360guru** 1 year, 7 months ago

Selected Answer: B

Option B.

upvoted 3 times

 **ggrodsckiy** 1 year, 11 months ago

Correct B.

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: B

its a B

upvoted 2 times

 **Jonalb** 2 years ago

Selected Answer: B

B

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 2 times

 **SmileyCloud** 2 years ago

Selected Answer: B

B - Look at the link, step 5 -> <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 2 times

 **SkyZeroZx** 2 years ago

Selected Answer: B

B. Select the Swap Environment URLs option.

upvoted 2 times

 **shree2023** 2 years ago

Selected Answer: B

B to swap from blue to green

upvoted 1 times

 **bhanus** 2 years 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** 2 years ago

B of course

upvoted 1 times

 **psyx21** 2 years ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

Question #288

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.

Correct Answer: C

Community vote distribution

C (100%)

 **nexus2020** Highly Voted 1 year, 6 months ago

Selected Answer: C

ALB – B is out
S3 is good enough, EFS and EBS are too much for image processing
upvoted 5 times

 **Alabi** Highly Voted 1 year, 6 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 5 times

 **career360guru** Most Recent 1 year, 1 month ago

Selected Answer: C

Option C
upvoted 1 times

 **ggrodsckiy** 1 year, 5 months ago

Correct C.
upvoted 1 times

 **NikkyDicky** 1 year, 5 months ago

Selected Answer: C

its a C
upvoted 1 times

 **SmileyCloud** 1 year, 6 months ago

Selected Answer: C

C - no doubt, SQS and CloudFront for processed image retrieval
upvoted 4 times

 **SkyZeroZx** 1 year, 6 months ago

Selected Answer: C

C without doubt
upvoted 1 times

 **shree2023** 1 year, 6 months ago

Selected Answer: C

C indeed
upvoted 1 times

 **MoussaNoussa** 1 year, 6 months ago

C without doubt
upvoted 2 times

 **psyx21** 1 year, 6 months 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.

Correct Answer: A

Community vote distribution

A (59%)

D (41%)

✉  **ggrodskiy** Highly Voted 2 years, 5 months 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 25 times

✉  **ayadmawla** 2 years ago

You need the pause of writing to the old db because of the lag in the replication.

upvoted 1 times

✉  **kgpoj** 1 year, 4 months ago

D is wrong, you should choose A.

look at this blog: <https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/>

In step 4 you do need to pause write

upvoted 2 times

✉  **kgpoj** 1 year, 4 months ago

Sorry, typo, step 4

upvoted 1 times

✉  **totten** Highly Voted 2 years, 2 months ago

Selected Answer: A

You cannot natively convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster. Instead, you can create an Amazon Aurora MySQL replica of the RDS MySQL DB instance:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Replica.html>

<https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/>

upvoted 10 times

✉  **lunt** Most Recent 2 weeks ago

Selected Answer: A

A is the exact way to do it as of DEC2025.

D is the way to describe is but without the lower level details of the exact steps that A actually contains. This is the misdirect - both are actually correct but A is accurate and D is right but not as much detail. Clue is the in D's wording "Convert" - there is no convert feature or function, there is a migration option that starts the process with "Create a replica" or the exact first step in A.

upvoted 1 times

✉ **Blair77** 2 months, 3 weeks ago

Selected Answer: D

For real-time, multi-region read/write access, the Aurora MySQL Global Database with write forwarding is the only AWS-managed solution that meets the requirement.

upvoted 2 times

✉ **fa6d93f** 3 months, 1 week ago

Selected Answer: D

D. Convert the RDS MySQL to Aurora MySQL (which is supported via snapshot conversion). Then, set up an Aurora Global Database with a secondary region (eu-west-1). Enable write forwarding so that writes in the secondary region are forwarded to the primary region. Aurora Global Database provides:

Low latency reads in the secondary region.

Write forwarding: writes from the secondary region are sent to the primary region and replicated back with typical latency under 1 second.

Real-time consistency because the replication is built on the Aurora storage layer.

Both regions can write (via write forwarding) and read with minimal latency.

This meets all requirements:

No downtime during conversion (snapshot conversion to Aurora).

Real-time updates across regions.

Low latency for reads in Europe.

Writes possible in both regions (with write forwarding).

Therefore, option D is the correct solution.

upvoted 2 times

✉ **Soliner_Bilgi_Teknolojileri** 4 months, 1 week ago

Selected Answer: D

Answer D is correct because it converts the existing RDS for MySQL into an Aurora MySQL Global Database, adds eu-west-1 as a secondary Region, and enables write forwarding. This design allows applications in both the US and Europe to write locally while forwarding writes to the primary, ensuring real-time data consistency and low latency access across Regions.

upvoted 3 times

✉ **albert_kuo** 9 months, 3 weeks ago

Selected Answer: D

[us-east-1] [eu-west-1]
| [Aurora Primary] | [Aurora Secondary]
| | |
[US App] [EU App]
| | |
[Writes] [Write Forwarding]

upvoted 1 times

✉ **Peaches35** 12 months ago

Selected Answer: D

Option D is correct because Option A involves additional steps and downtime for promoting the replica and reconfiguring the application. It also does not directly address the need for real-time updates between Regions.

upvoted 2 times

✉ **sashenka** 1 year, 2 months ago

Selected Answer: D

Key Issues with Option A

Unnecessary Complexity and Risk

Option A requires multiple steps including creating a replica, pausing writes, promoting the replica, and reconfiguring the application. Each step introduces potential points of failure and complexity.

The process requires application downtime during the conversion process.

Business Impact

Pausing application writes means service interruption for customers.

The multi-step process extends the duration of service disruption.

Reconfiguring applications multiple times increases the risk of errors.

upvoted 2 times

✉ **sashenka** 1 year, 2 months ago

Changed to A
upvoted 1 times

 **kgpoj** 1 year, 4 months ago
<https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/>

A is correct. You do need to pause write before creating replica.
upvoted 1 times

 **Daniel76** 1 year, 4 months ago

Selected Answer: D

Aurora supports cross-region replication and write forwarding. Only need to promote DB Custer in the failover scenario, not for migration.
upvoted 1 times

 **HelpnoseNse** 1 year, 5 months ago

Selected Answer: D

Vote D.
On top of ggrodskiy's point, standalone DB cluster only support 1 region. If multiple regions are required then DB cluster won't be standalone.
upvoted 2 times

 **seetpt** 1 year, 7 months ago

Selected Answer: A

A for me
upvoted 1 times

 **Russ99** 1 year, 9 months ago

Selected Answer: D

This approach leverages Amazon Aurora's Global Database capability, which allows for a single database to span multiple AWS regions, thus enabling low-latency reads and writes in multiple regions and providing data replication across regions with minimal latency. By converting the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster and enabling write forwarding, the solution supports writes in multiple regions and ensures that the data is synchronized across the regions in real time. This setup allows customers in both the US and Europe to see updates from each other as they happen, meeting the requirement for real-time data consistency and low application latency.

upvoted 3 times

 **LazyAutonomy** 1 year, 11 months ago

Galera + ProxySQL ftw
upvoted 1 times

 **tmlong18** 1 year, 11 months ago

Selected Answer: A

D said 'Convert' but not 'Mirgrate'. You cannot convert RDS MySQL to Aurora MySQL natively.
upvoted 6 times

 **duriselman** 2 years ago

D CORRECT
D. Aurora Global Database with Write Forwarding:

This solution addresses all requirements:

Real-time data access and updates: Aurora provides global secondary databases in the chosen region (eu-west-1) for low latency and consistent data.

Minimal downtime: Aurora automatically handles failovers and data synchronization between regions.

Write forwarding: Both regions can perform write operations, ensuring real-time updates for all users.

High availability: Aurora offers automatic backups and failover capabilities.

Therefore, D. Converting the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster with a secondary Region in eu-west-1 and enabling write forwarding is the most suitable solution. It meets all requirements for data availability, minimal latency, real-time updates, and high availability for both US and European customers.

upvoted 3 times

 **ayadmawla** 2 years ago

The first statement in D ("Convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster.") is wrong, therefore D is wrong. The multiple choice is based on these tricks. Real life is a different matter when we say "Convert" to mean go through the process of replacing by replicating, etc.

upvoted 1 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.

Correct Answer: B

Community vote distribution

B (86%)

14%

 **SkyZeroZx**  2 years, 5 months 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 7 times

 **SmileyCloud**  2 years, 6 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 5 times

 **JoeTromundo**  1 year, 2 months ago

Selected Answer: B

<https://repost.aws/knowledge-center/aws-sftp-endpoint-type>
upvoted 2 times

 **Syre** 1 year, 3 months ago

Selected Answer: A

B is wrong, it's similar to A but uses a VPC-hosted endpoint, which is unnecessary for this public-facing scenario and adds complexity without any clear benefit.
upvoted 1 times

✉  **duriselvan** 2 years ago

<https://docs.aws.amazon.com/transfer/latest/userguide/create-server-in-vpc.html> -b ans
upvoted 2 times

✉  **duriselvan** 2 years ago

S Fargate and a Network Load Balancer provides the most efficient and secure solution, meeting all the requirements without compromising availability, introducing unnecessary complexity, or disrupting existing customer access.
upvoted 1 times

✉  **career360guru** 2 years, 1 month ago

Selected Answer: B

Option B
upvoted 1 times

✉  **rif** 2 years, 2 months ago

Answer is B.
<https://aws.amazon.com/blogs/storage/use-ip-whitelisting-to-secure-your-aws-transfer-for-sftp-servers/>
upvoted 1 times

✉  **NikkyDicky** 2 years, 5 months ago

Selected Answer: B

B of course. need SG to whitelist IPs
upvoted 1 times

✉  **YodaMaster** 2 years, 5 months ago

Selected Answer: B

<https://repost.aws/knowledge-center/aws-sftp-endpoint-type>
upvoted 2 times

✉  **ozelllll** 2 years, 6 months ago

Selected Answer: B

It's B: <https://repost.aws/knowledge-center/aws-sftp-endpoint-type>
upvoted 4 times

✉  **gd1** 2 years, 6 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** 2 years, 6 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** 2 years, 6 months ago

Selected Answer: A

Correct Answer is A
upvoted 3 times

✉  **rxhan** 2 years, 4 months ago

again wrong, dont be quick and wrong.
upvoted 2 times

Question #291

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.

Correct Answer: B

Community vote distribution

B (96%)	4%
---------	----

 **softarts** Highly Voted 1 year, 10 months 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 6 times

 **kejam** Most Recent 1 year, 5 months ago

Selected Answer: B

Answer B:
<https://docs.aws.amazon.com/batch/latest/userguide/best-practices.html>
 upvoted 2 times

 **Niko13** 1 year, 6 months ago

Selected Answer: B

Correct Answer is B
 upvoted 1 times

 **career360guru** 1 year, 7 months ago

Selected Answer: B

B is right answer. In C in addition to 3 year reserved instances NLB is extra cost.
 upvoted 4 times

 **career360guru** 1 year, 7 months ago

Compared to on-demand, Reserved instances can be upto 73% reduction but Spot can go upto 90%.
 upvoted 2 times

 **hglopes** 1 year, 10 months 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** 1 year, 11 months ago

Selected Answer: B

its a B

upvoted 1 times

 **SmileyCloud** 2 years 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 4 times

 **easytoo** 2 years ago

b-b-b-b-b-b-b

upvoted 2 times

 **gd1** 2 years ago

Selected Answer: B

S3 + Batch with SOT servers

upvoted 2 times

 **Don2021** 2 years ago

Support B as answer. MOST cost effective

upvoted 1 times

 **psyx21** 2 years ago

Selected Answer: B

Correct Answer is B

upvoted 2 times

Question #292

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.

Correct Answer: A*Community vote distribution*

A (90%)	10%
---------	-----

 **bhanus**  2 years, 6 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 8 times

 **AgboolaKun**  3 months, 1 week ago

Selected Answer: A

A is the correct answer here.

B is wrong because public endpoint for Transfer Family doesn't provide static IP addresses for vendor allowlisting.

upvoted 1 times

 **3967974** 5 months, 2 weeks ago

Selected Answer: B

Public endpoint configuration is on Transfer Family server and not on VPC. So Answer is B and A. A VPC Endpoint is a service that allows resources within your VPC to connect to other AWS services privately.

upvoted 1 times

 **Syre** 1 year, 3 months ago

Selected Answer: B

A is wrong. The use of an internet-facing VPC endpoint for AWS Transfer Family is not necessary here. The publicly accessible endpoint provided by AWS Transfer Family itself meets the requirement for external access. Also, assigning Elastic IPs to subnets is unnecessary because AWS Transfer Family manages public IPs.

upvoted 2 times

 **duriselvan** 2 years ago

a IS ANS

Here's why this solution is optimal:

Managed SFTP: AWS Transfer Family eliminates the need to manage and maintain SFTP servers, reducing operational overhead compared to EC2-based solutions.

High availability: It provides built-in high availability, ensuring continuous access to SFTP services even in case of component failures.

Static IP addresses: The internet-facing VPC endpoint with Elastic IP addresses provides fixed IPs for external vendors, meeting their security requirements.

Secure file storage: EFS offers a managed, scalable, and highly available file system, ensuring secure file storage and access for downstream applications.

NFS compatibility: EFS integrates seamlessly with NFS, allowing easy migration of downstream applications to the new file system.

upvoted 3 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

Option A

upvoted 2 times

 **ggrodskiy** 2 years, 5 months ago

Correct A.

upvoted 2 times

 **Jonalb** 2 years, 5 months ago

Selected Answer: A

AAAAAAA

upvoted 2 times

 **NikkyDicky** 2 years, 5 months ago

Selected Answer: A

its an A.. static IPs

upvoted 1 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: A

It's A. You can't have elastic IP with B.

upvoted 2 times

 **Jonalb** 2 years, 6 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 3 times

 **Alabi** 2 years, 6 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 3 times

 **gd1** 2 years, 6 months ago

Selected Answer: A

A is correct for Pvt IP addresses.

upvoted 1 times

 **bhanus** 2 years, 6 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** 2 years, 6 months ago

Selected Answer: A

Correct Answer is A

upvoted 2 times

Question #293

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.

Correct Answer: A
Community vote distribution

A (88%) 13%

 **YodaMaster** Highly Voted 2 years, 5 months ago

This question was painful to read.

upvoted 59 times

 **shaam80** Highly Voted 2 years ago

Selected Answer: A

Answer - A

D is closest, but wrong as you subnets cannot be modified. They have to be deleted and re-created.

upvoted 14 times

 **gmehra** Most Recent 7 months, 4 weeks ago

Selected Answer: D

Option D is the best solution as it allows the adoption of the new AZ without adding additional IPv4 address space and without service downtime. It carefully reallocates the existing subnets' address space across the three AZs while ensuring that the Auto Scaling group maintains healthy instances during each step of the process.

upvoted 1 times

 **youonebe** 1 year, 1 month ago

Selected Answer: D

D is the answer.

upvoted 1 times

 **Syre** 1 year, 3 months ago

Selected Answer: D

A is wrong. It involves a complex process of deleting and recreating subnets, which could lead to downtime and operational complexity. Also, the approach of creating new subnets from the old address space is risky and can be prone to errors.

upvoted 1 times

 **duriselvan** 2 years ago

D is ans
ere's why this option is the most suitable:

Minimal downtime: It minimizes downtime by gradually shifting instances between subnets within the same VPC, ensuring continuous connectivity to the on-premises environment.

No additional address space: It utilizes the existing IPv4 address space by splitting the subnets, avoiding the need for additional resources.

Phased approach: It implements the changes in manageable steps, minimizing risk and allowing for rollback if necessary.

upvoted 2 times

 **gary_gary** 2 years, 1 month ago

For the CIDR range, what's after '-'? Is something missing?

upvoted 1 times

 **Mikado211** 2 years, 1 month ago

Selected Answer: A

B do not follow the need of no downtime

C will force you to migrate to a new CIDR

A and D are similar except that in A you recreate the subnets while in D you update the subnets.
But you cannot update the subnets, you have to remove and recreate them.

So A is the correct answer.

upvoted 9 times

 **totten** 2 years, 2 months ago

Selected Answer: A

In a scenario where you must add a new AZ without service downtime, option A, which progressively transitions to new subnets in the new AZ while keeping the existing infrastructure running, is a better choice. This approach ensures high availability and minimal disruption to your services.

Option D is not correct. You cannot update the CIDR block of an existing Amazon VPC subnet without recreating it.

upvoted 4 times

 **Blingy** 2 years, 3 months 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 2 times

 **Arnaud92** 2 years, 3 months 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** 2 years, 4 months 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 years, 5 months ago

Selected Answer: A

A. can't update subnet

upvoted 3 times

 **Christina666** 2 years, 5 months ago

These answers are big pain to read

upvoted 5 times

 **SmileyCloud** 2 years, 6 months ago

Selected Answer: A

A - Correct. You can't modify subnet as D says.

upvoted 2 times

 **nexus2020** 2 years, 6 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 intrupption

C: is a joke.....

upvoted 4 times

 **Jackhemo** 2 years, 6 months ago

Selected Answer: A

olabiba.ai says "A". Chatgpt kept bouncing between "B" & "D".

upvoted 1 times

Question #294

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.

Correct Answer: A

Community vote distribution

A (100%)

 **bhanus** Highly Voted 2 years 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 7 times

 **SmileyCloud** 1 year, 11 months ago

The tags are different for each OU.

upvoted 5 times

 **ayadmawla** Highly Voted 1 year, 6 months ago

Selected Answer: A

The key to the answer is in the first sentence of A and B. You can create a Tag Policy in the Management Account not OU since the OU is not an "Account" but a target where a policy is applied. Tag Policy is not the same as an SCP.

See: <https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>

upvoted 7 times

 **Mikado211** Most Recent 1 year, 7 months ago

Ok this is strange if you do not use this stuff regularly as AWS uses "tag policy" for several different configuration services.

You can apply a tag policy on the management account through AWS Organization. If you do it all child OUs will inherit the tag policy.

If you do the same "tag policy" on the management account using AWS Resource Groups Tag Editor it will not be inherited.

B was a very seductive answer, even chatGPT made a mistake here by defining this answer as good in first occurrence.

But considering we use AWS Organization to manage everything, it's clearly an AWS Organization Tag Policy which is used here. So a tag policy applied on the management account will be inherited by the child OUs.

Answer is A.

AWS terminology can be really bad.

upvoted 1 times

 **ggrodskiy** 1 year, 11 months ago

Correct A.

upvoted 1 times

 **NikkyDicky** 1 year, 11 months ago

Selected Answer: A

A. tag policy create in management account
upvoted 3 times

 **SkyZeroZx** 1 year, 12 months 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 clouformation ? is incorrect in this case
D) AWS Service Catalog ? why ? incorrect
upvoted 2 times

 **SmileyCloud** 2 years 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** 2 years ago

Selected Answer: A

AAAAAAAAAAAAAA
upvoted 1 times

 **jubileu84** 2 years ago

Correct Answer is A
upvoted 1 times

 **SkyZeroZx** 2 years 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** 2 years ago

Selected Answer: A

olabiba.ai says 'A'
upvoted 1 times

 **psyx21** 2 years ago

Selected Answer: A

Correct Answer is A
upvoted 1 times

 **bmdf** 2 years ago

Selected Answer: A

What not use SCP?
upvoted 1 times

Question #295

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.

Correct Answer: C*Community vote distribution*

C (62%)

B (34%)

 **SmileyCloud** Highly Voted 2 years, 6 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 16 times

 **titi_r** 1 year, 8 months ago

I've tested it myself in the AWS Console – correct answer is "B". To change the instance type you have 3 options, and all of them require modifying the ASG's config:

1. Create a new revision of the current launch template, then change the ASG config to use it.
2. Create a new launch template, then change the ASG config to use it.
3. Use the option "Override launch template" in the ASG config.

If you only create a new revision of the launch template, the ASG will continue to use the old revision. The state that you cannot change the instance type from the ASG config is NOT true and anybody can verify it in the AWS Console.

upvoted 7 times

 **helloworldabc** 1 year, 4 months ago

just C

upvoted 1 times

 **LazyAutonomy** Highly Voted 1 year, 11 months ago

Selected Answer: B

The answer used to be C, but now it's B. But not for the reasons others here have mentioned. The question states that "The Auto Scaling group configuration uses only one type of instance". This implies the ASG config has implemented instance overrides, which - you guessed it - overrides the instance type that's specified in the launch template. You could cut new versions of launch templates until you're blue in the face, it won't make a lick of difference if the ASG config is overriding the instance type. And because ASGs can be modified, I reckon that puts a nail in C's coffin, making B the new correct answer. I think this is the first question (out of 400+) where the moderator-selected solution was correct and the community-voted solution was incorrect.

upvoted 8 times

 **fartosh** 1 year, 6 months ago

I believe "The Auto Scaling group configuration uses only one type of instance." is just a badly phrased sentence and the question designer only meant that instances running under AutoScaling Group are of one instance type. I understand the sentence as a suggestion to improve the state by specifying multiple types instead.

Apart from the wording, there's nothing wrong with answer C. It lets you stop worrying about the future instance generations, too, compared to B where you have to modify the instance type whenever a new generation is released. Also, as specific instance types can be temporarily unavailable (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-capacity>), C can smoothly use another available instance automatically.

upvoted 2 times

 **ciscochamps** Most Recent 3 months, 1 week ago

Selected Answer: B

Answer is B

upvoted 1 times

✉ **Soliner_Bilgi_Teknolojileri** 4 months, 1 week ago

Selected Answer: B

B is correct because it follows rightsizing best practices: choosing an instance type that matches the actual CPU and memory usage. This directly lowers cost and increases utilization, while requiring the least ongoing configuration changes.

upvoted 1 times

✉ **Curious76** 5 months, 3 weeks ago

Selected Answer: C

With EC2 Attribute-based Instance Selection (ABIS), you can:

Define desired vCPU, memory, and other instance characteristics (e.g., architecture, burstable/non-burstable).

Let EC2 automatically choose instance types that match those attributes.

Auto Scaling automatically selects the best available instance type, considering price and availability.

This eliminates the need to manually maintain a list of instances — it adapts as AWS adds or removes instance types.

Least configuration maintenance.

Improves cost-efficiency.

Improves resilience to Spot or On-Demand availability changes.

upvoted 2 times

✉ **LuongTo** 1 year ago

Selected Answer: C

A out since "similar" still be under utilized.

B reported information about utilization look sexy, B is feasible, but specify "an instance type" would not be flexible as C

C using launch template, specify CPU and memory instead of instance type => AWS will select suitable instance type, this is for the "future" requirement

D seems overkill

upvoted 1 times

✉ **Syre** 1 year, 3 months ago

Selected Answer: A

Why Option C is Less Optimal:

Single Instance Type Limitation: By specifying CPU and memory requirements for a single instance type, you limit the flexibility of your Auto Scaling group. If the chosen instance type does not fully match the application's varying load, it may result in either underutilization or performance issues.

No Cost Optimization: This option does not take advantage of cost differences among different instance types. Without multiple instance types, you miss out on opportunities to select more cost-effective options based on current pricing and utilization needs.

Future Configuration Changes: While specifying the right instance type initially is good, it doesn't address changing application requirements or price fluctuations over time. It could still require adjustments in the future if the chosen instance type becomes less cost-effective or if application requirements change.

upvoted 1 times

✉ **tgv** 1 year, 4 months ago

Selected Answer: B

Perhaps it's an older question that AWS intended for us to solve using C.

But nowadays days its B for the reasons explained by some of the people in this thread.

I would be really surprised to see this question in the exam, but if I will - I'll definitely go with B

upvoted 1 times

✉ **053081f** 1 year, 5 months ago

Selected Answer: A

Correct answer is A:

This solution allows for a mix of instance types, which can help optimize costs and increase utilization.

By using similar instance types, it ensures compatibility with the application's requirements.

This approach requires the least number of configuration changes in the future as it provides flexibility to automatically use different instance types as they become available or as prices change.

B. This option limits the Auto Scaling group to a single instance type again, which doesn't provide flexibility for future changes.
C. Specifying CPU and memory requirements without instance types may lead to unexpected instance selections and potential compatibility issues.

D. Using a script with the AWS Price List Bulk API could lead to frequent changes and may select instance types that aren't optimal for the application's needs.

upvoted 2 times

✉ **seetpt** 1 year, 7 months ago

Selected Answer: C

C for me
upvoted 2 times

 titi_r 1 year, 8 months ago

Selected Answer: B
I've tested it myself in the AWS Console – correct answer is "B". To change the instance type you have 3 options, and all of them require modifying the ASG's config:

1. Create a new revision of the current launch template, then change the ASG config to use it.
2. Create a new launch template, then change the ASG config to use it.
3. Use the option "Override launch template" in the ASG config.

If you only create a new revision of the launch template, the ASG will continue to use the old revision. The state that you cannot change the instance type from the ASG config is NOT true and anybody can verify it in the AWS Console.

upvoted 4 times

 career360guru 1 year, 9 months ago

Selected Answer: C
Option C
upvoted 3 times

 adelyn||||||| 1 year, 10 months ago

C:

Auto scaling group is built on top of launch template, you can reference AMI in template, but not in auto scaling group

upvoted 1 times

 igor12ghsj577 1 year, 10 months ago

AWS does not allow to edit launch configuration. If you notice, we define instance type at time of launch configuration. So if you want to change instance type in Auto Scaling group than you need to create new launch configuration for that.

upvoted 2 times

 tmlong18 1 year, 11 months ago

Selected Answer: B
C is wrong.

Let's assume a scenario where the optimal hardware requirement for a program under load is 4GB of RAM for every 1 CPU.

However, you have specified only one type of instance with 1CPU and 1GB RAM.

Even if you choose Option C and apply load balancing, having 4 instances of 1CPU and 1GB RAM (totaling 4CPU and 4GB RAM) will still result in an issue of low CPU utilization.

upvoted 2 times

 ayadmaawla 2 years ago

Selected Answer: C
Key to the Answer is "Modify". Launch templates are immutable; after you create a launch template, you can't modify it. Instead, you can create a new version of the launch template that includes any changes you require.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/manage-launch-template-versions.html>
upvoted 6 times

 duriselvan 2 years ago

b IS ANS
Minimal configuration changes: This solution only requires modifying the Auto Scaling group configuration to add the new, more efficient instance type and remove the old, underutilized type. This minimizes future maintenance and reduces the risk of introducing errors.

Scalability and flexibility: The Auto Scaling group will automatically scale up and down based on demand, even with the new instance type. This ensures high availability and cost-effectiveness.

Future-proof: This approach doesn't rely on specific instance types or the AWS Price List Bulk API, making it more adaptable to future changes and updates in the AWS ecosystem.

upvoted 1 times

Question #296

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.

Correct Answer: D*Community vote distribution*

D (49%)	C (48%)	4%
---------	---------	----

 **finesse_999**  2 years, 4 months 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 27 times

 **mike5656** 1 year ago

agree with titi_r
upvoted 1 times

 **backtorod** 2 years, 2 months ago

Agreed
upvoted 1 times

 **titi_r** 1 year, 8 months ago

"C" does not mention a restore operation at all. Where will Route 53 route the traffic in the secondary Region: to the DB snapshots in the AWS Backup vault maybe?
So, D should be the right option.

P.S. Very badly written question btw.

upvoted 4 times

 **chico2023**  2 years, 4 months 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 7 times

 **helloworldabc** 1 year, 4 months ago

just D
upvoted 1 times

 **Halliphax** 1 year, 1 month ago

just C

upvoted 1 times

 **EzKkk** Most Recent 1 month, 2 weeks ago

B is the correct answer, this solution is a classic Pilot Light solution for DR.

First, we have to identify the possible failure point of this system and obviously, they are Aurora and DynamoDB.

- For Aurora, instead of using expensive global db option, we can use Aurora Serverless option in secondary region and let it auto pause when no traffic is received. We then use DMS job to periodically sync data between primary region and secondary region.

- For DynamoDB, we can also create a regional setup and trigger UpdateItem API to sync data.

When the primary region goes out, the secondary region lit up and Route 53 point traffic to healthy region.

upvoted 1 times

 **Blair77** 2 months, 3 weeks ago

Selected Answer: D

For multi-region, near-real-time DR with 2-hour RPO and 4-hour RTO, the managed multi-region replication features (Aurora Global DB + DynamoDB Global Tables) + Route 53 failover is the simplest and most cost-effective solution.

upvoted 1 times

 **ciscochamps** 3 months, 1 week ago

Selected Answer: C

C obviously

upvoted 1 times

 **fa6d93f** 3 months, 1 week ago

Selected Answer: D

Option D is the most cost-effective solution that reliably meets the 2-hour RPO and 4-hour RTO requirements. It uses Aurora global database and DynamoDB global tables for low-latency replication, ensuring minimal data loss and fast recovery. Route 53 failover is sufficient for switching traffic within the RTO, and it avoids the additional cost of CloudFront (used in Option A). While Option B is cheaper, its custom replication introduces complexity and risk, making Option D the better balance of cost, reliability, and simplicity.

upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 4 months, 1 week ago

Selected Answer: C

C is correct because cross-Region AWS Backup provides the cheapest solution that still meets the requirements: backups every 2 hours satisfy the RPO, and restoring infrastructure and data within 4 hours satisfies the RTO — without the high ongoing cost of continuous replication.

upvoted 1 times

 **studybuddy12** 6 months, 3 weeks ago

Selected Answer: D

D. Near real-time replication with Aurora global database and DynamoDB global tables, easily meeting the 2-hour RPO.

Quick failover capability with Route 53, meeting the 4-hour RTO.

A more cost-effective solution compared to option A (no CloudFront costs) and option B (no need for custom replication setup with DMS, EventBridge, and Lambda).

upvoted 2 times

 **albert_kuo** 9 months, 3 weeks ago

Selected Answer: D

AWS Backup has the lowest cost but cannot fulfill RTO requirement.

upvoted 2 times

 **PSPaul** 11 months, 3 weeks ago

Selected Answer: D

I voted for D.

While option C (using AWS Backup) might seem cost-effective, it may not consistently meet RTO/RPO requirements, especially for large datasets. The reliability of AWS Backup, while generally good, cannot guarantee meeting specific recovery time and recovery point objectives.

The question might be designed to trick you into choosing the cheapest option, but a reliable disaster recovery solution is crucial. Therefore, I chose option D."**

upvoted 3 times

 **SIJUTHOMASP** 1 year ago

Selected Answer: C

I think we need to assume the ideal situation whenever there is no specific mention about the database size. In ideal situation 2 hours is more than sufficient to take backup. Since the question has the key for cost-effectiveness, the answer would be C. In addition, there are multiple options available to expedite the recovery from backup if the normal path can't meet RTO.

upvoted 2 times

 **sashenka** 1 year, 2 months ago

Selected Answer: D

Why AWS Backup (Option C) May Not Be Suitable:

Cross-region snapshot copies "can take hours to complete" depending on database size and regions involved. Since the database size is unknown Cross-region copies have variable completion times. We need to guarantee an RPO of 2 hours. AWS Backup cannot reliably guarantee the 2-hour RPO requirement due to these uncertainties.

Better Solution:

Aurora Global Database (Option D) would be more appropriate because:

It provides replication lag of typically less than 1 second, easily meeting the 2-hour RPO requirement. It enables fast global failover to secondary regions in minutes, meeting the 4-hour RTO requirement. Route 53 failover routing provides automated traffic switching during recovery. While Aurora Global Database may be more expensive than AWS Backup, it's the only solution among the options that can definitively guarantee meeting both the RPO and RTO requirements regardless of database size. Therefore, Option D is the correct choice as it's the only solution that can reliably meet both the RPO and RTO requirements with certainty.

upvoted 2 times

 **AloraCloud** 1 year, 2 months ago

The ONLY reason I am going with C is that AWS Backup is generally more cost-effective compared to continuous replication setups like Aurora Global Database or DynamoDB Global Tables1.

It allows you to create point-in-time backups and restore them in a secondary region, meeting the RPO requirement of 2 hours and RTO requirement of 4 hours

upvoted 1 times

 **tsangckl** 1 year, 4 months ago

Selected Answer: D

vote for D. Global table

upvoted 3 times

 **seetpt** 1 year, 7 months ago

Selected Answer: C

C for me

upvoted 1 times

 **43c89f4** 1 year, 8 months ago

My answer is B.

B is cheapest and it will create only when event occurs. it will complete within 2hours.

C and D are costly options compare to BH

upvoted 1 times

 **bjexamprep** 1 year, 9 months ago

Selected Answer: C

AWS often publish this kind of bad framed question. The question is looking for most cost effective solution. So I believe C is the expected answer even it is not complete answer. But C has three big problems:

1. a backup is a backup, if it doesn't provide a way to restore, it is only a backup and is not a complete DR.

2. It doesn't mention the frequency of the backup nor the continuous backup, which means we don't know whether it can meet the 2hr RPO.

3. It doesn't mention the ECS DR. Well, neither does the other answers.

Aurora global db and DynamoDB global table are apparently more expensive. With the question design, they should be excluded even they are actually complete answers.

upvoted 5 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.

Correct Answer: A

Community vote distribution

A (92%)	8%
---------	----

✉️  **dkx** [Highly Voted ] 2 years, 5 months 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 12 times

✉️  **albert_kuo** [Most Recent ] 9 months, 3 weeks ago

Selected Answer: A

CloudFront does NOT support to specify casing-insensitive query string

upvoted 1 times

✉️  **ChanduWodeyar** 1 year, 6 months ago

Answer:D is best and cheap.

upvoted 1 times

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

just A

upvoted 1 times

✉️  **LazyAutonomy** 1 year, 11 months ago

Selected Answer: C

OMG so now I have to invoke and pay for a Lambda for every single GET request that traverses my CDN? No, F*** that. If D isn't supported then ciao bella s/Cloudfront/Cloudflare/g and say hello to Apache running mod_substitute thank you very much.

upvoted 1 times

✉️  **duriselvan** 2 years ago

Caching based on query string parameters

If you configure CloudFront to cache based on query string parameters, you can improve caching if you do the following:

Configure CloudFront to forward only the query string parameters for which your origin will return unique objects.

upvoted 1 times

✉️  **duriselvan** 2 years ago

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cache-hit-ratio.html>

upvoted 1 times

duriselvan 2 years ago

D is ans

D. Casing-insensitive query string processing:

This is the simplest and fastest solution to implement.

It will treat requests with the same query string but different character casing as identical, boosting the cache hit ratio.

It utilizes built-in functionality of CloudFront without requiring additional services or configurations.

Remember, while other options might offer additional functionalities, the primary goal is to quickly improve the cache hit ratio. Specifying casing-insensitive query string processing achieves this with minimal impact and complexity.

upvoted 1 times

ggrodskiy 2 years, 5 months ago

Correct A.

upvoted 2 times

NikkyDicky 2 years, 5 months ago

Selected Answer: A

its an A

D would be nice if was supported

upvoted 2 times

SmileyCloud 2 years, 6 months ago

Selected Answer: A

A - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examples-normalize-query-string-parameters>

upvoted 3 times

SmileyCloud 2 years, 6 months ago

A - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examples-normalize-query-string-parameters>

upvoted 1 times

nexus2020 2 years, 6 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 2 years, 6 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 2 years, 6 months ago

Selected Answer: A

A is the answer -to sort parameters by name and force them to be lowercase

upvoted 2 times

bhanus 2 years, 6 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 2 years, 6 months ago

A is answer

upvoted 1 times

psyx21 2 years, 6 months ago

Selected Answer: A

Correct Answer is A

upvoted 1 times

Question #298

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.

Correct Answer: C*Community vote distribution*

C (61%)	A (30%)	9%
---------	---------	----

 **YodaMaster** Highly Voted 2 years, 5 months 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 33 times

 **yog927** 1 year, 9 months ago

The trick is not to read the question first. Here is what I do:
 1. Read all options.
 2. Eliminate the incorrect ones, and settle on 1 or 2 options.
 3. Scroll through the question last.
upvoted 11 times

 **yorkicurke** 2 years, 2 months ago

any news about your exam?
upvoted 3 times

 **AMYMY** 1 year, 10 months ago

I failed just cuz of time mngmnt ,now I'm here again to give myself one more chance,...:-,(.....
Anyone here's to help me with exam by sharing their experience??
upvoted 1 times

 **07c2d2a** 1 year, 10 months ago

did you actually see any of the same questions on the test?
upvoted 2 times

 **SkyZeroZx** Highly Voted 2 years, 5 months ago

if you got far it means you are persistent, good luck on your exam
upvoted 21 times

 **aka1177** Most Recent 3 weeks ago

Selected Answer: A

Answer is A;
C is incorrect since is not use Full load, but only CDC. Also there is a statement that DB has a lot of writes, So CDC won't manage replication in an hour.
upvoted 1 times

 **Asagumo** 1 month ago

Selected Answer: D

Dは AWS Backup を利用するという記述が抜けています。それも推測するのがプロフェッショナルです。
upvoted 1 times

 **Deztroyer88** 1 month, 1 week ago

Selected Answer: A

C may be most cost effective, but do you have any idea on how long it will take to restore a DB from S3 ?

upvoted 1 times

 **4845c28** 4 months, 1 week ago

Selected Answer: A

C is wrong.

CDC task type only captures changes from source databases after we start the task. This is useful when target already contains up-to-date data.

In option C there is nothing mentioned about backing up database first.

And on top of that using DMS for backing up data is like using fork to eat the soup, technically you can do it but come on

A is wrong because you cannot disable default backups.

Global database may not be the cheapest option but is the only correct one

upvoted 2 times

 **CAIYasia** 8 months, 3 weeks ago

Selected Answer: C

D is wrong. Aurora's built-in automated backups are continuous but not customizable in frequency

upvoted 1 times

 **ahhatem** 1 year ago

Selected Answer: A

I don't know but isn't the exam supposed to be about being a professional architect? What kind of professional architect would recommend C knowing that a 100 things can go wrong in such a solution!

upvoted 1 times

 **0dc6cac** 6 months ago

pretty sure a professional architect would read the question and understand that it's looking for the best cost-effective solution.

upvoted 1 times

 **kgpoj** 1 year, 3 months ago

For those who are voting for D, here are a few simple facts:

- You can't disable Aurora automated backup;

- You can't change Aurora backup frequency - it's automated and point-in-time, you just need to define retention period which is the period for which you can perform a point-in-time recovery (1 day for free, max 35)

upvoted 1 times

 **Daniel76** 1 year, 4 months ago

Between A and C, I choose A.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database-getting-started.html#aurora-global-database-attaching>

For C, note there's high volume of writes daily. Can CDC to S3 bucket in another region keep up with 1-hour RPO? Although C has considered lowest cost for backup, does it consider the time taken to restore to full aurora database in the second region up and running?

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: C

Ask for 1-hour RPO, cheapest

Aurora Global can do 1-second RPO, but expensive

DMS with CDC can do 1-hour RPO and cheaper

upvoted 4 times

 **trungtd** 1 year, 6 months ago

Selected Answer: C

Option A will replicate "the whole database", we only need "data"

upvoted 2 times

 **BrijMohan08** 1 year, 8 months ago

Selected Answer: D

option D provides the most cost-effective solution by leveraging Aurora backups with a 1-hour frequency and cross-Region replication to meet the disaster recovery requirements with the desired RPO.

upvoted 4 times

 **YOUSSEFWAID** 1 year, 8 months ago

Selected Answer: C

RPO is a requirement and not RTO. They are talking about replicating the data in the Aurora database to another Region to meet disaster recovery requirements.

upvoted 1 times

✉️  **TonytheTiger** 1 year, 9 months ago

Selected Answer: A

My head hurts after reading the last 2 questions and 45 mins later, still confuse. I am looking at the key requirements, RPO <1h, meet DR requirements, and LOWEST Cost. After reading the link below and all of the comments, I think Option A fulfills all the requirements in the question.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

upvoted 5 times

✉️  **teo2157** 1 year, 9 months ago

Selected Answer: A

Github copilot

While AWS Database Migration Service (DMS) can be used to replicate ongoing changes from the Aurora database to an Amazon S3 bucket in another region using a change data capture (CDC) task, it's important to note that DMS does not create a standard SQL dump or backup file that can be directly restored to an Aurora database.

The data migrated to S3 by DMS is in Apache Parquet format, a columnar storage file format optimized for speed and for a small footprint. This format is not directly restorable to an Aurora database.

If you need to restore the data to an Aurora database, you would need to use a service like AWS Glue or Amazon Athena to read the data from S3 and then insert it into Aurora. This process could be complex and time-consuming, and might not meet your RPO of 1 hour.

upvoted 6 times

✉️  **sashenka** 1 year, 2 months ago

RTO is not mentioned in the requirements so all we care about is the RPO of the data. We do not care about the format either so long as all the data is there as of an hour or less prior to the disaster.

upvoted 1 times

✉️  **teo2157** 1 year, 9 months ago

Selected Answer: A

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. Is it possible to restore data from the S3 bucket to an Aurora Database?

upvoted 1 times

Question #299

Topic 1

A company's solutions architect is evaluating an AWS workload that was deployed several years ago. The application tier is stateless and runs on a single large Amazon EC2 instance that was launched from an AMI. The application stores data in a MySQL database that runs on a single EC2 instance.

The CPU utilization on the application server EC2 instance often reaches 100% and causes the application to stop responding. The company manually installs patches on the instances. Patching has caused downtime in the past. The company needs to make the application highly available.

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

- A. Move the application tier to AWS Lambda functions in the existing VPC. Create an Application Load Balancer to distribute traffic across the Lambda functions. Use Amazon GuardDuty to scan the Lambda functions. Migrate the database to Amazon DocumentDB (with MongoDB compatibility).
- B. Change the EC2 instance type to a smaller Graviton powered instance type. Use the existing AMI to create a launch template for an Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. Migrate the database to Amazon DynamoDB.
- C. Move the application tier to containers by using Docker. Run the containers on Amazon Elastic Container Service (Amazon ECS) with EC2 instances. Create an Application Load Balancer to distribute traffic across the ECS cluster. Configure the ECS cluster to scale based on CPU utilization. Migrate the database to Amazon Neptune.
- D. Create a new AMI that is configured with AWS Systems Manager Agent (SSM Agent). Use the new AMI to create a launch template for an Auto Scaling group. Use smaller instances in the Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. Migrate the database to Amazon Aurora MySQL.

Correct Answer: D

Community vote distribution

D (100%)

 **Ustad** Highly Voted 1 year, 1 month ago

Selected Answer: D

No development effort needed so no need to migrate nonSQL or to Neptune. and no need to rework it based on lambda.
upvoted 5 times

 **joleneinthebackyard** Most Recent 1 year, 1 month ago

Selected Answer: D

A: No guarantee that the work can finish within 15 minutes limit of Lambda
 B, C: Migrate MySQL to DynamoDB or Neptune? Big no no to migrate to different type of database unless the requirement says so.
 D: Classic architecture: ALB + ASG + EC2, scale based on CPU Utilization for cost optimization. The use of SSM to create AMI for launch template of ASG is correct. Aurora MySQL is compatible with current MySQL database.
upvoted 4 times

 **Mikado211** 1 year, 1 month ago

Selected Answer: D

A - you will spend some time to adapt an old platform to a lamdba function + the application works with mysql not with mongodb
 B - You do not want a smaller instance when you have a performance problem
 C - you will have to readapt a whole application to containerization on ECS which is not even the most flexible virtualization platform even if it theoretically requires less maintenance

 D - The most classic way of migrating such application : you create a new platform, you make the application more scalable by using an ASG + you migrate your MySQL server from an overloaded EC2 instance to a managed service.
upvoted 1 times

 **AM_aws** 1 year, 2 months ago

Selected Answer: D

With least development time, from MySQL to Amazon Aurora MySQL.
upvoted 1 times

 **airgead** 1 year, 2 months ago

Answer: D

Because MySQL Database will be compatible with Aurora MySQL

- A. Lambda is not the correct solution as it will be more development effort
- B. Changing to DynamoDB from MySQL (Relational Database) will be more development effort.
- C. More development effort to convert to Docker.

upvoted 2 times

 **patryk99999** 1 year, 2 months ago

Selected Answer: D

I think D

upvoted 1 times

Question #300

Topic 1

A company is planning to migrate several applications to AWS. The company does not have a good understanding of its entire application estate. The estate consists of a mixture of physical machines and VMs.

One application that the company will migrate has many dependencies that are sensitive to latency. The company is unsure what all the dependencies are. However the company knows that the low-latency communications use a custom IP-based protocol that runs on port 1000. The company wants to migrate the application and these dependencies together to move all the low-latency interfaces to AWS at the same time.

The company has installed the AWS Application Discovery Agent and has been collecting data for several months.

What should the company do to identify the dependencies that need to be migrated in the same phase as the application?

- A. Use AWS Migration Hub and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Turn on data exploration in Amazon Athena. Query the data that is transferred between the servers to identify the servers that communicate on port 1000. Return to Migration Hub. Create a move group that is based on the findings from the Athena queries.
- B. Use AWS Application Migration Service and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Configure Application Migration Service to launch test instances for all the servers that interact with the application. Perform acceptance tests on the test instances. If no issues are identified, create a move group that is based on the tested servers.
- C. Use AWS Migration Hub and select the servers that host the application. Turn on data exploration in Network Access Analyzer. Use the Network Access Analyzer console to select the servers that host the application. Select a Network Access Scope of port 1000 and note the matching servers. Return to Migration Hub. Create a move group that is based on the findings from Network Access Analyzer.
- D. Use AWS Migration Hub and select the servers that host the application. Push the Amazon CloudWatch agent to the identified servers by using the AWS Application Discovery Agent. Export the CloudWatch logs that the agents collect to Amazon S3. Use Amazon Athena to query the logs to find servers that communicate on port 1000. Return to Migration Hub. Create a move group that is based on the findings from the Athena queries.

Correct Answer: A

Community vote distribution

A (93%) 7%

 **Sab**  2 years, 1 month ago

Selected Answer: A

Answer A . Network access analyzer is to validate network usage OF aws services and not on-prem

Migration hub has feature for network visualization and Athena can be used to query data

<https://aws.amazon.com/blogs/mt/using-aws-migration-hub-network-visualization-to-overcome-application-and-server-dependency-challenges/>

<https://aws.amazon.com/about-aws/whats-new/2020/11/aws-migration-hub-includes-network-visualization/>
upvoted 16 times

 **joleneinthebackyard**  2 years, 1 month ago

Selected Answer: A

Architecture pattern is Discovery Service + Migration Hub + Athena for data exploration:
<https://docs.aws.amazon.com/application-discovery/latest/userguide/explore-data.html>

- A: looks fine
- B: AWS Application Migration Service is for lift and shift, not for dependency mapping
- C: Network Access Analyzer only for AWS resources, not for on-prem
- D: not the use case of CloudWatch.

upvoted 7 times

 **AzureDP900**  1 year, 1 month ago

A

- AWS Migration Hub allows you to collect and analyze migration-related data, such as network traffic and server dependencies.
- By selecting the servers that host the application and visualizing the network graph, you can identify other servers that interact with the application.
- Turning on data exploration in Amazon Athena allows you to query the collected data and gain insights into the interactions between servers.

- Querying the data for port 1000 will help you identify servers that communicate using this custom protocol.
 - Returning to Migration Hub and creating a move group based on the findings from the Athena queries ensures that you're moving all relevant dependencies together with the application.
- This approach uses AWS Migration Hub's capabilities to collect, analyze, and visualize migration-related data, making it an efficient and effective way to identify dependencies for migration.

upvoted 1 times

 **Syre** 1 year, 3 months ago

Selected Answer: C

C seems to be more suitable

upvoted 1 times

 **9f02c8d** 1 year, 6 months ago

Option C - identifying Servers Communicating on Port 1000: In the Network Access Analyzer console, you can select the servers that host the application and specify a Network Access Scope of port 1000. This will allow you to identify the servers that communicate with the application using the custom IP-based protocol on port 1000, which are the dependencies that need to be migrated together.

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just A

upvoted 2 times

 **ayadmawla** 2 years ago

Selected Answer: A

See: <https://docs.aws.amazon.com/migrationhub/latest/ug/network-diagram.html>

and <https://aws.amazon.com/about-aws/whats-new/2020/11/aws-migration-hub-includes-network-visualization/>

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

A is right answer.

upvoted 1 times

 **KungLjao** 2 years, 1 month ago

Selected Answer: C

Should work with c

upvoted 1 times

 **airgead** 2 years, 2 months ago

Answer: C

To identify the dependencies that need to be migrated in the same phase as the application, the company can use the AWS Application Discovery Agent data. In this case, the sensitive low-latency communications use a custom IP-based protocol that runs on port 1000. The goal is to find servers that communicate on port 1000. Option C would be the most appropriate approach

upvoted 3 times

Question #301

A company is building an application that will run on an AWS Lambda function. Hundreds of customers will use the application. The company wants to give each customer a quota of requests for a specific time period. The quotas must match customer usage patterns. Some customers must receive a higher quota for a shorter time period.

Which solution will meet these requirements?

- A. Create an Amazon API Gateway REST API with a proxy integration to invoke the Lambda function. For each customer, configure an API Gateway usage plan that includes an appropriate request quota. Create an API key from the usage plan for each user that the customer needs.
- B. Create an Amazon API Gateway HTTP API with a proxy integration to invoke the Lambda function. For each customer configure an API Gateway usage plan that includes an appropriate request quota Configure route-level throttling for each usage plan. Create an API Key from the usage plan for each user that the customer needs.
- C. Create a Lambda function alias for each customer. Include a concurrency limit with an appropriate request quota. Create a Lambda function URL for each function alias. Share the Lambda function URL for each alias with the relevant customer.
- D. Create an Application Load Balancer (ALB) in a VPC. Configure the Lambda function as a target for the ALB. Configure an AWS WAF web ACL for the ALB. For each customer configure a role-based rule that includes an appropriate request quota.

Correct Answer: A*Community vote distribution*

A (88%) 12%

 **ayadmawla**  2 years ago

Selected Answer: A

REST APIs and HTTP APIs are both RESTful API products. REST APIs support more features than HTTP APIs, while HTTP APIs are designed with minimal features so that they can be offered at a lower price. Choose REST APIs if you need features such as API keys, per-client throttling, request validation, AWS WAF integration, or private API endpoints. Choose HTTP APIs if you don't need the features included with REST APIs.

upvoted 10 times

 **career360guru**  2 years, 1 month ago

Selected Answer: A

Option A answer is little confusing because it talks about Quota but not about Throttle limits. Option B mentions route-level throttling that is also not correct. Route-level throttling can not be applied at per user basis.
So option A is right answer.

upvoted 5 times

 **AzureDP900**  1 year, 1 month ago

A

This approach allows you to create a separate API Gateway instance for each customer, which enables you to implement quotas at the API level.

By using a proxy integration, you can invoke the Lambda function on behalf of each customer, while still enforcing their individual quota limits.

Configuring an API Gateway usage plan and creating an API key for each user within a customer's organization allows you to manage and enforce quotas for each user separately.

This solution is particularly well-suited for managing multiple customers with different quota requirements. By using API Gateway, you can create separate APIs for each customer, which enables fine-grained control over quota enforcement at the client level.

upvoted 1 times

 **Andres123456** 2 years, 1 month ago

Selected Answer: A

Option A

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

upvoted 2 times

 **Sab** 2 years, 1 month ago

Selected Answer: B

In order to achieve "Some customers must receive a higher quota for a shorter time period.", throttling should be set with rate and burst can be set using Throttling

upvoted 3 times

 **albert_kuo** 9 months, 3 weeks ago

Amazon API Gateway HTTP API does not support usage plan

upvoted 1 times

 **gonzales** 2 years, 1 month ago

Selected Answer: A

Option A

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

upvoted 4 times

 **KungLjao** 2 years, 1 month ago

Selected Answer: A

Its A, you dont need route level throttling

upvoted 1 times

 **Jun_W** 2 years, 2 months ago

Option B

route-level throttling for each usage plan

upvoted 1 times

 **AM_aws** 2 years, 2 months ago

Selected Answer: A

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

HTTP API doesn't include USAGE feature.

upvoted 1 times

 **airgead** 2 years, 2 months ago

Option A

Create REST API with Proxy Integration and for each customer set the usage plan and Create API Key.

<https://medium.com/geekculture/api-key-and-usage-plan-integration-with-aws-api-gateway-2d07bbb9a2a4>

upvoted 1 times

Question #302

Topic 1

A company is planning to migrate its on-premises VMware cluster of 120 VMs to AWS. The VMs have many different operating systems and many custom software packages installed. The company also has an on-premises NFS server that is 10 TB in size. The company has set up a 10 Gbps AWS Direct Connect connection to AWS for the migration.

Which solution will complete the migration to AWS in the LEAST amount of time?

- A. Export the on-premises VMs and copy them to an Amazon S3 bucket. Use VM Import/Export to create AMIs from the VM images that are stored in Amazon S3. Order an AWS Snowball Edge device. Copy the NFS server data to the device. Restore the NFS server data to an Amazon EC2 instance that has NFS configured.
- B. Configure AWS Application Migration Service with a connection to the VMware cluster. Create a replication job for the VMS. Create an Amazon Elastic File System (Amazon EFS) file system. Configure AWS DataSync to copy the NFS server data to the EFS file system over the Direct Connect connection.
- C. Recreate the VMs on AWS as Amazon EC2 instances. Install all the required software packages. Create an Amazon FSx for Lustre file system. Configure AWS DataSync to copy the NFS server data to the FSx for Lustre file system over the Direct Connect connection.
- D. Order two AWS Snowball Edge devices. Copy the VMs and the NFS server data to the devices. Run VM Import/Export after the data from the devices is loaded to an Amazon S3 bucket. Create an Amazon Elastic File System (Amazon EFS) file system. Copy the NFS server data from Amazon S3 to the EFS file system.

Correct Answer: B

Community vote distribution

B (95%)	5%
---------	----

 **Ustad** Highly Voted 2 years, 1 month ago

Selected Answer: B

I'll go with B as 10G direct connection is faster than enough for workload not so big.
EFS and DataSync are feasible as well.

upvoted 8 times

 **saptati** Most Recent 11 months, 2 weeks ago

Selected Answer: B

B is correct. Let's assume, the total data to transfer is 22,240 GB ($120 \text{ VMs} \times 100 \text{ GB}$ [each estimated average size] = 12,000 GB and 10,240 GB for NFS data). Using a 10 Gbps Direct Connect link, the theoretical transfer speed is 1.25 GB/s, and accounting for 80% efficiency due to overhead, the effective speed is 1.0 GB/s. The estimated transfer time is $22,240 \text{ GB} \div 1.0 \text{ GB/s} = 22,240 \text{ seconds}$, or about 6.18 hours. Therefore, the migration can be completed in approximately 6 hours and 10 minutes, leveraging high-speed connectivity and efficient AWS migration services.

A, C, and D are incorrect: A and D involve longer migration times due to delays from physical shipment and multiple processing steps, while C is incorrect because a manual process would take significantly longer than automated migration tools.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Option B is the best solution because it:

- Uses AWS Application Migration Service (also known as Storage Gateway), which is designed for high-speed and low-latency data transfer between on-premises infrastructure and AWS.
- Replicates the VMs with all their software packages installed, ensuring a complete migration with no additional configuration required.
- Creates an Amazon EFS file system to store the NFS server data, which is a highly available and scalable file storage service that can be easily scaled up or down as needed.
- Uses AWS DataSync to copy the NFS server data from the on-premises infrastructure to the EFS file system over the Direct Connect connection.

This approach ensures a complete and fast migration of all VMs and data to AWS, with minimal downtime and configuration required.

upvoted 1 times

 **titi_r** 1 year, 8 months ago

Selected Answer: D

Ans D.

The questions states "The VMs have many different operating systems and many custom software packages installed". However, the AWS AMS supports only limited and commonly used OSes and apps.

Q: What operating systems and applications are supported by AWS Application Migration Service?

AWS Application Migration Service allows you to migrate physical, virtual, and cloud source servers to AWS for a variety of supported operating systems (OS). AWS Application Migration Service supports commonly used applications such as SAP, Oracle, and Microsoft SQL Server.

<https://aws.amazon.com/application-migration-service/faqs/#:~:text=AWS%20Application%20Migration%20Service%20allows,Oracle%2C%20and%20Microsoft%20SQL%20Server>.
upvoted 1 times

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

just B

upvoted 1 times

✉ **Dgix** 1 year, 9 months ago

Selected Answer: B

A is too time-consuming.
B is viable
C is viable, but overengineered as the DC connection has enough capacity.
upvoted 1 times

✉ **Dgix** 1 year, 9 months ago

Typo:

C is too time-consuming

D is viable, but overengineered as the DC connection has enough capacity.

upvoted 1 times

✉ **ftaws** 1 year, 11 months ago

10Gbps = 1.25GB/s = 4.5TB/H

upvoted 1 times

✉ **career360guru** 2 years, 1 month ago

B is the right answer

upvoted 2 times

✉ **Andres123456** 2 years, 1 month ago

Selected Answer: B

Option B.
10 Gbps AWS Direct Connect connection
upvoted 4 times

✉ **KungLjao** 2 years, 1 month ago

Selected Answer: B

B, 13mins to transfer 10tb
upvoted 3 times

✉ **carpa_jo** 1 year, 12 months ago

More like 2.5 hrs, but still a lot faster than shippings Snowballs back and forth...

upvoted 2 times

✉ **Jun_W** 2 years, 2 months ago

Option B.

10 Gbps AWS Direct Connect connection
upvoted 4 times

✉ **airgead** 2 years, 2 months ago

Option D is the correct answer by using Snowball Edge each have 80TB capacity.

A - Does not make sense to use only 1 Snowball Edge, also NFS to NFS server in EC2 it is not correct! Use AWS EFS

B - Using Replication will be slow, there is not parellasim especially with additional NFS data transfer

C - Install required software, as it is custom software, it may be time consuming os 120 VMs

upvoted 2 times

Question #303

Topic 1

An online survey company runs its application in the AWS Cloud. The application is distributed and consists of microservices that run in an automatically scaled Amazon Elastic Container Service (Amazon ECS) cluster. The ECS cluster is a target for an Application Load Balancer (ALB). The ALB is a custom origin for an Amazon CloudFront distribution.

The company has a survey that contains sensitive data. The sensitive data must be encrypted when it moves through the application. The application's data-handling microservice is the only microservice that should be able to decrypt the data.

Which solution will meet these requirements?

- A. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a field-level encryption profile and a configuration. Associate the KMS key and the configuration with the CloudFront cache behavior.
- B. Create an RSA key pair that is dedicated to the data-handling microservice. Upload the public key to the CloudFront distribution. Create a field-level encryption profile and a configuration. Add the configuration to the CloudFront cache behavior.
- C. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the KMS key to encrypt the sensitive data.
- D. Create an RSA key pair that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the private key of the RSA key pair to encrypt the sensitive data.

Correct Answer: B

Community vote distribution

B (86%)

11%

 **gonzales** Highly Voted 2 years, 1 month ago

Selected Answer: B

Please have a look at: <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html> steps:

- Get a public key-private key pair
- Create a field-level encryption profile
- Create a field-level encryption configuration
- Link to a cache behavior

An RSA key pair includes a private and a public key (asymmetric)

upvoted 15 times

 **career360guru** Highly Voted 2 years, 1 month ago

Selected Answer: B

You need to RSA key for Field level Encryption and not KMS Symmetric Key so B is the right answer

upvoted 7 times

 **TomTom** Most Recent 1 year ago

Selected Answer: C

Why not C?

By using KMS and Lambda@Edge, you can ensure that sensitive data is encrypted both at rest and in transit, providing a robust and secure solution for your distributed application.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Here's why option B works:

Creating an RSA key pair allows you to generate a public-private key pair, where the private key is used for decryption and the public key is used for encryption.

Uploading the public key to CloudFront allows the distribution to use this key to encrypt sensitive data as it moves through the application.

Using field-level encryption with CloudFront and Amazon S3 ensures that only the data-handling microservice (which has access to the private key) can decrypt the sensitive data.

upvoted 1 times

 **Chakanetsa** 1 year, 3 months ago

Selected Answer: B

The following steps provide an overview of setting up field-level encryption. For specific steps, see Set up field-level encryption.

- Get a public key-private key pair.
- Create a field-level encryption profile
- Create a field-level encryption configuration.
- Link to a cache behavior.

upvoted 2 times

 **9f02c8d** 1 year, 6 months ago

Option B - field-level encryption requires public/private key pair

upvoted 3 times

 **VerRi** 1 year, 9 months ago

Selected Answer: B

field-level encryption in CloudFront uses asymmetric encryption with RSA key

upvoted 1 times

 **Russ99** 1 year, 11 months ago

Selected Answer: A

CloudFront only supports field-level encryption with symmetric KMS keys, not with RSA keys. In this specific scenario, Option A would be the correct answer because it leverages the native capabilities of CloudFront and meets the requirement of centralized key management for decrypting sensitive data.

upvoted 4 times

 **Russ99** 1 year, 11 months ago

B is correct, Not A

upvoted 2 times

 **cachac** 2 years, 1 month ago

Selected Answer: B

ALGORITHM: CloudFront uses RSA/ECB/OAEPWithSHA-256AndMGF1Padding as the algorithm for encrypting, so you must use the same algorithm to decrypt the data.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html#field-level-encryption-decrypt>
upvoted 3 times

 **KungLjao** 2 years, 1 month ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

upvoted 2 times

 **airgead** 2 years, 2 months ago

Answer: A

use field-level encryption with AWS Key Management Service (KMS) so that it can encrypt when sent through Cloud Distribution and only the specific microservice with access to the appropriate KMS key can decrypt it.

RSA does not work as Microservice data handling cannot decrypt it.

It does not require Lambda @Edge to perform to encrypt the data, just Associate the KMS key and the configuration with the CloudFront cache behavio

upvoted 1 times

Question #304

A solutions architect is determining the DNS strategy for an existing VPC. The VPC is provisioned to use the 10.24.34.0/24 CIDR block. The VPC also uses Amazon Route 53 Resolver for DNS. New requirements mandate that DNS queries must use private hosted zones. Additionally instances that have public IP addresses must receive corresponding public hostnames

Which solution will meet these requirements to ensure that the domain names are correctly resolved within the VPC?

- A. Create a private hosted zone. Activate the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC. Update the VPC DHCP options set to include domain-name-servers=10.24.34.2.
- B. Create a private hosted zone Associate the private hosted zone with the VPC. Activate the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC. Create a new VPC DHCP options set, and configure domain-name-servers=AmazonProvidedDNS. Associate the new DHCP options set with the VPC.
- C. Deactivate the enableDnsSupport attribute for the VPCActivate the enableDnsHostnames attribute for the VPCCreate a new VPC DHCP options set, and configure domain-name-servers=10.24.34.2. Associate the new DHCP options set with the VPC.
- D. Create a private hosted zone. Associate the private hosted zone with the VPC. Activate the enableDnsSupport attribute for the VPC. Deactivate the enableDnsHostnames attribute for the VPC. Update the VPC DHCP options set to include domain-name-servers=AmazonProvidedDNS.

Correct Answer: B

Community vote distribution

B (100%)

 **s61** Highly Voted 2 years, 1 month ago

Selected Answer: B

Both settings need to be enabled to allow assigning of public DNS names and use of Amazon DNS, see <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#AmazonDNS>

upvoted 8 times

 **JMAN1** Highly Voted 1 year, 11 months ago

Selected Answer: B

A is wrong because the question says it use AWS DNS rather than 10.24.34.2 custom DNS server.
C is wrong because same reason with A.
D is wrong because we need to activate DnsSupport and DnsHostnames.

Please correct me if I am wrong.

upvoted 5 times

 **kajiyatta** Most Recent 1 year ago

Selected Answer: B

A,D incorrect = Can't update DHCP option.
C incorrect = Not create private hosted zone.
upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option B is correct

To meet the requirements, you need to:

Use private hosted zones for DNS queries.

Assign public hostnames to instances with public IP addresses.

Creating a private hosted zone (Option B) meets these requirements by providing a private DNS resolution service within the VPC.

Associating the private hosted zone with the VPC ensures that DNS queries are resolved using this zone.

Activating enableDnsSupport and enableDnsHostnames attributes for the VPC allows instances to use the private hosted zone for DNS lookups and assigns public hostnames to instances with public IP addresses, respectively.

Creating a new VPC DHCP options set with domain-name-servers=AmazonProvidedDNS ensures that instances receive the correct DNS server information.

upvoted 1 times

✉️  **career360guru** 2 years, 1 month ago

Selected Answer: B
Enable both the dns options.
upvoted 4 times

✉️  **nublit** 2 years, 1 month ago

Selected Answer: B
B is the best answer
upvoted 2 times

✉️  **bustedd** 2 years, 1 month ago

B enables both settings
upvoted 2 times

Question #305

Topic 1

A data analytics company has an Amazon Redshift cluster that consists of several reserved nodes. The cluster is experiencing unexpected bursts of usage because a team of employees is compiling a deep audit analysis report. The queries to generate the report are complex read queries and are CPU intensive.

Business requirements dictate that the cluster must be able to service read and write queries at all times. A solutions architect must devise a solution that accommodates the bursts of usage.

Which solution meets these requirements MOST cost-effectively?

- A. Provision an Amazon EMR cluster Offload the complex data processing tasks.
- B. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using a classic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.
- C. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using an elastic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.
- D. Turn on the Concurrency Scaling feature for the Amazon Redshift cluster.

Correct Answer: D

Community vote distribution

D (100%)

 **AzureDP900** 1 year, 1 month ago

D is right

Concurrency Scaling is a feature in Amazon Redshift that allows you to scale your cluster's concurrency level up or down based on usage, without having to manually resize the cluster.

By turning on Concurrency Scaling, the cluster will automatically scale up when CPU utilization reaches a certain threshold (in this case, 80%), and then scale back down when usage returns to normal. This allows you to meet unexpected bursts of usage while keeping costs under control.

This solution meets the business requirements by ensuring that read and write queries can be serviced at all times, while also being cost-effective.

upvoted 2 times

 **alexandercamachop** 1 year, 10 months ago

Selected Answer: D

"With the Concurrency Scaling feature, you can support thousands of concurrent users and concurrent queries, with consistently fast query performance. When you turn on concurrency scaling, Amazon Redshift automatically adds additional cluster capacity to process an increase in both read and write queries."

<https://docs.aws.amazon.com/redshift/latest/dg/concurrency-scaling.html>

upvoted 3 times

 **cypkir** 2 years, 1 month ago

Answer C

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just D

upvoted 2 times

 **career360guru** 2 years, 1 month ago

Selected Answer: D

Best option is D

upvoted 2 times

 **nublit** 2 years, 1 month ago

Selected Answer: D

The most cost-effective solution for addressing bursts of usage and accommodating complex queries in Amazon Redshift is to turn on the Concurrency Scaling feature for the Amazon Redshift cluster.

upvoted 2 times

 **Ustad** 2 years, 1 month ago

Selected Answer: D

Simply D

upvoted 1 times

 **AM_aws** 2 years, 2 months ago

Selected Answer: D

<https://aws.amazon.com/blogs/big-data/scale-amazon-redshift-to-meet-high-throughput-query-requirements/#:~:text=Use%20Concurrency%20Scaling%20to%20dynamically,data%20warehouse%20using%20Amazon%20Redshift.>
upvoted 4 times

 **airghead** 2 years, 2 months ago

Answer: D

The most cost-effective solution for addressing bursts of usage and accommodating complex queries in Amazon Redshift is to turn on the Concurrency Scaling feature for the Amazon Redshift cluster.

upvoted 4 times

Question #306

A research center is migrating to the AWS Cloud and has moved its on-premises 1 PB object storage to an Amazon S3 bucket. One hundred scientists are using this object storage to store their work-related documents. Each scientist has a personal folder on the object store. All the scientists are members of a single IAM user group.

The research center's compliance officer is worried that scientists will be able to access each other's work. The research center has a strict obligation to report on which scientist accesses which documents. The team that is responsible for these reports has little AWS experience and wants a ready-to-use solution that minimizes operational overhead.

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

- A. Create an identity policy that grants the user read and write access. Add a condition that specifies that the S3 paths must be prefixed with `$(aws:username)`. Apply the policy on the scientists' IAM user group.
- B. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket. Store the trail output in another S3 bucket. Use Amazon Athena to query the logs and generate reports.
- C. Enable S3 server access logging. Configure another S3 bucket as the target for log delivery. Use Amazon Athena to query the logs and generate reports.
- D. Create an S3 bucket policy that grants read and write access to users in the scientists' IAM user group.
- E. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket and write the events to Amazon CloudWatch. Use the Amazon Athena CloudWatch connector to query the logs and generate reports.

Correct Answer: AB*Community vote distribution*

AB (75%) AC (15%) 10%

 **FZA24** 11 months, 2 weeks ago

Selected Answer: AB

BUT, The question is not clearly formulated.
Nothing mentions the requirement that a scientist must only access his own folder.

upvoted 1 times

 **juanife** 10 months, 2 weeks ago

the question affirms the following: "The research center's compliance officer is worried that scientists will be able to access each other's work." it is equal to say that each scientist only must have access to his own data and not other data

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option A allows for secure and isolated access to each scientist's personal folder by prefixing the S3 paths with `$(aws:username)`, ensuring that scientists can only access their own documents. This aligns with the research center's compliance officer's concern about preserving data isolation.
Option B configures a CloudTrail trail to capture all object-level events in the S3 bucket, providing detailed information on who accessed which documents. This meets the requirement for reporting on document access by scientists.

upvoted 1 times

 **Daniel76** 1 year, 2 months ago

Selected Answer: AB
Option E problem is cloudwatch need to be exported to s3 bucket to be queried by Athena.

upvoted 1 times

 **9f02c8d** 1 year, 6 months ago

Option AB
upvoted 1 times

 **ele** 1 year, 10 months ago

Selected Answer: AB
Not C: Server access log records are delivered on a best-effort basis.

upvoted 4 times

 **hogtrough** 1 year, 10 months ago

To elaborate further, "The completeness and timeliness of server logging is not guaranteed. The log record for a particular request might be delivered long after the request was actually processed, or it might not be delivered at all."

upvoted 1 times

 **07c2d2a** 1 year, 10 months ago

AB is correct. They key here is that the logs are required to be accurate for compliance reasons. Server access isn't good enough here. "Server access log records are delivered on a best-effort basis. Most requests for a bucket that is properly configured for logging result in a delivered log record. Most log records are delivered within a few hours of the time that they are recorded, but they can be delivered more frequently"

upvoted 3 times

 **mhampar12** 1 year, 11 months ago

Selected Answer: AC

"The team that is responsible for these reports has little AWS experience and wants a ready-to-use solution that minimizes operational overhead."

upvoted 1 times

 **mhampar12** 1 year, 11 months ago

A and C

"The team that is responsible for these reports has little AWS experience and wants a ready-to-use solution that minimizes operational overhead."

upvoted 1 times

 **vibzr2023** 1 year, 11 months ago

Answer: AB

Option C is incorrect because enabling S3 server access logging and delivering the logs to another S3 bucket does not directly address the requirement to report on which scientist accesses which documents. While the logs can be queried, it does not provide a straightforward solution for generating the required reports.

Option D is incorrect because creating an S3 bucket policy that grants read and write access to users in the scientists' IAM user group does not address the compliance officer's concern about scientists being able to access each other's work. It also does not provide a solution for reporting on which scientist accesses which documents.

upvoted 2 times

 **altonh** 10 months ago

Both B & C use Athena to query the logs and generate reports

upvoted 2 times

 **George88** 2 years, 1 month ago

Answer: AB

<https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/>

upvoted 4 times

 **D10SJoker** 2 years, 1 month ago

Selected Answer: AB

In Amazon S3, you can identify requests using an AWS CloudTrail event log. AWS CloudTrail is the preferred way of identifying Amazon S3 requests, but if you are using Amazon S3 server access logs, see Using Amazon S3 access logs to identify requests.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-request-identification.html>

upvoted 1 times

 **kairosfc** 2 years, 1 month ago

Selected Answer: BD

It doesn't mention that the folder name is the AWS username. There is no guarantee that alternative "A" will be effective.

upvoted 2 times

 **Jay_2pt0_1** 2 years ago

I think BD as well

upvoted 1 times

 **LS1168** 2 years, 1 month ago

Selected Answer: AB

CloudTrail + Identify so A and B, there was another question on CloudTrail vs. S3 Server Access logging, always CloudTrail wins

upvoted 3 times

 **Andres123456** 2 years, 1 month ago

Selected Answer: AB

AB

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 1 times

 **AMohanty** 2 years, 1 month ago

AB

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 2 times

 **Tofu13** 2 years, 1 month ago

Look for

Turn on logs for a subset of objects (prefix)

-> Only possible for CloudTrail
upvoted 1 times

 **Ustad** 2 years, 1 month ago

Selected Answer: AB

To Audit: B is the correct one

To Act: A is the correct one but not so effective.

upvoted 1 times

 **s61** 2 years, 1 month ago

Selected Answer: AB

CloudTrail provides more detailed logging than S3 server access logging

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-s3-access-logs-to-identify-requests.html>

upvoted 2 times

Question #307

Topic 1

A company uses AWS Organizations to manage a multi-account structure. The company has hundreds of AWS accounts and expects the number of accounts to increase. The company is building a new application that uses Docker images. The company will push the Docker images to Amazon Elastic Container Registry (Amazon ECR). Only accounts that are within the company's organization should have access to the images.

The company has a CI/CD process that runs frequently. The company wants to retain all the tagged images. However, the company wants to retain only the five most recent untagged images.

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

- A. Create a private repository in Amazon ECR. Create a permissions policy for the repository that allows only required ECR operations. Include a condition to allow the ECR operations if the value of the aws:PrincipalOrgID condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five
- B. Create a public repository in Amazon ECR. Create an IAM role in the ECR account. Set permissions so that any account can assume the role if the value of the aws:PrincipalOrgID condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five.
- C. Create a private repository in Amazon ECR. Create a permissions policy for the repository that includes only required ECR operations. Include a condition to allow the ECR operations for all account IDs in the organization. Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.
- D. Create a public repository in Amazon ECR. Configure Amazon ECR to use an interface VPC endpoint with an endpoint policy that includes the required permissions for images that the company needs to pull. Include a condition to allow the ECR operations for all account IDs in the company's organization. Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.

Correct Answer: A*Community vote distribution*

A (100%)

  **AzureDP900** 1 year, 1 month ago

Option A

A private repository in Amazon ECR restricts access to only authorized accounts within the company's organization.

The permissions policy ensures that only required ECR operations are allowed, reducing operational overhead.

The condition in the permissions policy allows ECR operations for accounts within the company's organization, further reducing overhead.

Finally, adding a lifecycle rule to delete untagged images over the count of five simplifies image management and reduces storage costs.
upvoted 1 times  **ftaws** 1 year, 11 months ago

How to associate the policy in ECR repository ?

I think A is also wrong....

upvoted 1 times

  **shaam80** 2 years ago

Answer A. Use ECR Lifecycle policy. Also using OrgId is more scalable with more accounts will be added than adding accounts individually. Less operational overhead.

upvoted 4 times

  **career360guru** 2 years, 1 month ago**Selected Answer: A**

A is right option.

upvoted 2 times

  **nublit** 2 years, 1 month ago**Selected Answer: A**

Only A is a good idea

upvoted 2 times

  **joleneinthebackyard** 2 years, 1 month ago**Selected Answer: A**

B, D: stop reading at "public repository"
A: policy specific to aws:PrincipalOrgId equal company's organization ID
C: policy allow all account ID (effectively the same actually) but use Eventbridge + lambda while ECR has lifecycle policy.
upvoted 4 times

 **s61** 2 years, 1 month ago

Selected Answer: A

Also A

upvoted 1 times

 **KungLjao** 2 years, 1 month ago

Selected Answer: A

A works for all requirements

upvoted 1 times

Question #308

Topic 1

A solutions architect is reviewing a company's process for taking snapshots of Amazon RDS DB instances. The company takes automatic snapshots every day and retains the snapshots for 7 days.

The solutions architect needs to recommend a solution that takes snapshots every 6 hours and retains the snapshots for 30 days. The company uses AWS Organizations to manage all of its AWS accounts. The company needs a consolidated view of the health of the RDS snapshots.

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

- A. Turn on the cross-account management feature in AWS Backup. Create a backup plan that specifies the frequency and retention requirements. Add a tag to the DB instances. Apply the backup plan by using tags. Use AWS Backup to monitor the status of the backups.
- B. Turn on the cross-account management feature in Amazon RDS. Create a snapshot global policy that specifies the frequency and retention requirements. Use the RDS console in the management account to monitor the status of the backups.
- C. Turn on the cross-account management feature in AWS CloudFormation. From the management account, deploy a CloudFormation stack set that contains a backup plan from AWS Backup that specifies the frequency and retention requirements. Create an AWS Lambda function in the management account to monitor the status of the backups. Create an Amazon EventBridge rule in each account to run the Lambda function on a schedule.
- D. Configure AWS Backup in each account. Create an Amazon Data Lifecycle Manager lifecycle policy that specifies the frequency and retention requirements. Specify the DB instances as the target resource. Use the Amazon Data Lifecycle Manager console in each member account to monitor the status of the backups.

Correct Answer: A*Community vote distribution*

A (100%)

 **KungLjao** Highly Voted 2 years, 1 month ago

Selected Answer: A

Crossaccount management is a feature of only the aws backup service.
upvoted 6 times

 **AzureDP900** Most Recent 1 year, 1 month ago

This solution uses AWS Backup, which provides a centralized view of all backups across accounts. It allows for automatic snapshotting every 6 hours, meeting the requirement for frequent snapshots. The retention period of 30 days is also easily managed using AWS Backup policies. Using tags to apply the backup plan and monitor the status of backups simplifies the process and reduces operational overhead. Therefore, using AWS Backup (Option A) with cross-account management enabled provides the least operational overhead while still meeting the requirements for frequent snapshots and long-term retention
upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: A

Option A
upvoted 3 times

 **s61** 2 years, 1 month ago

Selected Answer: A

<https://docs.aws.amazon.com/aws-backup/latest/devguide/create-cross-account-backup.html>
upvoted 3 times

 **AM_aws** 2 years, 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/aws-backup/latest/devguide/create-cross-account-backup.html>
upvoted 3 times

 **airgead** 2 years, 2 months ago

Answer: A
User BAWS BBackup > Cross Accounr > backup plan for frequency and retention and health of the backup
upvoted 2 times

Question #309

A company is using AWS Organizations with a multi-account architecture. The company's current security configuration for the account architecture includes SCPs, resource-based policies, identity-based policies, trust policies, and session policies.

A solutions architect needs to allow an IAM user in Account A to assume a role in Account B.

Which combination of steps must the solutions architect take to meet this requirement? (Choose three.)

- A. Configure the SCP for Account A to allow the action.
- B. Configure the resource-based policies to allow the action.
- C. Configure the identity-based policy on the user in Account A to allow the action.
- D. Configure the identity-based policy on the user in Account B to allow the action.
- E. Configure the trust policy on the target role in Account B to allow the action.
- F. Configure the session policy to allow the action and to be passed programmatically by the GetSessionToken API operation.

Correct Answer: ACE

Community vote distribution

ACE (53%)	BCE (33%)	13%
-----------	-----------	-----

✉  **Andres123456** Highly Voted 2 years, 1 month ago

Selected Answer: BCE

- C) Attach an identity-based policy to the IAM user in Account A (allowed to assume IAM role in Account B)
- E) Configure the trust policy on the target role in Account B (accountID of the trusted account which is Account A)
- B) Configure a resource-based policy which allows certain actions on resources which reside in Account B)

reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

upvoted 12 times

✉  **JMAN1** 1 year, 11 months ago

IAM roles and resource-based policies delegate access across accounts only within a single partition. For example, assume that you have an account in US West (N. California) in the standard aws partition. You also have an account in China (Beijing) in the aws-cn partition. You can't use an Amazon S3 resource-based policy in your account in China (Beijing) to allow access for users in your standard aws account.

So B can't be answer.

upvoted 1 times

✉  **airgead** Highly Voted 2 years, 2 months ago

Answer: C, E, F

Attach a policy to the IAM user in Account A > Trust Policy in Account B > GetSessionToken API operation

upvoted 11 times

✉  **ele** 1 year, 10 months ago

F is wrong, you cannot use GetSessionToken to configure session policy.

You can pass a single inline session policy programmatically by using the policy parameter with the AssumeRole, AssumeRoleWithSAML, AssumeRoleWithWebIdentity, and GetFederationToken API operations.

ACE is correct answer.

upvoted 2 times

✉  **a178080** Most Recent 4 months, 3 weeks ago

Selected Answer: BCE

SCP does not grant permission it's a guardrail (it's a deny policy always) so the option is wrongly worded!

upvoted 3 times

✉  **eesa** 9 months, 1 week ago

Selected Answer: ACE

- C. Configure the identity-based policy on the user in Account A to allow the action.

The IAM user in Account A needs permission to assume the role in Account B.

This is done by attaching an identity-based policy that allows the sts:AssumeRole action on the target role in Account B.

- E. Configure the trust policy on the target role in Account B to allow the action.

The IAM role in Account B must trust the user from Account A.
This is done by adding a trust policy to the role, specifying Account A's user or a specific IAM principal from Account A.

- A. Configure the SCP for Account A to allow the action.

Service Control Policies (SCPs) act as guardrails at the AWS Organizations level.
If there is an SCP that denies cross-account role assumption, it must be modified to allow sts:AssumeRole for Account A.
upvoted 2 times

 **albert_kuo** 9 months, 3 weeks ago

Selected Answer: ACE

IAM Role does not support Resource-Based Policy, we should apply Trust Policy instead.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Option A (Configure the SCP for Account A to allow the action) is correct because the SCP would need to be configured to allow the assumption of roles from one account to another.

Option C (Configure the identity-based policy on the user in Account A to allow the action) is also correct, as it would define the permissions that the IAM user has within their own account.

And finally, Option E (Configure the trust policy on the target role in Account B to allow the action) is necessary because it specifies the external identity provider and the roles that can be assumed by users from that identity provider.
upvoted 1 times

 **Daniel76** 1 year, 1 month ago

Selected Answer: ACE

Revising my earlier vote to ACE, agree that resource based policies is not required. SCP though apply restriction rather than allow, reviewing it to ensure it doesn't block this access does make sense.

upvoted 1 times

 **sashenka** 1 year, 2 months ago

Correct Options:

- A. Configure the SCP for Account A to allow the action.
- C. Configure the identity-based policy on the user in Account A to allow the action.
- E. Configure the trust policy on the target role in Account B to allow the action.

Explanation of Incorrect Options:

- B. Configure the resource-based policies to allow the action:

Resource-based policies are typically used to control access to specific resources like S3 buckets, not for cross-account role assumption.

- D. Configure the identity-based policy on the user in Account B to allow the action:

The identity-based policy for users in Account B is not relevant here, as the user in Account A needs permission to assume the role.
upvoted 5 times

 **Syre** 1 year, 2 months ago

Selected Answer: BCE

SCPs are not necessary at all here...

upvoted 2 times

 **wbedair** 1 year, 3 months ago

Selected Answer: ACE

the ask is steps to "ASSUME A ROLE" not to "access the resource" . so option B and F are wrong as with A, C, E I can still assume the role regardless of the configuration of resource policy and session policy who can still deny access to the resource
upvoted 1 times

 **Daniel76** 1 year, 4 months ago

Selected Answer: BCE

To allow an IAM user in Account A to assume a role in Account B - we only need identity-based , resource-based and trust policies. Session policy and SCP not required.

upvoted 2 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: ACE

A (SCP) is more relevant than B (resource-based policies) because, while SCPs are not granting permissions, they could potentially restrict actions. Therefore, ensuring that the SCP in Account A (and Account B) does not block the necessary sts:AssumeRole action is important. B (resource-based policies) isn't relevant for the cross-account role assumption in this context.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

A: SCPs (Service Control Policies) are used to set permission boundaries at the organizational or account level. SCPs can restrict or allow certain actions, but they do not grant permissions directly. An SCP in Account A would typically not be responsible for directly allowing a user to assume a role in Account B, though it could block the action if not configured properly.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

B: Resource-based policies are policies attached directly to AWS resources (like S3 buckets or IAM roles). However, in this scenario, resource-based policies are less relevant because the focus is on role assumption, which is governed by identity policies and trust policies rather than resource-based policies.

upvoted 1 times

 **alex_heavy** 1 year, 5 months ago

Selected Answer: CDE

E Trust policy in B

D Identity-based policy on the ROLE in Account B to allow the action (I think typo in question)

C Configure the identity-based policy on the user in Account A to allow the action.

Just try it in AWS env.

upvoted 1 times

 **trungtd** 1 year, 6 months ago

Selected Answer: BCE

you generally do not need to modify the Service Control Policies (SCPs) to allow one account's IAM users to assume roles in another account, as long as the SCPs do not explicitly deny the required actions (like sts:AssumeRole).

upvoted 2 times

 **9f02c8d** 1 year, 6 months ago

BCE - SCP is not required here & used for deny not for allow

upvoted 2 times

 **red_panda** 1 year, 7 months ago

Selected Answer: BCE

Answer is BCE.

SCPs are not used for ALLOW actions but for DENY actions at Org level.

upvoted 2 times

 **teo2157** 1 year, 7 months ago

Selected Answer: ACE

The key point here is "The company's current security configuration for the account architecture includes SCPs," so if SCPs are in place, the SCP in the account A has to be configured to allow the action.

upvoted 2 times

Question #310

Topic 1

A company wants to use Amazon S3 to back up its on-premises file storage solution. The company's on-premises file storage solution supports NFS, and the company wants its new solution to support NFS. The company wants to archive the backup files after 5 days. If the company needs archived files for disaster recovery, the company is willing to wait a few days for the retrieval of those files.

Which solution meets these requirements MOST cost-effectively?

- A. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- B. Deploy an AWS Storage Gateway volume gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the volume gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.
- C. Deploy an AWS Storage Gateway tape gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the tape gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- D. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.

Correct Answer: D

Community vote distribution

D (100%)

 **AzureDP900** 1 year, 1 month ago

D

This option meets all the requirements as follows:

The file gateway supports NFS, meeting the company's requirement for a file-based storage solution.

Moving files from the on-premises file storage solution to the file gateway ensures that the backup files are stored in S3, meeting the company's need for cloud-based backup.

Creating an S3 Lifecycle rule to move files to Glacier Deep Archive after 5 days meets the company's requirement for archiving backup files and reducing storage costs.

Using Glacier Deep Archive also meets the requirement for archived files to be retrieved over time, as it allows for retrieval of data at a later date with some delay.

upvoted 1 times

 **carpa_jo** 1 year, 12 months ago

Selected Answer: D

Glacier Deep Archive is more cost-effective than Standard-IA, so A and C are out.

Decision between B and D: The solution requires support for NFS -> File Gateway instead of Volume Gateway --> D it is.

upvoted 4 times

 **career360guru** 2 years, 1 month ago

Selected Answer: D

Option D

upvoted 2 times

 **nublit** 2 years, 1 month ago

Selected Answer: D

D, with Deep Archive, Retrieval time within 12 hours

upvoted 2 times

 **Ustad** 2 years, 1 month ago

Selected Answer: D

File Gateway

Glacier

upvoted 3 times

 **s61** 2 years, 1 month ago

Selected Answer: D

D - File Gateway supports NFS and Deep Glacier is the cheapest storage option in S3

upvoted 2 times

 **airgead** 2 years, 2 months ago

Answer: D

using AWS Storage file is appropriate and straight to S3 Glacier Deep Archive is most cost efficient as the company is willing to wait a few days for the retrieval of those files in case of DR

upvoted 3 times

Question #311

Topic 1

A company runs its application on Amazon EC2 instances and AWS Lambda functions. The EC2 instances experience a continuous and stable load. The Lambda functions experience a varied and unpredictable load. The application includes a caching layer that uses an Amazon MemoryDB for Redis cluster.

A solutions architect must recommend a solution to minimize the company's overall monthly costs.

Which solution will meet these requirements?

- A. Purchase an EC2 instance Savings Plan to cover the EC2 instances. Purchase a Compute Savings Plan for Lambda to cover the minimum expected consumption of the Lambda functions. Purchase reserved nodes to cover the MemoryDB cache nodes.
- B. Purchase a Compute Savings Plan to cover the EC2 instances. Purchase Lambda reserved concurrency to cover the expected Lambda usage. Purchase reserved nodes to cover the MemoryDB cache nodes.
- C. Purchase a Compute Savings Plan to cover the entire expected cost of the EC2 instances, Lambda functions, and MemoryDB cache nodes.
- D. Purchase a Compute Savings Plan to cover the EC2 instances and the MemoryDB cache nodes. Purchase Lambda reserved concurrency to cover the expected Lambda usage.

Correct Answer: A*Community vote distribution*

A (88%)

12%

 **airgead**  2 years, 1 month ago

Selected Answer: A

EC2 - Saving Plan, MemoryDB - Reserved Node, Lambda - Compute Saving Plan
upvoted 10 times

 **blackgamer**  2 years, 1 month ago

Answer is A, it saves the most cost saving option.
B and D are out as reserved concurrency doesn't help for cost saving. Compared between A&C, A is more cost effective solution, additionally compute saving plan doesn't cover costs for elastic cache node.
upvoted 6 times

 **AzureDP900**  1 year, 1 month ago

A
This solution addresses each component of the application separately:

Purchasing an EC2 instance Savings Plan (Option A) provides a discounted rate for EC2 instances, which are experiencing continuous and stable load.

Buying a Compute Savings Plan for Lambda (Option A) covers the minimum expected consumption of the Lambda functions, which have unpredictable and varied load. This plan type is specifically designed for workloads with varying usage patterns.

Purchasing reserved nodes to cover the MemoryDB cache nodes (Option A) provides a discounted rate for the cache layer, which has stable and predictable load.

upvoted 1 times

 **shaam80** 2 years ago

A makes sense. Reserved concurrency for Lambda doesn't address cost savings nor varied load. And compute plans don't cover MemoryDB. Reserved nodes should work.

upvoted 1 times

 **salazar35** 2 years, 1 month ago

Selected Answer: A
Compute Saving Plans don't cover MemoryDB
upvoted 3 times

 **D10SJoker** 2 years, 1 month ago

Selected Answer: A
We don't know the expected load of Lambda so B and D out (it says expected Lambda usage) and A it's more cost effective than C
upvoted 2 times

 **career360guru** 2 years, 1 month ago

A is most cost effective.

upvoted 1 times

 **KungLjao** 2 years, 1 month ago

Selected Answer: A

Reserved concurrency for lambda wont reduce costs, and lambda will benefit from compute savings plan <https://aws.amazon.com/about-aws/whats-new/2020/02/aws-lambda-participates-in-compute-savings-plans/>

upvoted 3 times

 **Jun_W** 2 years, 2 months ago

Selected Answer: A

ChatGPT

upvoted 5 times

 **airgead** 2 years, 2 months ago

Selected Answer: B

EC2 - Saving Plan, MemoryDB - Reserved Node, Lambda - reserved concurrency

upvoted 3 times

 **airgead** 2 years, 1 month ago

Change this to A as it is correct that Lambda Reserved Concurrency does not help in saving costs.

upvoted 2 times

Question #312

Topic 1

A company is launching a new online game on Amazon EC2 instances. The game must be available globally. The company plans to run the game in three AWS Regions us-east-1, eu-west-1, and ap-southeast-1. The game's leaderboards, player inventory and event status must be available across Regions.

A solutions architect must design a solution that will give any Region the ability to scale to handle the load of all Regions. Additionally, users must automatically connect to the Region that provides the least latency.

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

- A. Create an EC2 Spot Fleet. Attach the Spot Fleet to a Network Load Balancer (NLB) in each Region. Create an AWS Global Accelerator IP address that points to the NLB. Create an Amazon Route 53 latency-based routing entry for the Global Accelerator IP address. Save the game metadata to an Amazon RDS for MySQL DB instance in each Region. Set up a read replica in the other Regions.
- B. Create an Auto Scaling group for the EC2 instances. Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses geoproximity routing and points to the NLB in that Region. Save the game metadata to MySQL databases on EC2 instances in each Region. Set up replication between the database EC2 instances in each Region.
- C. Create an Auto Scaling group for the EC2 instances. Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses latency-based routing and points to the NLB in that Region. Save the game metadata to an Amazon DynamoDB global table.
- D. Use EC2 Global View. Deploy the EC2 instances to each Region. Attach the instances to a Network Load Balancer (NLB). Deploy a DNS server on an EC2 instance in each Region. Set up custom logic on each DNS server to redirect the user to the Region that provides the lowest latency. Save the game metadata to an Amazon Aurora global database.

Correct Answer: C

Community vote distribution

C (100%)

 **AzureDP900** 1 year, 1 month ago

C

This solution allows any Region to scale to handle the load of all Regions, meeting the first requirement.

By using latency-based routing with Amazon Route 53, users are automatically connected to the Region that provides the least latency, meeting the second requirement.

Saving game metadata to an Amazon DynamoDB global table eliminates the need for replication between Regions, reducing operational overhead.

upvoted 2 times

 **vibzr2023** 1 year, 11 months ago

Answer: C

keywords "latency-based routing" and "DynamoDB global table."

upvoted 4 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

Option C that uses DynamoDB wins

upvoted 3 times

 **nublit** 2 years, 1 month ago

Selected Answer: C

C, Latency > Geoproximity.

upvoted 4 times

 **joleneinthebackyard** 2 years, 1 month ago

Selected Answer: C

easy C

upvoted 2 times

 **Bad_Mat** 2 years, 1 month ago

Should be C

upvoted 2 times

 **KungLjao** 2 years, 1 month ago

Selected Answer: C

C 100%

upvoted 1 times

 **Jun_W** 2 years, 2 months ago

Selected Answer: C

Latency Routing

upvoted 1 times

 **airgead** 2 years, 2 months ago

Selected Answer: C

Autoscaling and NLB for Load Distribution, Latency Routing for Least Latency and DynamoDB Global Table for replication across regions.

upvoted 2 times

Question #313

A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company's AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet-bound traffic through the appliances.

A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPCs.

Which steps should the solutions architect recommend to meet these requirements? (Choose three.)

- A. Deploy two firewall appliances into the shared services VPC, each in a separate Availability Zone.
- B. Create a new Network Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Network Load Balancer. Add each of the firewall appliance instances to the target group.
- C. Create a new Gateway Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Gateway Load Balancer. Add each of the firewall appliance instances to the target group.
- D. Create a VPC interface endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.
- E. Deploy two firewall appliances into the shared services VPC, each in the same Availability Zone.
- F. Create a VPC Gateway Load Balancer endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.

Correct Answer: ACF*Community vote distribution*

ACF (87%) 6%

 **ayadmawla**  2 years ago

Selected Answer: ACF

Need (A) two firewalls spread over two availability zones for HA and balanced by an NLB, then (C) a Gateway Load Balancer to interface to the virtual 3rd party network firewalls through the NLB, then (F) a Gateway Load Balancer EndPoint in the Consumer VPC with routes taking the traffic to the shared GLB + Firewalls

A simple diagram is given here so you don't forget if you are visual like me :)
<https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html>
 upvoted 16 times

 **ayadmawla** 2 years ago

apologies, I meant balanced by the GLB (A)
 upvoted 3 times

 **s61**  2 years, 1 month ago

Selected Answer: ACF

ACF
<https://docs.aws.amazon.com/vpc/latest/privatelink/create-gateway-load-balancer-endpoint-service.html>
 upvoted 6 times

 **TomTom**  1 year ago

Selected Answer: ABF

Why Not A,B,F?
 For option C, Using a Gateway Load Balancer is suitable for load balancing traffic entering the VPC, but it doesn't provide the same level of fault tolerance as a Network Load Balancer. Gateway Load Balancers are primarily used for routing traffic between VPCs.
 upvoted 1 times

 **Chris_W_1234** 1 month, 3 weeks ago

From Google: Gateway Load Balancers (GLB) are designed to insert and manage third-party virtual network appliances, operating at the IP packet level (Layer 3) to scale and route traffic to them transparently. Network Load Balancers (NLB) are built for high-performance, low-latency TCP/UDP traffic, operating at the transport layer (Layer 4) and routing based on IP address and port.

I'd like to think of it this way: ALBs and NLBs for sending traffic *into* a service. GLBs inspect traffic and *route* traffic somewhere else.
 upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

Selected Answer: ACF

A, C, F for sure.
Using Gateway Load Balancer for distributing traffic across multiple virtual appliances
upvoted 1 times

 **sarlos** 1 year, 7 months ago

healthy virtual appliances means gateway load balancer.
upvoted 1 times

 **enk** 2 years, 1 month ago

Selected Answer: ABD
Obviously A over E. GWLB's don't make good load balancers. Avoid C and F. Need NLB to minimize the failover time between the (2) 3rd party FW's.
upvoted 1 times

 **enk** 2 years, 1 month ago

Well, I read a bit further on Gateway Load Balancers and a 3rd party firewall is the perfect scenario to use a GwLB. So, looks like the correct answers are ACF.
upvoted 2 times

 **Ustad** 2 years, 1 month ago

Selected Answer: ACF
<https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-gateway-load-balancer-supported-architecture-patterns/>
upvoted 4 times

 **airgead** 2 years, 2 months ago

Selected Answer: ACD
A: Use 2 firewall Appliances for each AZ
C: Use GWLB for 3rd party appliances routing traffic
D: enables the routing of outbound internet-bound traffic through the firewall appliances.
upvoted 2 times

 **KungLjao** 2 years, 1 month ago

Why not gw endpoint?
upvoted 1 times

Question #314

Topic 1

A solutions architect needs to migrate an on-premises legacy application to AWS. The application runs on two servers behind a load balancer. The application requires a license file that is associated with the MAC address of the server's network adapter. It takes the software vendor 12 hours to send new license files. The application also uses configuration files with a static IP address to access a database server, host names are not supported.

Given these requirements, which combination of steps should be taken to implement highly available architecture for the application servers in AWS? (Choose two.)

- A. Create a pool of ENIs. Request license files from the vendor for the pool, and store the license files in Amazon S3. Create a bootstrap automation script to download a license file and attach the corresponding ENI to an Amazon EC2 instance.
- B. Create a pool of ENIs. Request license files from the vendor for the pool, store the license files on an Amazon EC2 instance. Create an AMI from the instance and use this AMI for all future EC2 instances.
- C. Create a bootstrap automation script to request a new license file from the vendor. When the response is received, apply the license file to an Amazon EC2 instance.
- D. Edit the bootstrap automation script to read the database server IP address from the AWS Systems Manager Parameter Store, and inject the value into the local configuration files.
- E. Edit an Amazon EC2 instance to include the database server IP address in the configuration files and re-create the AMI to use for all future EC2 instances.

Correct Answer: AD

Community vote distribution

AD (100%)

 **airgead** Highly Voted 2 years, 1 month ago

Selected Answer: AD

.Option A covers the licensing aspect, and option D addresses the configuration file requirements.
upvoted 7 times

 **d401c0d** Most Recent 10 months, 3 weeks ago

Selected Answer: AD

pool of ENIs and store using S3 since that is better than storing in EC2. You already have a bootstrap script so you EDIT it.
upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option A creates a pool of ENIs (Elastic Network Interfaces), which allows the application servers to have multiple network interfaces with different MAC addresses. This is necessary because the software vendor requires license files associated with specific MAC addresses.

Storing the license files in Amazon S3 makes it easier to manage and distribute them across multiple instances.

Option D updates the bootstrap automation script to use the AWS Systems Manager (SSM) Parameter Store to retrieve the database server IP address. This allows the configuration files to be dynamically updated, eliminating the need for a static IP address.
upvoted 2 times

 **sarlos** 1 year, 7 months ago

AD are the right answer
upvoted 1 times

 **duriselvan** 2 years ago

AD AS
<https://aws.amazon.com/blogs/aws/new-elastic-network-interfaces-in-the-virtual-private-cloud/>
upvoted 3 times

 **career360guru** 2 years, 1 month ago

Selected Answer: AD
A & D are right options
upvoted 3 times

 **s61** 2 years, 1 month ago

Selected Answer: AD
AD
Bootstrap scripts

upvoted 3 times

Question #315

Topic 1

A company runs its sales reporting application in an AWS Region in the United States. The application uses an Amazon API Gateway Regional API and AWS Lambda functions to generate on-demand reports from data in an Amazon RDS for MySQL database. The frontend of the application is hosted on Amazon S3 and is accessed by users through an Amazon CloudFront distribution. The company is using Amazon Route 53 as the DNS service for the domain. Route 53 is configured with a simple routing policy to route traffic to the API Gateway API.

In the next 6 months, the company plans to expand operations to Europe. More than 90% of the database traffic is read-only traffic. The company has already deployed an API Gateway API and Lambda functions in the new Region.

A solutions architect must design a solution that minimizes latency for users who download reports.

Which solution will meet these requirements?

- A. Use an AWS Database Migration Service (AWS DMS) task with full load to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to latency-based routing to connect to the API Gateway API.
- B. Use an AWS Database Migration Service (AWS DMS) task with full load plus change data capture (CDC) to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.
- C. Configure a cross-Region read replica for the RDS database in the new Region. Change the Route 53 record to latency-based routing to connect to the API Gateway API.
- D. Configure a cross-Region read replica for the RDS database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.

Correct Answer: C*Community vote distribution*

C (96%) 4%

 **whenthan** Highly Voted 2 years, 1 month ago

Selected Answer: C

minimizes latency for users who download reports.
upvoted 11 times

 **s61** Highly Voted 2 years, 1 month ago

Selected Answer: C

C
Question specifies minimal latency for end users, latency based is more appropriate than geo based routing
upvoted 5 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Option C creates a cross-Region read replica of the RDS database in the new Region, which allows users to access and download reports from a database that is closer to their location.
The read-only traffic makes this solution suitable, as it does not require any write operations on the secondary database.
Configuring latency-based routing on Route 53 directs users to the closest available API Gateway API based on their geolocation, which minimizes latency for report downloads.
upvoted 1 times

 **sarlos** 1 year, 7 months ago

Answer is C
upvoted 1 times

 **VerRi** 1 year, 9 months ago

Selected Answer: C
minimizes latency
upvoted 1 times

 **salazar35** 2 years, 1 month ago

Selected Answer: C
C - minimizes latency for users who download reports
upvoted 3 times

 **career360guru** 2 years, 1 month ago

Selected Answer: C

As latency is key Option C
upvoted 2 times

 **Ustad** 2 years, 1 month ago

Selected Answer: C

The concern is the latency not the region itself.
upvoted 3 times

 **KungLjao** 2 years, 1 month ago

Selected Answer: D

Geo routing ftw
upvoted 1 times

Question #316

Topic 1

A software company needs to create short-lived test environments to test pull requests as part of its development process. Each test environment consists of a single Amazon EC2 instance that is in an Auto Scaling group.

The test environments must be able to communicate with a central server to report test results. The central server is located in an on-premises data center. A solutions architect must implement a solution so that the company can create and delete test environments without any manual intervention. The company has created a transit gateway with a VPN attachment to the on-premises network.

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

- A. Create an AWS CloudFormation template that contains a transit gateway attachment and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets to deploy a new stack for each VPC in the account. Deploy a new VPC for each test environment.
- B. Create a single VPC for the test environments. Include a transit gateway attachment and related routing configurations. Use AWS CloudFormation to deploy all test environments into the VPC.
- C. Create a new OU in AWS Organizations for testing. Create an AWS CloudFormation template that contains a VPC, necessary networking resources, a transit gateway attachment, and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets for deployments into each account under the testing OU. Create a new account for each test environment.
- D. Convert the test environment EC2 instances into Docker images. Use AWS CloudFormation to configure an Amazon Elastic Kubernetes Service (Amazon EKS) cluster in a new VPC, create a transit gateway attachment, and create related routing configurations. Use Kubernetes to manage the deployment and lifecycle of the test environments.

Correct Answer: B

Community vote distribution

B (87%)	13%
---------	-----

 **Richqua** Highly Voted 2 years, 1 month ago

This question is very vague. It doesn't say whether each test env is in a separate VPC or a separate account. Not sure why Transit gateway is used here.

upvoted 9 times

 **joleneinthebackyard** Highly Voted 2 years, 1 month ago

Selected Answer: B

- A: no need for new VPC for each test
- B: sounds ok
- C: creating new OU for each test? -> out
- D: too complex since need to containerize from code in EC2 instance

upvoted 7 times

 **aka1177** 2 weeks, 6 days ago

C says - "...for deployments into each account under the testing OU" - it's a good practice to separate environments;
upvoted 1 times

 **AzureDP900** Most Recent 1 year, 1 month ago

B

Option B creates a single VPC for all test environments, which allows them to share the same transit gateway attachment and routing configurations.

This approach can simplify the network configuration and reduce the overhead of managing multiple VPCs.

Each test environment still has its own isolated network space within the shared VPC, ensuring security and isolation between environments.

In fact, option B is a good solution when the requirements don't specify that each test environment needs to have its own isolated network space. Since the test environments only need to communicate with a central server in an on-premises data center, using a single VPC might be sufficient.

upvoted 1 times

 **red_panda** 1 year, 7 months ago

Selected Answer: A

I'm going with A.

There is no need to have the Transit Gateway without more VPCs for each account.

It's also a best practices to have separate environments to isolate test.

upvoted 2 times

 **helloworldabc** 1 year, 4 months ago

justy b

upvoted 1 times

 **career360guru** 2 years, 1 month ago

Selected Answer: B

Choice is between A & B. Given there are no other requirements for using stacksets B is most simple.

upvoted 3 times

 **JMAN1** 1 year, 11 months ago

I am following your answer. :)

upvoted 1 times

 **titi_r** 1 year, 8 months ago

What's the purpose of the transit gateway in this case and what you'll do if you want to delete a single test environment? I lean more to A.

upvoted 2 times

 **Chris_W_1234** 1 month, 3 weeks ago

The question states that each test "environment" consists of a single EC2 instance in an ASG. So to delete a test env, simply delete EC2 instance and ASG.

upvoted 1 times

 **nublit** 2 years, 1 month ago

Selected Answer: B

B is the best answer

upvoted 1 times

 **Ustad** 2 years, 1 month ago

Selected Answer: B

LEAST operational overhead -> B

no need to over-complicate it

upvoted 1 times

 **KungLjao** 2 years, 1 month ago

Selected Answer: B

Not sure about the benefits of using a stack set in this case, going with B

upvoted 1 times

Question #317

Topic 1

A company is deploying a new API to AWS. The API uses Amazon API Gateway with a Regional API endpoint and an AWS Lambda function for hosting. The API retrieves data from an external vendor API, stores data in an Amazon DynamoDB global table, and retrieves data from the DynamoDB global table. The API key for the vendor's API is stored in AWS Secrets Manager and is encrypted with a customer managed key in AWS Key Management Service (AWS KMS). The company has deployed its own API into a single AWS Region.

A solutions architect needs to change the API components of the company's API to ensure that the components can run across multiple Regions in an active-active configuration.

Which combination of changes will meet this requirement with the LEAST operational overhead? (Choose three.)

- A. Deploy the API to multiple Regions. Configure Amazon Route 53 with custom domain names that route traffic to each Regional API endpoint. Implement a Route 53 multivalue answer routing policy.
- B. Create a new KMS multi-Region customer managed key. Create a new KMS customer managed replica key in each in-scope Region.
- C. Replicate the existing Secrets Manager secret to other Regions. For each in-scope Region's replicated secret, select the appropriate KMS key.
- D. Create a new AWS managed KMS key in each in-scope Region. Convert an existing key to a multiRegion key. Use the multi-Region key in other Regions.
- E. Create a new Secrets Manager secret in each in-scope Region. Copy the secret value from the existing Region to the new secret in each in-scope Region.
- F. Modify the deployment process for the Lambda function to repeat the deployment across in-scope Regions. Turn on the multi-Region option for the existing API. Select the Lambda function that is deployed in each Region as the backend for the multi-Region API.

Correct Answer: ABC

Community vote distribution

ABC (78%)

BCF (22%)

 **AzureDP900** 1 year, 1 month ago

Deploying the API to multiple Regions (A) allows the company's API to run across multiple Regions, meeting one of the requirements. Creating a new KMS multi-Region customer managed key (B) ensures that the encryption keys used to store the vendor's API secret are accessible across multiple Regions. This allows the company to use a single secret in Secrets Manager across all Regions, reducing operational overhead. Replicating the existing Secrets Manager secret to other Regions (C) is not necessary if you have an AWS-managed key or a multi-region customer managed key (B), but it's still a valid option that can meet the requirement. In fact, the combination of A, B, and C would be the most suitable answer, as they all contribute to ensuring that the API components can run across multiple Regions in an active-active configuration with minimal operational overhead.

upvoted 1 times

 **fab2872** 1 year, 1 month ago

BCF "A" does not create the Lambda in other regions. " The API uses Amazon API Gateway with a Regional API endpoint and an AWS Lambda function for hosting. "

upvoted 2 times

 **obihuang** 1 year, 9 months ago

Why C? Does the new KMS key not need to create a new encrypted secret?

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: ABC

A, B , C are the right options.

upvoted 3 times

 **adelyn|||||||** 1 year, 11 months ago

ABC:

A : deploy the API to other region includes deploy the lambda functions too. so F is not needed.

upvoted 2 times

 **bjexamprep** 1 year, 9 months ago

that's a big assumption

upvoted 2 times

✉ **alexbraila** 1 year ago

Not so big, no. The question states:

The API uses Amazon API Gateway with a Regional API endpoint and an AWS Lambda function for hosting

In my understanding, the above says that the API includes the API Gateway and the Lambda function
upvoted 3 times

✉ **duriselvan** 2 years ago

ABC ANS <https://aws.amazon.com/blogs/compute/building-a-multi-region-serverless-application-with-amazon-api-gateway-and-aws-lambda/>

upvoted 1 times

✉ **HappyPrince** 2 years ago

Selected Answer: BCF

The diagram mentioned here supports F

<https://docs.aws.amazon.com/architecture-diagrams/latest/multi-region-api-gateway-with-cloudfront/multi-region-api-gateway-with-cloudfront.html>

upvoted 2 times

✉ **yuliaqwerty** 2 years ago

it is mention here about AWS Lambda @Edge not simple lambda

upvoted 1 times

✉ **career360guru** 1 year, 11 months ago

This diagram has cloudfront. Option F does not include Cloudfront. So F is not correct.

upvoted 1 times

✉ **Sheyla** 2 years ago

Selected Answer: ABC

ABC is the answer

upvoted 3 times

✉ **shaaam80** 2 years ago

Selected Answer: ABC

Cannot convert single region KMS to multi-region. ABC is the answer

upvoted 3 times

✉ **shaaam80** 2 years ago

Cannot convert single region KMS to multi-region. ABC is the answer

upvoted 3 times

✉ **career360guru** 2 years, 1 month ago

Selected Answer: BCF

B, C and D is right answer. In an Active Active setup with Regional API Gateway endpoint Lambda must be deployed in each Region.
<https://aws.amazon.com/blogs/compute/building-a-multi-region-serverless-application-with-amazon-api-gateway-and-aws-lambda/>

upvoted 2 times

✉ **s61** 2 years, 1 month ago

Selected Answer: ABC

<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-create.html>

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

upvoted 4 times

✉ **KungLjao** 2 years, 1 month ago

Selected Answer: ABC

ABC, others make no sense

upvoted 1 times

Question #318

Topic 1

An online retail company hosts its stateful web-based application and MySQL database in an on-premises data center on a single server. The company wants to increase its customer base by conducting more marketing campaigns and promotions. In preparation, the company wants to migrate its application and database to AWS to increase the reliability of its architecture.

Which solution should provide the HIGHEST level of reliability?

- A. Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon Neptune
- B. Migrate the database to Amazon Aurora MySQL. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in an Amazon ElastiCache for Redis replication group.
- C. Migrate the database to Amazon DocumentDB (with MongoDB compatibility). Deploy the application in an Auto Scaling group on Amazon EC2 instances behind a Network Load Balancer. Store sessions in Amazon Kinesis Data Firehose.
- D. Migrate the database to an Amazon RDS MariaDB Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon ElastiCache for Memcached.

Correct Answer: B

Community vote distribution

B (100%)

✉  **gonzales** Highly Voted 2 years, 1 month ago

Selected Answer: B

Amazon Aurora provides built-in security, continuous backups, serverless compute, up to 15 read replicas, automated multi-Region replication, and integrations with other AWS services.

Redis supports replication: <https://aws.amazon.com/elasticsearch/redis-vs-memcached/>. When adding both solutions B seems the correct answer

upvoted 7 times

✉  **AzureDP900** Most Recent 1 year, 1 month ago

B .. This solution provides a high level of reliability by using Amazon Aurora MySQL as the database service, which:

Is a fully managed relational database service that supports up to 31 synchronous replicas across three Availability Zones (AZs) within a region.

Provides automatic failover and redundancy through Multi-AZ deployments.

Deploying the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer provides:

Elastic scaling of instances to match changing traffic demands.

High availability through load balancing and instance replication across AZs.

Storing sessions in an Amazon ElastiCache for Redis replication group adds:

Caching capabilities with automatic failover and redundancy, ensuring high availability.

upvoted 2 times

✉  **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B is an obvious answer.

upvoted 1 times

✉  **shaaam80** 2 years ago

Selected Answer: B

Neptune, MariaDB & Kinesis Firehose out!

B is the right answer, very reliable with Aurora

upvoted 3 times

✉  **joleneinthebackyard** 2 years, 1 month ago

Selected Answer: B

A, C: store sessions in Neptune or Kinesis Firehose? -> out

D: migrate MySQL to MariaDB instance out of the blue? -> out

B is valid with classic architecture.

upvoted 4 times

✉  **s61** 2 years, 1 month ago

Selected Answer: B

Highest availability is the key

upvoted 2 times

Question #319

A company's solutions architect needs to provide secure Remote Desktop connectivity to users for Amazon EC2 Windows instances that are hosted in a VPC. The solution must integrate centralized user management with the company's on-premises Active Directory. Connectivity to the VPC is through the internet. The company has hardware that can be used to establish an AWS Site-to-Site VPN connection.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy an EC2 instance as a bastion host in the VPC. Ensure that the EC2 instance is joined to the domain. Use the bastion host to access the target instances through RDP.
- B. Configure AWS IAM Identity Center (AWS Single Sign-On) to integrate with the on-premises Active Directory by using the AWS Directory Service for Microsoft Active Directory AD Connector. Configure permission sets against user groups for access to AWS Systems Manager. Use Systems Manager Fleet Manager to access the target instances through RDP.
- C. Implement a VPN between the on-premises environment and the target VPEnsure that the target instances are joined to the on-premises Active Directory domain over the VPN connection. Configure RDP access through the VPN. Connect from the company's network to the target instances.
- D. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy a Remote Desktop Gateway on AWS by using an AWS Quick Start. Ensure that the Remote Desktop Gateway is joined to the domain. Use the Remote Desktop Gateway to access the target instances through RDP.

Correct Answer: B

Community vote distribution

B (52%)

C (46%)

✉  **Pilot** Highly Voted 2 years ago

I think this question is not really about Active Directory or AD Connector.

A secure VPN connection is all you need in this question.

The company has hardware can be used to establish an AWS S2S connection.

In order to have a secure connection, the first thing you have to do is to implement a VPN connection between on-premise and target VPC.

So C is the answer.

upvoted 25 times

✉  **Sab** Highly Voted 2 years, 1 month ago

Selected Answer: B

You cannot join an EC2 to On-prem AD just over the VPN. You should be having an AD connector for the same.

<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>

upvoted 16 times

✉  **bjexamprep** 1 year, 12 months ago

Can you provide the link saying why EC2 cannot join an onprem AD over VPN? As long as the network connectivity is created, I don't see a problem for an EC2 instance to join an on-prem domain.

upvoted 7 times

✉  **tmlong18** 1 year, 11 months ago

<https://aws.amazon.com/tw/blogs/networking-and-content-delivery/integrating-your-directory-services-dns-resolution-with-amazon-route-53-resolvers/>

You should config DHCP and DNS

upvoted 1 times

✉  **bjexamprep** 1 year, 9 months ago

AWS might recommend the consumers to use Active directory connect, but cannot deny using on-prem ADDS directly. And as long as the network is connected, all you need is to create a custom DHCP option set pointing to that ADDS.

upvoted 4 times

✉  **bjexamprep** 1 year, 9 months ago

The article is about "Integrating your Directory Service's DNS resolution with Amazon Route 53 Resolvers". It doesn't mean an EC2 cannot join an onprem AD. If AWS says you can't use onprem AD even the network is connected, that is really a terrible design. I don't think AWS can design it that way.

upvoted 3 times

✉  **aka1177** Most Recent 2 weeks, 6 days ago

Selected Answer: C

AWS Managed AD total costs = standard AWS managed ad per month ~100USD + 2 EC2 (2xDC on your VPC) ~160USD = ~300 USD
 VPN total costs ~ (0.05 USD per hour) =~40USD per month
 so VPN is most cost effective solution ----- answer is C

upvoted 1 times

SaritaH 4 months, 2 weeks ago

Selected Answer: C

C. Site-to-Site VPN + domain join to on-prem AD + RDP over VPN

This uses the company's hardware (already available), so VPN cost is minimal (just AWS VPN hourly + data transfer).

You domain join the EC2 instances directly to the on-prem AD.

You RDP over VPN → no need to expose ports publicly.

Very cost-effective (just VPN connection + normal EC2).

Verdict: Also secure and cheap — but requires that users connect from the corporate network, not from anywhere on the internet unless VPN client is deployed. The question says "connectivity to the VPC is through the internet", so this fits if VPN is used.

upvoted 1 times

3967974 4 months, 2 weeks ago

Selected Answer: C

seems most logical.

upvoted 1 times

AI8282 5 months, 2 weeks ago

Selected Answer: C

If the end user connects to their corporate VPN which has all the routes to all of their other providers (for example maybe they also use GCP, 3rd party services, maybe they also use Azure or have multiple on prem data centers) then C is indeed correct. The user authenticates against their local AD. Their request to the Windows machine is routed by them to AWS and they use their AD credentials.

If the end user directly bypasses the corporate network and goes straight to AWS, B would be right.

Since the first option is way more common from my experience, and the question explicitly stated cost and nothing else, I'm going with C personally.

upvoted 1 times

eesa 9 months, 1 week ago

Selected Answer: B

No need for a bastion host or VPN:

AWS Systems Manager Fleet Manager enables secure RDP access without exposing instances to the internet.

Cost-effective:

No need for dedicated bastion hosts or Remote Desktop Gateway instances.
 AD Connector is cheaper than a fully managed AWS Directory Service.

Seamless Active Directory integration:

IAM Identity Center (AWS SSO) can integrate with on-premises AD via AD Connector.
 Users authenticate with existing AD credentials.

More secure than direct RDP over VPN or bastion hosts:

No public RDP exposure.

No need for additional infrastructure like Remote Desktop Gateway.

upvoted 3 times

AI8282 5 months, 2 weeks ago

The question asked specifically only for the MOST cost-effectively. It doesn't care about ease of management or if it's more secure.

RDP isn't publicly exposed its exposed to IPs within the network only the VPN sends encrypted traffic over the internet with a VPN.

Seamless AD integration at an additional cost and management expense isn't needed when it can just join the domain. It's less cost effective than just using your own on prem AD that you already have setup without paying for an additional service.

The remote desktop scenario isn't using a gateway they are directly using RDP to connect to the specific target machine without a hop in the middle.

Going with C.

upvoted 2 times

85b5b55 10 months, 2 weeks ago

Selected Answer: B

IDC SSO + AWS Directory Service for MS AD connector.

upvoted 2 times

d401c0d 10 months, 3 weeks ago

Selected Answer: C

AWS IAM Identity Center (SSO) with On-Prem AD Authentication

AD Connector allows AWS services and applications to authenticate users against on-prem Active Directory.

When Not to Use AD Connector

- If you require high availability, since AD Connector depends on a stable connection to on-prem AD.
- If you need Group Policy Object (GPO) support in AWS, as AD Connector does not provide this.
- If you need Kerberos authentication or NTLM authentication within AWS, as it only forwards authentication requests.
- If you require full AD domain replication, consider AWS Managed Microsoft AD instead.

upvoted 1 times

JaffaDaffa 11 months, 4 weeks ago

Selected Answer: C

On-prem AD joining via VPN is the most cost effective compared to AD connector

upvoted 2 times

bhanus 1 year ago

Selected Answer: B

Once VPN connectivity is established between on-prem and AWS. RDP should be sufficient to connect.

Secure Remote Desktop connectivity: The VPN provides a secure, encrypted tunnel for RDP traffic between the on-premises network and the EC2 instances in the VPC.

Integration with on-premises Active Directory: By joining the EC2 instances to the existing on-premises Active Directory domain, you leverage the centralized user management that's already in place.

upvoted 2 times

SIJUTHOMASP 1 year ago

Selected Answer: B

The requirement is to use the on-prem AD integrated with the EC2. Although with VPN, RDP can't be established but the AD sync is not possible within EC2 without AD connector. Hence the right answer is B.

upvoted 2 times

bhanus 1 year ago

Selected Answer: C

Questin aks to use the existing S2S Vpn.

The Site-to-Site VPN ensures secure communication between the on-premises environment and the AWS VPC without exposing the EC2 instances to the internet.

I will go with C

upvoted 2 times

dv1 1 year ago

Selected Answer: C

B would be correct if we were not told that hardware for creating a VPN is available.

upvoted 1 times

AzureDP900 1 year, 1 month ago

B

This solution integrates centralized user management with the company's on-premises Active Directory, meets the requirement of secure Remote Desktop connectivity, and is cost-effective.

Configuring AWS Single Sign-On (SSO) with the AD Connector allows users to access EC2 Windows instances using their existing Active Directory credentials, which eliminates the need for additional infrastructure or configuration.

Using Systems Manager Fleet Manager to access the target instances through RDP provides a secure and managed way to connect to EC2 instances without requiring a Remote Desktop Gateway or a bastion host.

upvoted 2 times

0b43291 1 year, 1 month ago

Selected Answer: C

Solution C is the most cost-effective:

Implement a VPN between the on-premises environment and the target VPC, join the EC2 instances to the on-premises Active Directory domain over the VPN, configure RDP access through the VPN, and connect from the company's network. This approach leverages existing infrastructure, requires no additional managed services, utilizes existing hardware for the VPN, and provides direct connectivity without bastion hosts, minimizing costs.

upvoted 1 times

Daniel76 1 year, 1 month ago

Selected Answer: B

1) using AD connector, AWS cloud IAM is authenticated against the on prem AD. extra Managed AD in AWS cloud is not required.

2) A cost effective, secure remote desktop setup is achieved with a fleet manager, accessed via console by IAM identity centre login against the on prem AD. Saving the cost of bastion host , vpn gateway or rdp gateway.

upvoted 2 times

Question #320

A company's compliance audit reveals that some Amazon Elastic Block Store (Amazon EBS) volumes that were created in an AWS account were not encrypted. A solutions architect must implement a solution to encrypt all new EBS volumes at rest.

Which solution will meet this requirement with the LEAST effort?

- A. Create an Amazon EventBridge rule to detect the creation of unencrypted EBS volumes. Invoke an AWS Lambda function to delete noncompliant volumes.
- B. Use AWS Audit Manager with data encryption.
- C. Create an AWS Config rule to detect the creation of a new EBS volume. Encrypt the volume by using AWS Systems Manager Automation.
- D. Turn on EBS encryption by default in all AWS Regions.

Correct Answer: D

Community vote distribution

D (83%)

C (17%)

 **joleneinthebackyard** Highly Voted 2 years, 1 month ago

Selected Answer: D

"must implement a solution to encrypt all NEWWW EBS volumes at rest."
upvoted 7 times

 **PSPaul** Most Recent 1 year ago

Selected Answer: D

C only address existing unencrypted EBS, not preventing future unencrypted

D is so clear "Proactively prevents the creation of unencrypted EBS volumes"
The key word is all new EBS volume
upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

D

The company requires that all new EBS volumes be encrypted at rest.
Turning on EBS encryption by default for all regions will automatically encrypt any new EBS volume created, meeting the compliance requirement with minimal effort.
This approach ensures that encryption is enabled for all new volumes without requiring additional configuration or automation.
upvoted 1 times

 **mark_232323** 1 year, 5 months ago

Selected Answer: C

there is no direct way to encrypt existing unencrypted EBS volumes or snapshots.
<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>
upvoted 1 times

 **Daniel76** 1 year, 1 month ago

The question ask to encrypt new EBS, not the existing.

upvoted 1 times

 **Russ99** 1 year, 6 months ago

Selected Answer: D

I am not picking an answer, I just wanted to point out that EBS encryption is regions specific. option D says : Turn on EBS encryption by default in all AWS Regions. there is no such feature. Option D still appears to be the best answer
upvoted 1 times

 **Daniel76** 1 year, 1 month ago

We may consider it meant to be doing this configuration region by region. It's still require the least effort doing that. :)

upvoted 1 times

 **vibzr2023** 1 year, 11 months ago

Answer: D

Encryption of Amazon Elastic Block Store (Amazon EBS) volumes is important to an organization's data protection strategy. It is an important step in establishing a well-architected environment. Although there is no direct way to encrypt existing unencrypted EBS volumes or snapshots, you can encrypt them by creating a new volume or snapshot.
<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>

upvoted 4 times

career360guru 1 year, 11 months ago

Selected Answer: D

Option D

upvoted 1 times

airgead 2 years, 1 month ago

Selected Answer: D

The keyword is all NEW EBS volumes.

So by make EBS Encryption default, it means all new EBS will be encrypted without additional configuration.

upvoted 2 times

s61 2 years, 1 month ago

Selected Answer: D

Least effort option

upvoted 3 times

gonzales 2 years, 1 month ago

Selected Answer: D

The question states: ' A solutions architect must implement a solution to encrypt all new EBS volumes at rest'
reference: <https://repost.aws/knowledge-center/ebs-automatic-encryption>

upvoted 3 times

KungLjao 2 years, 1 month ago

Selected Answer: C

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>

upvoted 3 times

Question #321

A research company is running daily simulations in the AWS Cloud to meet high demand. The simulations run on several hundred Amazon EC2 instances that are based on Amazon Linux 2. Occasionally, a simulation gets stuck and requires a cloud operations engineer to solve the problem by connecting to an EC2 instance through SSH.

Company policy states that no EC2 instance can use the same SSH key and that all connections must be logged in AWS CloudTrail.

How can a solutions architect meet these requirements?

- A. Launch new EC2 instances, and generate an individual SSH key for each instance. Store the SSH key in AWS Secrets Manager. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the GetSecretValue action. Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client.
- B. Create an AWS Systems Manager document to run commands on EC2 instances to set a new unique SSH key. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement to run Systems Manager documents. Instruct the engineers to run the document to set an SSH key and to connect through any SSH client.
- C. Launch new EC2 instances without setting up any SSH key for the instances. Set up EC2 Instance Connect on each instance. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the SendSSHPublicKey action. Instruct the engineers to connect to the instance by using a browser-based SSH client from the EC2 console.
- D. Set up AWS Secrets Manager to store the EC2 SSH key. Create a new AWS Lambda function to create a new SSH key and to call AWS Systems Manager Session Manager to set the SSH key on the EC2 instance. Configure Secrets Manager to use the Lambda function for automatic rotation once daily. Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client.

Correct Answer: C

Community vote distribution

C (100%)

 **airgead** Highly Voted 2 years, 1 month ago

Selected Answer: C

Answer C is correct with the following reasons:

The keywords: "no EC2 instance can use the same SSH key" AND "all connections must be logged in AWS CloudTrail."

1. EC2 Instance connect using temporary ssh key, one-time SSH keys each time the user connects
2. User connections via EC2 Instance Connect are logged to AWS CloudTrail

upvoted 8 times

 **KungLjao** Highly Voted 2 years, 1 month ago

Selected Answer: C

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/connect-linux-inst-eic.html>

upvoted 7 times

 **Soliner_Bilgi_Teknolojileri** Most Recent 4 months ago

Selected Answer: C

C is correct because EC2 Instance Connect uses the SendSSHPublicKey API call, which is logged in CloudTrail, and it provides a unique, temporary SSH key per connection. This satisfies both requirements: no shared keys and full connection logging.

upvoted 1 times

 **svenkata18** 1 year, 7 months ago

D

Why not D. In C with instance connect, there are 100s of instances and key would be created for each instance manually would take lot of time

upvoted 2 times

 **TonytheTiger** 1 year, 8 months ago

Option C - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-configure-IAM-role.html>

upvoted 1 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: C

Option C - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-configure-IAM-role.html>

upvoted 1 times

 **SKS** 1 year, 8 months ago

can some one justify why cant use AWS system manager (Session manager) option B ??

upvoted 1 times

 **marchelok** 1 year, 6 months ago

No CloudTrail logging for AWS system manager documents.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 2 times

Question #322

Topic 1

A company is migrating mobile banking applications to run on Amazon EC2 instances in a VPC. Backend service applications run in an on-premises data center. The data center has an AWS Direct Connect connection into AWS. The applications that run in the VPC need to resolve DNS requests to an on-premises Active Directory domain that runs in the data center.

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

- A. Provision a set of EC2 instances across two Availability Zones in the VPC as caching DNS servers to resolve DNS queries from the application servers within the VPC.
- B. Provision an Amazon Route 53 private hosted zone. Configure NS records that point to on-premises DNS servers.
- C. Create DNS endpoints by using Amazon Route 53 Resolver. Add conditional forwarding rules to resolve DNS namespaces between the on-premises data center and the VPC.
- D. Provision a new Active Directory domain controller in the VPC with a bidirectional trust between this new domain and the on-premises Active Directory domain.

Correct Answer: C

Community vote distribution

C (100%)

 **trungtd** Highly Voted 1 year, 6 months ago

Option C: Amazon Route 53 Resolver with Conditional Forwarding Rules

Least Administrative Overhead: This option leverages AWS-managed services to handle DNS resolution without the need to manage additional infrastructure or complicated configurations.

Route 53 Resolver Endpoints: Create inbound and outbound endpoints to handle DNS queries between AWS and the on-premises environment.

Inbound Endpoints: Allow on-premises systems to resolve DNS names hosted in AWS.

Outbound Endpoints: Forward DNS queries from AWS to on-premises DNS servers.

Conditional Forwarding Rules: Set up rules to forward specific domain queries (like your Active Directory domain) to the on-premises DNS servers. This ensures seamless DNS resolution for the applications in the VPC.

B: Private hosted zones are intended for DNS records within AWS.

A & D: too much overhead

upvoted 5 times

 **AzureDP900** Most Recent 1 year, 1 month ago

C is right

The company needs to resolve DNS requests from EC2 instances in a VPC to an on-premises Active Directory domain that runs in a data center with an AWS Direct Connect connection.

Amazon Route 53 Resolver is specifically designed for this use case, providing a secure way to enable name resolution between your on-premises and cloud-based resources.

By using Route 53 Resolver, you can create DNS endpoints within the VPC that resolve DNS queries to the on-premises Active Directory domain without requiring any additional infrastructure or overhead in the data center.

upvoted 1 times

 **sarlos** 1 year, 7 months ago

Why not B?

upvoted 2 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: C

Answer is C, least admin overhead using Route 53 resolver with conditional forwarding

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: C

Answer C

upvoted 1 times

 **airgead** 2 years, 1 month ago

Selected Answer: C

Option C: Amazon Route 53 Resolver > Conditional Forwarding
Lower Maintenance than Option A which using EC2.

upvoted 4 times

 **gonzales** 2 years, 1 month ago

Selected Answer: C

To forward DNS queries from your VPCs to your network, you create an outbound endpoint.
reference: <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html>
upvoted 3 times

 **Bad_Mat** 2 years, 1 month ago

I vote for C

upvoted 1 times

 **AM_aws** 2 years, 2 months ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-using-aws-directory-service-and-amazon-route-53/>

upvoted 3 times

Question #323

A company processes environmental data. The company has set up sensors to provide a continuous stream of data from different areas in a city. The data is available in JSON format.

The company wants to use an AWS solution to send the data to a database that does not require fixed schemas for storage. The data must be sent in real time.

Which solution will meet these requirements?

- A. Use Amazon Kinesis Data Firehose to send the data to Amazon Redshift.
- B. Use Amazon Kinesis Data Streams to send the data to Amazon DynamoDB.
- C. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to send the data to Amazon Aurora.
- D. Use Amazon Kinesis Data Firehose to send the data to Amazon Keyspaces (for Apache Cassandra).

Correct Answer: B

Community vote distribution

B (94%)

6%

 **shaam80** Highly Voted  2 years ago

Selected Answer: B

Kinesis Data streams is real-time. Firehose is near real-time. DynamoDB is not a relational DB and does not enforce fixed schemas on its tables. Answer is B

upvoted 9 times

 **FZA24** Most Recent  11 months, 2 weeks ago

Selected Answer: B

Ok B but there is not built-in directly connector between KDS and DynamoDB. All designs show a Lambda between them. Any link to illustrate this design?

upvoted 2 times

 **GabrielShiao** 11 months, 1 week ago

There is no exact correct answer. B is the only the incomplete approach

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

B is correct

Amazon DynamoDB is designed to handle high-traffic, real-time data streams and can store JSON-formatted data without requiring fixed schemas.

Kinesis Data Streams can capture and transform the data in real-time, and by sending it directly to DynamoDB, you can leverage DynamoDB's NoSQL key-value store with flexible schema support.

In fact, using Kinesis Data Streams to feed DynamoDB is a common pattern for building scalable, high-traffic applications that require real-time data processing.

upvoted 1 times

 **053081f** 1 year, 5 months ago

Selected Answer: D

By using Amazon Kinesis Data Firehose to send the data to Amazon Keyspaces, the company can efficiently stream real-time data and store it in a schema-less database, meeting the requirement for flexibility and real-time processing.

Option B is not correct:

While Amazon Kinesis Data Streams can handle real-time data, it does not directly integrate with Amazon DynamoDB. Additional steps are needed to process and insert the data into DynamoDB. Additionally, DynamoDB, though flexible, typically benefits from having a defined schema for efficient access patterns.

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just B

upvoted 2 times

 **anubha.agrahari** 1 year, 6 months ago

B, Firehose+ DynamoDB

<https://aws.amazon.com/blogs/database/working-with-json-data-in-amazon-dynamodb/>

upvoted 2 times

✉  **9f02c8d** 1 year, 6 months ago

Option D - By using Amazon Kinesis Data Firehose to send the environmental data to Amazon Keyspaces (for Apache Cassandra), you can leverage a fully managed streaming data ingestion service and a schema-flexible NoSQL database, meeting the requirements for real-time processing and storage of data without a fixed schema.

upvoted 1 times

✉  **vibzr2023** 1 year, 11 months ago

Answer: B

Option B leverages the strengths of both Kinesis Data Streams and DynamoDB to provide a scalable and real-time solution for ingesting and storing JSON-format data without fixed schemas.

Option A: Kinesis Data Firehose: While suitable for real-time data delivery, it has a limited set of destinations, not including DynamoDB.

upvoted 2 times

✉  **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

✉  **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

Correct B

upvoted 2 times

✉  **salazar35** 2 years, 1 month ago

Selected Answer: B

Load json format to DynamoDB

upvoted 2 times

✉  **Totoroha** 2 years, 1 month ago

Correct is B

Amazon DynamoDB: DynamoDB is a NoSQL database service provided by AWS that does not require fixed schemas

upvoted 3 times

✉  **career360guru** 2 years, 1 month ago

Selected Answer: B

B is right option. D is not correct because Firehose can not write to Keyspaces.

upvoted 1 times

✉  **cypkir** 2 years, 1 month ago

Correct is B

upvoted 1 times

Question #324

A company is migrating a legacy application from an on-premises data center to AWS. The application uses MongoDB as a key-value database. According to the company's technical guidelines, all Amazon EC2 instances must be hosted in a private subnet without an internet connection. In addition, all connectivity between applications and databases must be encrypted. The database must be able to scale based on demand.

Which solution will meet these requirements?

- A. Create new Amazon DocumentDB (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the instance endpoint to connect to Amazon DocumentDB.
- B. Create new Amazon DynamoDB tables for the application with on-demand capacity. Use a gateway VPC endpoint for DynamoDB to connect to the DynamoDB tables.
- C. Create new Amazon DynamoDB tables for the application with on-demand capacity. Use an interface VPC endpoint for DynamoDB to connect to the DynamoDB tables.
- D. Create new Amazon DocumentDB (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the cluster endpoint to connect to Amazon DocumentDB.

Correct Answer: B*Community vote distribution*

B (47%)	D (43%)	9%
---------	---------	----

 **Pilot** Highly Voted 2 years ago

The database must be able to scale based on demand, so Provisioned IOPS volume is out because they will be throttled. A and D are out. EC2 hosted in a private subnet without an internet connection, have to use VPC Endpoint, for DynamoDB, it must be Gateway VPC endpoint.

B is the answer.

upvoted 23 times

 **career360guru** Highly Voted 2 years, 1 month ago

Selected Answer: D

D is right option. Instance endpoint is for connecting specific instance (primary or replica) and not recommended.

upvoted 10 times

 **JMAN1** 1 year, 11 months ago

This time you are wrong. A and D option use provisioned IOPS which is not scalable.

Between B and C. DynamoDB only works with gateway endpoint. Answer is B.

upvoted 4 times

 **Josh1217** 1 year, 6 months ago

It does not say you need automated scaling. You can manually scale DynanoDB with provisioned IOPS.

upvoted 2 times

 **aka1177** Most Recent 1 month ago

Selected Answer: D

The database must be able to scale based on demand - DocumentDB can be scaled on demand just not automatically and with small downtime; There is no requirement for AUTO scaling.

Also MongoDb not always can be migrated to DynamoDB in other hand both support JSON;

So if you think about proper auto scaling its - B, you should use Dynamo DB with GW endpoint, but also you will have pain in the a** to migrate it from MongoDB to DynamoDB;

if you need only to have functionality scale on demand even with provisioned IOPS its - D, and DocumentDB fully support MongoDB is easy to migrate.

upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 4 months ago

Selected Answer: D

B is not correct because DynamoDB is not MongoDB-compatible. The legacy application expects a MongoDB API, so using DynamoDB would require significant application changes. Option D (Amazon DocumentDB with cluster endpoint) natively supports MongoDB, allows private subnet access, encrypted connections, and scales automatically.

upvoted 2 times

 **4845c28** 4 months, 1 week ago

Selected Answer: C

Option C

Gateway endpoint uses internet connection

Interface endpoint can be used with dynamodb:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-ddb>

upvoted 1 times

 **jimee11** 7 months, 2 weeks ago

Selected Answer: D

Need a Mongo compatible DB

upvoted 2 times

 **jimee11** 7 months, 1 week ago

Switching to B. Option D does not talk about how to privately connect to the cluster whereas in option B it references a VPC Gateway endpoint.

upvoted 1 times

 **papan83** 7 months, 3 weeks ago

Selected Answer: B

There is no concept of provision IOPS for DocumentDB , it uses cluster storage so option D (The verbiage) is incorrect .

upvoted 2 times

 **kyo** 10 months, 2 weeks ago

Selected Answer: D

MongoDB (document DB) and DynamoDB (key-value) are different. The question says the app uses MongoDB *as* a key-value store, which is odd. Migrating to DynamoDB means data model changes.

Options A and D include Provisioned IOPS, which is pricey, but the question doesn't mention cost optimization. AWS says DocumentDB scales, so PIOPS likely fits the "scale on demand" requirement. I lean towards D.

If key-value is all that matters, you could use DynamoDB, but that means app changes. With AWS PrivateLink for DynamoDB, B and C are basically the same, making them invalid.

So, D seems best, but it's not a slam dunk.

upvoted 1 times

 **PSPaul** 1 year ago

Selected Answer: D

Should be D

Document DB is good for MongoDB

Manual Scale limit to 15 read replica is not the issue. DynamoDB is not good compatible with MongoDB So, what's next if Dynamo is not support Mongo

upvoted 1 times

 **deepakR20** 1 year ago

Selected Answer: C

There seems to be a typo in the answer. The correct answer is DocumentDB with VPC endpoint, making "C" the right choice.

upvoted 1 times

 **TomTom** 1 year ago

Selected Answer: C

Should be option C.

While gateway endpoints can be secured, they still expose the database to the internet, albeit indirectly.

DynamoDB can use Interface VPC endpoint to connect to DynamoDB Tables.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

B is correct

Using a gateway VPC endpoint for DynamoDB (option B) does provide secure communication between your VPC and DynamoDB, and it meets the company's requirement for encrypted connectivity.

In fact, using a gateway VPC endpoint can help you achieve several benefits, including:

Securely communicate with DynamoDB without exposing your EC2 instances to the public internet

Encrypt all outgoing traffic from your VPC to DynamoDB

Meet security compliance requirements by controlling access to DynamoDB

upvoted 1 times

 **Daniel76** 1 year, 1 month ago

Selected Answer: B

Just summarizing from comments :)

A and D out because provisioned IOPS is not considered scalable.

C is out because DynamoDB only works with gateway vpc endpoint.

B works, because MongoDB only used as key value store, it make sense to replace it with DynamoDB with little impact to the requirements.

upvoted 5 times

 **AloraCloud** 1 year, 2 months ago

The key here is Can you use Amazon Dynamodb to replace a MongoDB used as a key-value database and the answer is YES!

Amazon DynamoDB supports interface VPC endpoints (AWS PrivateLink). This allows you to securely connect to DynamoDB from your VPC without the need for an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

upvoted 2 times

 **KenieOh** 1 year, 3 months ago

Selected Answer: D

D. This is the correct answer. Amazon DocumentDB (with MongoDB compatibility) meets the requirements:

1. It can be hosted in a private subnet without an internet connection, as required by the technical guidelines.
2. Connectivity between the application and the database can be encrypted, as stated in the requirements.
3. Amazon DocumentDB can scale based on demand, which is another requirement mentioned in the question.
4. The use of the cluster endpoint to connect to Amazon DocumentDB is the appropriate approach, as it provides a single, highly available endpoint for the database cluster.

Therefore, option D is the solution that best meets the given requirements.

upvoted 2 times

 **sashenka** 1 year, 2 months ago

DocumentDB's scaling is limited to 15 read replicas and requires manual intervention.

upvoted 2 times

 **Syre** 1 year, 3 months ago

Selected Answer: D

DynamoDB isn't compatible withMongo

upvoted 4 times

 **sashenka** 1 year, 2 months ago

While the application currently uses MongoDB, DynamoDB is suitable for key-value database workloads.

upvoted 2 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: B

EC2 has no such concept called `cluster endpoint`. has to be B

upvoted 3 times

Question #325

Topic 1

A company is running an application on Amazon EC2 instances in the AWS Cloud. The application is using a MongoDB database with a replica set as its data tier. The MongoDB database is installed on systems in the company's on-premises data center and is accessible through an AWS Direct Connect connection to the data center environment.

A solutions architect must migrate the on-premises MongoDB database to Amazon DocumentDB (with MongoDB compatibility).

Which strategy should the solutions architect choose to perform this migration?

- A. Create a fleet of EC2 instances. Install MongoDB Community Edition on the EC2 instances, and create a database. Configure continuous synchronous replication with the database that is running in the on-premises data center.
- B. Create an AWS Database Migration Service (AWS DMS) replication instance. Create a source endpoint for the on-premises MongoDB database by using change data capture (CDC). Create a target endpoint for the Amazon DocumentDB database. Create and run a DMS migration task.
- C. Create a data migration pipeline by using AWS Data Pipeline. Define data nodes for the on-premises MongoDB database and the Amazon DocumentDB database. Create a scheduled task to run the data pipeline.
- D. Create a source endpoint for the on-premises MongoDB database by using AWS Glue crawlers. Configure continuous asynchronous replication between the MongoDB database and the Amazon DocumentDB database.

Correct Answer: B

Community vote distribution

B (100%)

AzureDP900 1 year, 1 month ago

B is right

The company is migrating from MongoDB to Amazon DocumentDB, which requires a database migration service. AWS Database Migration Service (AWS DMS) provides a managed service that can perform this type of migration. Using AWS DMS allows the solutions architect to create a source endpoint for the on-premises MongoDB database using change data capture (CDC), which captures changes made to the original database and replicates them to the target database in real-time. This approach ensures minimal downtime and minimal data loss during the migration process.

upvoted 2 times

career360guru 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

edder 2 years ago

Selected Answer: B

<https://docs.aws.amazon.com/documentdb/latest/developerguide/docdb-migration.html>

upvoted 2 times

shaaam80 2 years ago

Selected Answer: B

B is straightforward. Use DMS to migrate to a Mongo DB Compatible Document DB instance on AWS. Correct!

upvoted 2 times

salazar35 2 years, 1 month ago

Selected Answer: B

B is correct

upvoted 2 times

Totoroha 2 years, 1 month ago

Correct is B

upvoted 2 times

career360guru 2 years, 1 month ago

Selected Answer: B

B is right option.

upvoted 3 times

Question #326

A company is rearchitecting its applications to run on AWS. The company's infrastructure includes multiple Amazon EC2 instances. The company's development team needs different levels of access. The company wants to implement a policy that requires all Windows EC2 instances to be joined to an Active Directory domain on AWS. The company also wants to implement enhanced security processes such as multi-factor authentication (MFA). The company wants to use managed AWS services wherever possible.

Which solution will meet these requirements?

- A. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.
- B. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.
- C. Create an AWS Directory Service Simple AD implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.
- D. Create an AWS Directory Service Simple AD implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.

Correct Answer: B*Community vote distribution*

B (53%)

A (47%)

 **HappyPrince** Highly Voted 2 years ago

Selected Answer: B

I support B as well per this link where EC2 is recommended:
https://docs.aws.amazon.com/workspaces/latest/adminguide/directory_administration.html
upvoted 13 times

 **nublit** Highly Voted 2 years ago

Selected Answer: B

B is correct. The question mention "Windows EC2", no "Windows user desktops". Maybe the Windows EC2 can be Windows Servers.
upvoted 12 times

 **aka1177** Most Recent 2 weeks, 6 days ago

Selected Answer: A

I would say A is the answer - since all services are AWS managed (requirement)
upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 4 months ago

Selected Answer: A

AWS Managed Microsoft AD provides full Active Directory features for domain-joining Windows EC2 instances, and WorkSpaces allows secure, managed access with MFA without exposing EC2 directly. This meets all requirements using managed services.
upvoted 1 times

 **AI8282** 5 months, 2 weeks ago

Selected Answer: A

This is so tough. The docs state if you're using more than 5 workspaces it's better to manage security through a centralized EC2 instance which leads towards B. The question makes no claims of how big the environment is but it eludes to it being small by saying 'A workspace' which would mean just 1 user since it's scoped to user. Nothing in the question highlights more than 5 or large teams either. It explicitly states managed services wherever possible. The workspace meets all of the technical requirements. It just doesn't scale well but the overhead for cost is minimal for a large organization, just a few dollars a workspace a month. I'm going to assume if it was very large they would tell us and not pick 'a workspace' but rather say 'workspaces'. Going with A.

Really tough one with the ambiguity.

upvoted 1 times

 **EzKkk** 2 weeks, 5 days ago

The problem with most of AWS certificate questions is its ambiguity. The question is constructed using hints with only one correct answer, not real life study. So, if the question hints that you have a checklist of requirements, you should only care about ticking all the boxes, not the correctness of the solution really. Learned the hard way :)

upvoted 1 times

 **Curious76** 5 months, 3 weeks ago

Selected Answer: B

I correct my answer after more searches

It aligns with AWS best practices for centralized, robust AD administration using an Amazon EC2 instance.

Why A (WorkSpaces) is not the best:

Even though it's possible to install AD tools on a WorkSpace, AWS recommends against it for anything beyond minimal scale (5+ WorkSpaces). It's less robust than using a dedicated EC2 instance.

Choose Option B because:

It uses AWS Managed Microsoft AD (required for MFA and full AD support).

It aligns with AWS best practices for centralized, robust AD administration using an Amazon EC2 instance.

upvoted 1 times

 **AI8282** 5 months, 3 weeks ago

Selected Answer: A

Going with A.

The company wants to use managed AWS services wherever possible, its explicitly stated. The scope of tasks is well defined and small. I suspect the recommendation is for larger deployments it wouldn't have said 'for MFA' and highlight such lightweight services.

https://docs.aws.amazon.com/workspaces/latest/adminguide/directory_administration.html

upvoted 1 times

 **Odc6cac** 6 months, 1 week ago

Selected Answer: A

A and B both work, but A is definitely more managed, so it has to be A

upvoted 1 times

 **Kaps443** 6 months, 2 weeks ago

Selected Answer: B

This is the most secure, scalable, and cost-effective solution that meets all of the technical and operational requirements.

upvoted 1 times

 **loreant** 6 months, 2 weeks ago

Selected Answer: A

The other options either lack required features (Simple AD options) or use less managed services (EC2 options), making them less suitable for the company's requirements.

upvoted 1 times

 **jimee11** 7 months, 2 weeks ago

Selected Answer: B

There is nothing in the requirements that remotely sways to Workspaces. Amazon Workspaces is costly, requires support to implement/maintain, and is much more complex.

upvoted 1 times

 **kyo** 10 months, 2 weeks ago

Selected Answer: A

The question does mention EC2 specifically, which makes the WorkSpaces solution a little less direct. However, the requirement to use managed AWS services "wherever possible" strongly suggests WorkSpaces for MFA. It's the most managed way to get that done.

So, while EC2 is mentioned, the emphasis on managed services and the need for MFA makes WorkSpaces the most likely answer. It's a trade-off, but the question is probably prioritizing managed services over strict adherence to only using EC2 for everything.

upvoted 2 times

 **GabrielShiao** 11 months ago

Selected Answer: A

use AWS managed services wherever possible.

While both A and B are feasible, A matches the question at most.

upvoted 1 times

 **FZA24** 11 months, 2 weeks ago

Selected Answer: A

The company wants to use managed AWS services wherever possible.

https://docs.aws.amazon.com/workspaces/latest/adminguide/directory_administration.html

You'll perform most administrative tasks for your WorkSpaces directory using directory management tools, such as the Active Directory Administration Tools. However, you'll use the WorkSpaces console to perform some directory-related tasks.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

B is right

The company wants to join all Windows EC2 instances to an Active Directory domain on AWS, which requires a full-featured Active Directory service.

Using AWS Directory Service for Microsoft Active Directory (Enterprise edition) meets this requirement by providing a managed directory service that can be used to manage and secure EC2 instances.

Launching an EC2 instance allows the development team to configure and test domain security configurations in a controlled environment, which is essential for ensuring the correct configuration of the Active Directory

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: A

Option A meets the requirements by using AWS Directory Service for Microsoft Active Directory, a managed service for hosting a full Active Directory domain. It also leverages Amazon WorkSpaces, a managed desktop service supporting MFA, for secure administrative access to configure the Active Directory domain, aligning with the company's preference for managed AWS services.

Option B: While creating an AWS Directory Service for Microsoft Active Directory implementation is correct, launching an EC2 instance for domain security configuration tasks is not the most suitable approach. EC2 instances require additional management overhead, and the company wants to use managed services wherever possible.

upvoted 1 times

 **Daniel76** 1 year, 1 month ago

Selected Answer: B

Add a vote to B as it is dangerously swaying to A.

The EC2 instances referred to should be the managed domain controller to manage EC2 instances that join the domain, to push down GPO policies etc. You can launch more than one for HA.

<https://aws.amazon.com/blogs/security/how-to-increase-the-redundancy-and-performance-of-your-aws-directory-service-for-microsoft-ad-directory-by-adding-domain-controllers/>

upvoted 1 times

Question #327

A company wants to migrate its on-premises application to AWS. The database for the application stores structured product data and temporary user session data. The company needs to decouple the product data from the user session data. The company also needs to implement replication in another AWS Region for disaster recovery.

Which solution will meet these requirements with the HIGHEST performance?

- A. Create an Amazon RDS DB instance with separate schemas to host the product data and the user session data. Configure a read replica for the DB instance in another Region.
- B. Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create a global datastore in Amazon ElastiCache for Memcached to host the user session data.
- C. Create two Amazon DynamoDB global tables. Use one global table to host the product data. Use the other global table to host the user session data. Use DynamoDB Accelerator (DAX) for caching.
- D. Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create an Amazon DynamoDB global table to host the user session data.

Correct Answer: D*Community vote distribution*

D (48%)	C (41%)	10%
---------	---------	-----

 **kadavahuhu** Highly Voted 1 year, 12 months ago

Selected Answer: C

C - DynamoDB is for structured, semi-structured and unstructured data. So it can also hold the product data. Indeed many e-commerce shops use DynamoDB to save the product catalogue. There is nothing in the question that would exclude DynamoDB for the product data. C has caching with DAX so it definitely has a higher performance than D which does not have caching and even no read replica in the same region.

upvoted 17 times

 **titi_r** 1 year, 7 months ago

"C" should be wrong. "B" should be correct.

"A traditional relational database management system (RDBMS) stores data in a normalized relational structure.

[...]

As a NON-relational database service, DynamoDB offers many advantages over traditional relational database management systems."

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-relational-modeling.html>

upvoted 3 times

 **helloworldabc** 1 year, 4 months ago

just D

upvoted 1 times

 **Wardove** Highly Voted 1 year, 10 months ago

Selected Answer: D

Structured Data = RDS

upvoted 9 times

 **fa6d93f** Most Recent 3 months, 1 week ago

Selected Answer: D

Product data stays in RDS (best match for structured relational data).

User session data goes into DynamoDB global table (great for ephemeral + global replication).

Decoupled workloads.

Very high performance.

upvoted 1 times

 **AI8282** 5 months, 2 weeks ago

Selected Answer: D

Memcached isn't supported in elasticache global tables:

<https://aws.amazon.com/elasticache/faqs/#topic-7>

"Global Datastore is supported on ElastiCache version 7.2 for Valkey and ElastiCache version 5.0.6 onward for Redis OSS."

<https://docs.aws.amazon.com/AmazonElastiCache/latest/dg/Redis-Global-Datastore.html>

upvoted 1 times

✉ **0dc6cac** 6 months, 1 week ago

Selected Answer: D

"Structured data" should be a giveaway.....no matter how fast DynamoDB is, it's still a key-value storage. Yeah a simple JSON can be stored effectively, but actual data will never be as fast as a proper RDS.

upvoted 2 times

✉ **loreant** 6 months, 2 weeks ago

Selected Answer: C

DynamoDB with DAX is specifically designed for high-performance use cases, making it the optimal choice when performance is the key requirement.

upvoted 2 times

✉ **jimee11** 7 months, 2 weeks ago

Selected Answer: C

Decoupling: Storing product data and session data in separate DynamoDB tables fully decouples the two data types.

High performance:

DynamoDB is highly performant for both structured and temporary data.

DAX provides microsecond latency caching for DynamoDB queries.

Global replication:

Global Tables provide multi-Region, active-active replication, meeting disaster recovery (DR) needs without complex setup.

Scalability: DynamoDB can scale automatically with minimal operational overhead.

upvoted 2 times

✉ **saptati** 12 months ago

Selected Answer: D

Option C is suboptimal because using DynamoDB for structured product data may be less efficient and more costly than RDS, especially for complex relationships and large datasets. It also adds unnecessary complexity and reduces query flexibility compared to relational databases. In contrast, option D offers a better solution by using RDS for structured product data and DynamoDB for session data, providing an optimal balance of performance, cost-effectiveness, and appropriate technology choices for different data types, while meeting the requirements for decoupling and cross-region replication. Thus, the correct answer is D.

upvoted 3 times

✉ **Miquella_The_Rizzler** 1 year ago

Selected Answer: C

DynamoDB provide microseconds to single digit latency read/write also DynamoDB support structured data just fine

upvoted 2 times

✉ **TomTom** 1 year ago

Selected Answer: C

Option C, provide highest performance.

Creating two Amazon DynamoDB global tables—one for product data and another for user session data—while utilizing DynamoDB Accelerator (DAX) for caching. This setup allows for low-latency access and high throughput, making it ideal for applications with demanding performance requirements. Additionally, DynamoDB's global tables offer built-in replication across regions, ensuring disaster recovery capabilities without compromising performance.

upvoted 3 times

✉ **alexbraila** 1 year ago

Selected Answer: C

This

<https://docs.aws.amazon.com/whitepapers/latest/big-data-analytics-options/amazon-dynamodb.html>

mentions indeed "DynamoDB stores structured data in tables". Based on the question, I would go with C

upvoted 2 times

✉ **0b43291** 1 year, 1 month ago

Selected Answer: C

Option C (using two DynamoDB global tables with DAX caching) provides the highest performance by leveraging the scalability, low latency, and caching capabilities of DynamoDB, while also meeting the requirements of data separation and replication for disaster recovery.

The other options have limitations or drawbacks:

Option A: While separate schemas in an Amazon RDS DB instance can separate the data, it lacks the performance and scalability of DynamoDB. Setting up replication across Regions for RDS is also more complex than using DynamoDB global tables.

Option B: This option separates the data and provides replication, but using Amazon ElastiCache for Memcached for user session data may not match DynamoDB's performance for structured data. Managing two different data stores (RDS and ElastiCache) can also add

complexity.

Option D: While separating the data and providing replication, using RDS for the product data may not be as performant as DynamoDB for structured data, especially with high-traffic workloads.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

D is correct

Decouples the product data from the user session data by using separate storage mechanisms (RDS and DynamoDB). Provides replication in another AWS Region for disaster recovery, which is necessary.

Dynamodb provides low latency reads and writes making it suitable for this application and high traffic application And DynamoDB has built-in features to automatically handle the replication of the user session data across regions.

upvoted 1 times

 **zolthar_z** 1 year, 4 months ago

Selected Answer: D
Answer is D, ElastiCache Global data Store only supports Redis

upvoted 4 times

 **junehc** 1 year, 5 months ago

I think D. ElastiCache for Memcached and DAX are good for read-heavy so they can improve performance, but not a good choice for read and write, and also Memcached – no replication

upvoted 2 times

 **trungtd** 1 year, 6 months ago

Selected Answer: D
Querying structured data on DynamoDB does not provide as good performance as RDS
upvoted 2 times

 **9f02c8d** 1 year, 7 months ago

C - To meet Disaster Recovery requirements & get high performance with DAX
upvoted 1 times

Question #328

A company orchestrates a multi-account structure on AWS by using AWS Control Tower. The company is using AWS Organizations, AWS Config, and AWS Trusted Advisor. The company has a specific OU for development accounts that developers use to experiment on AWS. The company has hundreds of developers, and each developer has an individual development account.

The company wants to optimize costs in these development accounts. Amazon EC2 instances and Amazon RDS instances in these accounts must be burstable. The company wants to disallow the use of other services that are not relevant.

What should a solutions architect recommend to meet these requirements?

- A. Create a custom SCP in AWS Organizations to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the SCP to the development OU.
- B. Create a custom detective control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU.
- C. Create a custom preventive control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU.
- D. Create an AWS Config rule in the AWS Control Tower account. Configure the AWS Config rule to allow the deployment of only burstable instances and to disallow services that are not relevant. Deploy the AWS Config rule to the development OU by using AWS CloudFormation StackSets.

Correct Answer: A

Community vote distribution

A (51%)

C (49%)

✉  **edder**  2 years ago

Selected Answer: C

I don't think it's appropriate to make SCP changes from Organization to an OU managed by Control Tower, as it will cause drift. The recommended method is to set it as Preventive.

<https://docs.aws.amazon.com/controlltower/latest/userguide/controls.html>
<https://docs.aws.amazon.com/controlltower/latest/userguide/governance-drift.html>

upvoted 11 times

✉  **Josh1217**  1 year, 6 months ago

Selected Answer: C

Cannot be A. SCP will create drift and SCPs are used for denying any specific action, not allow as stated in option A.

upvoted 7 times

✉  **AgboolaKun**  3 months, 1 week ago

Selected Answer: A

A is the correct answer.

About C - While AWS Control Tower does support preventive controls, SCPs are actually the mechanism used by Control Tower for preventive controls. Creating a custom preventive control directly in Control Tower is not the proper approach.

In this documentation - <https://docs.aws.amazon.com/controlltower/latest/controlreference/controls.html> that a few respondents referenced, there is a disclaimer there that says "We are transitioning our terminology to align better with industry usage and with other AWS services. During this time, you may see the previous term, guardrail, as well as the new term, control, in our documentation, console, blogs, and videos. These terms are synonymous for our purposes." Please take note.

upvoted 1 times

✉  **Soliner_Bilgi_Teknolojileri** 4 months ago

Selected Answer: A

A is correct because SCPs enforce policies across all accounts in an OU, preventing the use of non-burstable instances and irrelevant services at scale. C is not ideal because preventive Control Tower guardrails are less flexible and harder to manage across hundreds of accounts compared to SCPs.

upvoted 1 times

✉  **Denizka** 4 months, 2 weeks ago

Selected Answer: C

A (Custom SCP in AWS Organizations) → SCPs can block services, but cannot filter by instance type directly (you'd need conditions, but EC2 instance-type restrictions are tricky and not as native as Control Tower preventive guardrails)

upvoted 1 times

 **3967974** 4 months, 2 weeks ago

Selected Answer: C

SCP can not be used to allow.

upvoted 1 times

 **mpgioscia** 4 months, 2 weeks ago

Selected Answer: C

Answer C

upvoted 1 times

 **Deztroyer88** 7 months, 3 weeks ago

Selected Answer: A

No such thing as custom preventive guardrail. You have to set SCP and correct answer is A

upvoted 3 times

 **jimee11** 7 months, 2 weeks ago

Stop. Yes it does.

"Preventive guardrails enforce specific policies to help ensure that your accounts operate in alignment to compliance standards, and disallow actions that lead to policy violations."

<https://docs.aws.amazon.com/wellarchitected/latest/management-and-governance-guide/controls.html>

upvoted 1 times

 **BelloMio** 8 months, 3 weeks ago

Selected Answer: A

All the people that have selected C have never used guardrails in control tower.

There is no such guardrail to do this, plus you do not have the option to create custom guardrails.

upvoted 3 times

 **0b43291** 1 year, 1 month ago

Selected Answer: C

By using a custom preventive control (guardrail) in AWS Control Tower, the company can effectively enforce the deployment of only burstable instances and disallow the use of irrelevant services in the development OU, optimizing costs and ensuring compliance.

The other options are less effective or inappropriate:

Option A: SCPs in AWS Organizations lack the granularity of AWS Control Tower guardrails for this specific use case.

Option B: A detective control would detect non-compliant resources after deployment, not prevent it as required.

Option D: Creating an AWS Config rule and deploying via CloudFormation StackSets is more complex than using purpose-built AWS Control Tower guardrails.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

C is right.

A preventive control (guardrail) is designed to prevent users from taking specific actions if they don't meet the defined criteria. In this case, creating a custom preventive control would allow you to:

Define rules for what types of EC2 instances and RDS instances can be deployed in the development OU.

Specify which services are allowed or disallowed.

This approach provides real-time enforcement of desired resource usage patterns, helping the company prevent non-compliant resources from being created in the first place

upvoted 1 times

 **Halliphax** 1 year, 1 month ago

Selected Answer: C

C.

Cannot be A as SCPs are for deny policies only but the answer specifies creating an SCP to allow and deny.

upvoted 2 times

 **that1guy** 1 year, 2 months ago

Selected Answer: A

As long as you do not update the policies that Control Tower manages, this is fine:

> Don't use AWS Organizations to update service control policies (SCPs) attached to an OU that is registered with AWS Control Tower.

Doing so could result in the controls entering an unknown state, which will require you to reset your landing zone or re-register your OU in AWS Control Tower. Instead, you can create new SCPs and attach those to the OUs rather than editing the SCPs that AWS Control Tower has created.

upvoted 2 times

 **fabriciolff** 1 year, 2 months ago

Selected Answer: C

Preventive guardrails deployed by AWS Control Tower are implemented via service control policies (SCPs).
<https://docs.aws.amazon.com/wellarchitected/latest/management-and-governance-guide/controls.html>

upvoted 2 times

 **ahrentom** 1 year, 2 months ago

Selected Answer: C

I go with C, because of <https://docs.aws.amazon.com/controlltower/latest/userguide/governance-drift.html#drift-scp-attached-ou>

upvoted 2 times

 **mns0173** 1 year, 5 months ago

SCP and "allow" are always incompatible

upvoted 1 times

 **paderni** 1 year, 7 months ago

A -because SCPs are a more straightforward and integrated solution within AWS Organizations for this purpose than preventive controls in Control Tower

upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just c

upvoted 1 times

Question #329

A financial services company runs a complex, multi-tier application on Amazon EC2 instances and AWS Lambda functions. The application stores temporary data in Amazon S3. The S3 objects are valid for only 45 minutes and are deleted after 24 hours.

The company deploys each version of the application by launching an AWS CloudFormation stack. The stack creates all resources that are required to run the application. When the company deploys and validates a new application version, the company deletes the CloudFormation stack of the old version.

The company recently tried to delete the CloudFormation stack of an old application version, but the operation failed. An analysis shows that CloudFormation failed to delete an existing S3 bucket. A solutions architect needs to resolve this issue without making major changes to the application's architecture.

Which solution meets these requirements?

- A. Implement a Lambda function that deletes all files from a given S3 bucket. Integrate this Lambda function as a custom resource into the CloudFormation stack. Ensure that the custom resource has a DependsOn attribute that points to the S3 bucket's resource.
- B. Modify the CloudFormation template to provision an Amazon Elastic File System (Amazon EFS) file system to store the temporary files there instead of in Amazon S3. Configure the Lambda functions to run in the same VPC as the file system. Mount the file system to the EC2 instances and Lambda functions.
- C. Modify the CloudFormation stack to create an S3 Lifecycle rule that expires all objects 45 minutes after creation. Add a DependsOn attribute that points to the S3 bucket's resource.
- D. Modify the CloudFormation stack to attach a DeletionPolicy attribute with a value of Delete to the S3 bucket.

Correct Answer: A
Community vote distribution

A (95%)	5%
---------	----

 **HunkyBunky**  2 years, 1 month ago

Selected Answer: A

It should be A, because with DeletionPolicy you can only keep or delete bucket, but bucket can't be deleted if it is not empty. So better way in that case - to create a lambda function as a custom resource, that will clean bucket before deletion.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html>
<https://awstut.com/en/2022/05/08/create-and-delete-s3-object-by-cfn-custom-resource-en/>

upvoted 19 times

 **dankositze**  1 year, 10 months ago

Selected Answer: A

A because anyone who goes by the name of HunkyBunky must know what they are talking about
 upvoted 7 times

 **aka1177**  1 month ago

Selected Answer: A

the answer is A. C is not much since you can not create an S3 Lifecycle rule that expires all objects 45 minutes after creation. (24h is minimum)

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

A is correct, This solution meets the requirements because it allows you to delete the S3 bucket when deleting the CloudFormation stack, which was failing due to the bucket not being deleted. By implementing a Lambda function as a custom resource, you can trigger it to delete the S3 bucket when the CloudFormation stack is deleted, ensuring that all resources are properly cleaned up.

upvoted 1 times

 **federikinho** 1 year, 9 months ago

100% HunkyBunky explanation. You cannot just delete a non-empty bucket

upvoted 2 times

 **career360guru** 1 year, 11 months ago

Selected Answer: A

Option A. Option C can be a good option but application itself deletes the objects after 24 hours so it will affect and will require changes to application that is clearly stated in question as No.

upvoted 3 times

 **JOn102** 2 years ago

Selected Answer: A

Answer: A, I agree with @HunkyBunkys reasoning

upvoted 1 times

 **shaam80** 2 years ago

Selected Answer: A

Answer is A. S3 buckets can't be deleted if they are not empty. Create a Lambda function to empty the bucket so bucket can be deleted.

upvoted 4 times

 **salazar35** 2 years, 1 month ago

Selected Answer: A

Same as HunkyBunkys comment

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: D

For sure D

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Change to A. Its better option than D

upvoted 1 times

 **sat2008** 1 year, 10 months ago

D is not an option at all it will keep the S3 regardless empty or not and only delete the stack

upvoted 3 times

Question #330

Topic 1

A company has developed a mobile game. The backend for the game runs on several virtual machines located in an on-premises data center. The business logic is exposed using a REST API with multiple functions. Player session data is stored in central file storage. Backend services use different API keys for throttling and to distinguish between live and test traffic.

The load on the game backend varies throughout the day. During peak hours, the server capacity is not sufficient. There are also latency issues when fetching player session data. Management has asked a solutions architect to present a cloud architecture that can handle the game's varying load and provide low-latency data access. The API model should not be changed.

Which solution meets these requirements?

- A. Implement the REST API using a Network Load Balancer (NLB). Run the business logic on an Amazon EC2 instance behind the NLB. Store player session data in Amazon Aurora Serverless.
- B. Implement the REST API using an Application Load Balancer (ALB). Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
- C. Implement the REST API using Amazon API Gateway. Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
- D. Implement the REST API using AWS AppSync. Run the business logic in AWS Lambda. Store player session data in Amazon Aurora Serverless.

Correct Answer: C

Community vote distribution

C (100%)

 **nublit** Highly Voted 2 years ago

Selected Answer: C

C is correct. For Elastic Architecture the best option is API GW + Lambda + DynamoDB
upvoted 8 times

 **Pinina** Most Recent 1 year, 4 months ago

Selected Answer: C

Respuesta c
upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

option C
upvoted 2 times

 **shaam80** 2 years ago

C is correct. API Gateway, Lambda & DynamoDB for session data
upvoted 2 times

 **heatblur** 2 years, 1 month ago

Selected Answer: C

C is the right Answer: APIGW is the ideal choice for exposing the REST API because it can handle varying loads efficiently and scale automatically. API Gateway also integrates seamlessly with AWS Lambda, which is used for the business logic in this solution. This setup allows for easy management and can handle peaks in traffic without manual intervention.
upvoted 3 times

 **Totoroha** 2 years, 1 month ago

C is answer
upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: C

C for sure
upvoted 2 times

Question #331

Topic 1

A company is migrating an application to the AWS Cloud. The application runs in an on-premises data center and writes thousands of images into a mounted NFS file system each night. After the company migrates the application, the company will host the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system.

The company has established an AWS Direct Connect connection to AWS. Before the migration cutover, a solutions architect must build a process that will replicate the newly created on-premises images to the EFS file system.

What is the MOST operationally efficient way to replicate the images?

- A. Configure a periodic process to run the aws s3 sync command from the on-premises file system to Amazon S3. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system.
- B. Deploy an AWS Storage Gateway file gateway with an NFS mount point. Mount the file gateway file system on the on-premises server. Configure a process to periodically copy the images to the mount point.
- C. Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an S3 bucket by using a public VIF. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system.
- D. Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Configure a DataSync scheduled task to send the images to the EFS file system every 24 hours.

Correct Answer: D*Community vote distribution*

D (100%)

 **vip2** 1 year, 5 months ago

Selected Answer: D

see on-premises as source and AWS EFS as target
upvoted 2 times

 **Pics00094** 1 year, 9 months ago

B: no efs connection
upvoted 1 times

 **helloworldabc** 1 year, 4 months ago

just D
upvoted 1 times

 **vibzr2023** 1 year, 11 months ago

Answer: D
Option C is also correct but why you need s3 when DataSync moves data directly from the on-premises NFS to EFS, eliminating intermediate storage and transfer steps, reducing latency and potential bottlenecks.
upvoted 4 times

 **career360guru** 1 year, 11 months ago

Selected Answer: D

Option D
upvoted 1 times

 **zhdetn** 2 years ago

Selected Answer: D

<https://docs.aws.amazon.com/datasync/latest/userguide/datasync-in-vpc.html>
upvoted 3 times

 **Totoroha** 2 years ago

Everybody sure Answer is D?? So:
Amazon Elastic File System (Amazon EFS) does not offer AWS PrivateLink support directly.
upvoted 1 times

 **dutchy1988** 2 years ago

why not? See <https://docs.aws.amazon.com/efs/latest/ug/efs-vpc-endpoints.html>
Seems to be supported

upvoted 1 times

 **GoKhe** 2 years ago

but that is not for EFS APIs, not for data flow.

upvoted 1 times

 **GoKhe** 2 years ago

Also, EFS is accessed over a mount point which can be either an IP or DNS name. Both in private network. so, DX connection is good enough for it. PrivateLink in the answer is meaningless in this case

upvoted 2 times

 **shaam80** 2 years ago

Selected Answer: D

Answer - D. Leveraging AWS PrivateLink with a private VIF ensures a private and secure connection between the on-premises environment and the Amazon EFS file system. This eliminates the need for public internet access.

upvoted 1 times

 **salazar35** 2 years, 1 month ago

Selected Answer: D

D is most likely

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: D

D for sure

upvoted 3 times

Question #332

A company recently migrated a web application from an on-premises data center to the AWS Cloud. The web application infrastructure consists of an Amazon CloudFront distribution that routes to an Application Load Balancer (ALB), with Amazon Elastic Container Service (Amazon ECS) to process requests. A recent security audit revealed that the web application is accessible by using both CloudFront and ALB endpoints. However, the company requires that the web application must be accessible only by using the CloudFront endpoint.

Which solution will meet this requirement with the LEAST amount of effort?

- A. Create a new security group and attach it to the CloudFront distribution. Update the ALB security group ingress to allow access only from the CloudFront security group.
- B. Update ALB security group ingress to allow access only from the com.amazonaws.global.cloudfront.origin-facing CloudFront managed prefix list.
- C. Create a com.amazonaws.region.elasticloadbalancing VPC interface endpoint for Elastic Load Balancing. Update the ALB scheme from internet-facing to internal.
- D. Extract CloudFront IPs from the AWS provided ip-ranges.json document. Update ALB security group ingress to allow access only from CloudFront IPs.

Correct Answer: B

Community vote distribution

B (100%)

 **HunkyBunky**  2 years, 1 month ago

Selected Answer: B

Definitely - B, because you can't assign securityGroup on Cloudfront. Also, security group can have only 60 rules, so you can't add ALL CloudFront IPs into it, so prefix list

upvoted 7 times

 **tgv**  1 year, 4 months ago

Selected Answer: B

B for sure

upvoted 1 times

 **pangchn** 1 year, 9 months ago

Selected Answer: B

<https://aws.amazon.com/blogs/networking-and-content-delivery/limit-access-to-your-origins-using-the-aws-managed-prefix-list-for-amazon-cloudfront/>

upvoted 1 times

 **LazyAutonomy** 1 year, 11 months ago

Selected Answer: B

B, but this is why security architects > solution architects. Any cloudfront distribution, belonging to any account in any org will still have direct access the origin.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

 **zhdetn** 2 years ago

Selected Answer: B

https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-cloudfront-managed-prefix-list/?nc1=h_ls

upvoted 4 times

 **shaaam80** 2 years ago

Selected Answer: B

Allow ingress access to ALB SG only from CloudFront prefix list. Answer - B

upvoted 4 times

 **salazar35** 2 years, 1 month ago

Selected Answer: B

B is right

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 3 times

Question #333

A company hosts a community forum site using an Application Load Balancer (ALB) and a Docker application hosted in an Amazon ECS cluster. The site data is stored in Amazon RDS for MySQL and the container image is stored in ECR. The company needs to provide their customers with a disaster recovery SLA with an RTO of no more than 24 hours and RPO of no more than 8 hours.

Which of the following solutions is the MOST cost-effective way to meet the requirements?

- A. Use AWS CloudFormation to deploy identical ALB, EC2, ECS and RDS resources in two regions. Schedule RDS snapshots every 8 hours. Use RDS multi-region replication to update the secondary region's copy of the database. In the event of a failure, restore from the latest snapshot, and use an Amazon Route 53 DNS failover policy to automatically redirect customers to the ALB in the secondary region.
- B. Store the Docker image in ECR in two regions. Schedule RDS snapshots every 8 hours with snapshots copied to the secondary region. In the event of a failure, use AWS CloudFormation to deploy the ALB, EC2, ECS and RDS resources in the secondary region, restore from the latest snapshot, and update the DNS record to point to the ALB in the secondary region.
- C. Use AWS CloudFormation to deploy identical ALB, EC2, ECS, and RDS resources in a secondary region. Schedule hourly RDS MySQL backups to Amazon S3 and use cross-region replication to replicate data to a bucket in the secondary region. In the event of a failure, import the latest Docker image to Amazon ECR in the secondary region, deploy to the EC2 instance, restore the latest MySQL backup, and update the DNS record to point to the ALB in the secondary region.
- D. Deploy a pilot light environment in a secondary region with an ALB and a minimal resource EC2 deployment for Docker in an AWS Auto Scaling group with a scaling policy to increase instance size and number of nodes. Create a cross-region read replica of the RDS data. In the event of a failure, promote the replica to primary, and update the DNS record to point to the ALB in the secondary region.

Correct Answer: B*Community vote distribution*

B (88%)

12%

 **enk**  1 year, 7 months ago

Selected Answer: B

With an RTO of 24 hours, using the 'Cold' DR solution option B is the cheapest. Option D is a partial on DR solution which I would think would be more expensive in the long run then the 2nd ECR container in another region.

upvoted 9 times

 **shaaam80**  1 year, 7 months ago

Selected Answer: B

Since RTO is 24 hours, no need to have all resources provisioned already on site 2. Take RDS Snapshots every 8 hrs to satisfy RPO. Deploy the environment using CF incase of DR and restore RDS snapshots. Answer - B

upvoted 6 times

 **shaaam80** 1 year, 7 months ago

Also update DNS records to point to DR region

upvoted 1 times

 **Skillbuilder**  10 months, 1 week ago

If you're preparing for the AWS Certified Solutions Architect - Professional (SAP-C02) exam and looking for expert guidance, I highly recommend checking out the AWS Certified Solutions Architect – Associate training(<https://www.netcomlearning.com/certifications/aws-certified-solutions-architect---associate>) by NetCom Learning. This instructor-led training covers core AWS services, networking, security, cost optimization, and hands-on labs with real-world case studies—helping you build a strong foundation before tackling advanced certifications like SAP-C02. Understanding disaster recovery strategies like RTO (Recovery Time Objective) and RPO (Recovery Point Objective) is crucial for AWS architecture. This course will equip you with the skills needed to answer complex exam questions like this one!

upvoted 1 times

 **career360guru** 1 year, 5 months ago

Selected Answer: B

Option B is lowest cost.

upvoted 1 times

 **ProMax** 1 year, 7 months ago

Selected Answer: D

Answer is D

upvoted 3 times

 **heatblur** 1 year, 7 months ago

Selected Answer: B

B. ECR and RDS Snapshots in Two Regions: Storing Docker images in ECR in two regions and copying RDS snapshots to the secondary region is a good strategy. In case of failure, CloudFormation deploys necessary resources in the secondary region, and the DNS is updated. This option is more cost-effective than A, as it doesn't require maintaining a full duplicate environment or multi-region replication constantly.

upvoted 4 times

 **ProMax** 1 year, 7 months ago

Answer is D

upvoted 1 times

 **salazar35** 1 year, 7 months ago

Selected Answer: B

B is the most cost-effective

upvoted 2 times

 **Totoroha** 1 year, 7 months ago

Answer is C

upvoted 3 times

Question #334

A company is migrating its infrastructure to the AWS Cloud. The company must comply with a variety of regulatory standards for different projects. The company needs a multi-account environment.

A solutions architect needs to prepare the baseline infrastructure. The solution must provide a consistent baseline of management and security, but it must allow flexibility for different compliance requirements within various AWS accounts. The solution also needs to integrate with the existing on-premises Active Directory Federation Services (AD FS) server.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Create an organization in AWS Organizations. Create a single SCP for least privilege access across all accounts. Create a single OU for all accounts. Configure an IAM identity provider for federation with the on-premises AD FS server. Configure a central logging account with a defined process for log generating services to send log events to the central account. Enable AWS Config in the central account with conformance packs for all accounts.
- B. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Add OUs as necessary. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server.
- C. Create an organization in AWS Organizations. Create SCPs for least privilege access. Create an OU structure, and use it to group AWS accounts. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server. Configure a central logging account with a defined process for log generating services to send log events to the central account. Enable AWS Config in the central account with aggregators and conformance packs.
- D. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Configure an IAM identity provider for federation with the on-premises AD FS server.

Correct Answer: B

Community vote distribution

B (100%)

 **trungtd** 1 year, 6 months ago

Selected Answer: B

LEAST operational overhead: Control Tower
Integrate with existing AD: IAM Identity Center
upvoted 1 times

 **titi_r** 1 year, 7 months ago

Very poorly worded question. One must CONFIGURE (external) identity provider... but what does it mean:
(B) "connect IAM IC to on-prem ADFS" or
(C) "configure an IAM identity provider"!?!?

We have to guess what's the author wanted to say :

upvoted 1 times

 **AMYMY** 1 year, 10 months ago

Key point is "Flexibility" and least operational overhead, So I'll go with Opt B
upvoted 2 times

 **dankositze** 1 year, 10 months ago

Selected Answer: B

B. because:

(1) "Least amount of operational overhead" requirement is met with Control Tower. Control Tower automates the creation of a well-architected, multi-account environment using best-practice blueprints, and

(2) IAM Identity Center is the recommended approach for workforce authentication and authorization
upvoted 3 times

 **vibzr2023** 1 year, 11 months ago

Answer: B

- A. Manual setup: Requires more manual configuration and maintenance, increasing operational overhead.
- C. Central logging and Config setup: While valuable, these components add complexity and management overhead. Control Tower can automate their setup and management.
- D. IAM identity provider: Doesn't leverage Control Tower's automation and centralized management features, leading to more manual effort.

upvoted 2 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

 **GaryQian** 2 years ago

Selected Answer: B

B is better over D as it mentions OU.

upvoted 2 times

 **salazar35** 2 years, 1 month ago

Selected Answer: B

B over D, should add OU

upvoted 2 times

 **HunkyBunkY** 2 years, 1 month ago

Selected Answer: B

B or C, but B - provides LEAST amount of operational overhead

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 3 times

Question #335

Topic 1

An online magazine will launch its latest edition this month. This edition will be the first to be distributed globally. The magazine's dynamic website currently uses an Application Load Balancer in front of the web tier, a fleet of Amazon EC2 instances for web and application servers, and Amazon Aurora MySQL. Portions of the website include static content and almost all traffic is read-only.

The magazine is expecting a significant spike in internet traffic when the new edition is launched. Optimal performance is a top priority for the week following the launch.

Which combination of steps should a solutions architect take to reduce system response times for a global audience? (Choose two.)

- A. Use logical cross-Region replication to replicate the Aurora MySQL database to a secondary Region. Replace the web servers with Amazon S3. Deploy S3 buckets in cross-Region replication mode.
- B. Ensure the web and application tiers are each in Auto Scaling groups. Introduce an AWS Direct Connect connection. Deploy the web and application tiers in Regions across the world.
- C. Migrate the database from Amazon Aurora to Amazon RDS for MySQL. Ensure all three of the application tiers – web, application, and database – are in private subnets.
- D. Use an Aurora global database for physical cross-Region replication. Use Amazon S3 with cross-Region replication for static content and resources. Deploy the web and application tiers in Regions across the world.
- E. Introduce Amazon Route 53 with latency-based routing and Amazon CloudFront distributions. Ensure the web and application tiers are each in Auto Scaling groups.

Correct Answer: DE*Community vote distribution*

DE (100%)

shaaam80 Highly Voted 2 years ago**Selected Answer: DE**

Aurora Global databases, S3 cross region replication with Route 53, Cloud Front.

Answer - D&E

upvoted 6 times

shaaam80 2 years ago

Also Auto Scaling for Web & Appln tiers

upvoted 1 times

Daniel76 Most Recent 1 year, 1 month ago**Selected Answer: DE**

Wrong options:

A- logical CRR of multiple region replica may affect primary. s3 also should not replace web completely cuz there is still few write operations.

B- Direct connect irrelevant

C- private subnet irrelevant

upvoted 2 times

Dgix 1 year, 9 months ago**Selected Answer: DE**

D and E.

upvoted 1 times

dankositze 1 year, 10 months ago**Selected Answer: DE**

D and E for sure

upvoted 2 times

career360guru 1 year, 11 months ago**Selected Answer: DE**

Option D and E

upvoted 1 times

salazar35 2 years, 1 month ago

Selected Answer: DE

E for sure, D should be additional
upvoted 2 times

 cypkir 2 years, 1 month ago

Selected Answer: DE

Correct
upvoted 3 times

Question #336

An online gaming company needs to optimize the cost of its workloads on AWS. The company uses a dedicated account to host the production environment for its online gaming application and an analytics application.

Amazon EC2 instances host the gaming application and must always be available. The EC2 instances run all year. The analytics application uses data that is stored in Amazon S3. The analytics application can be interrupted and resumed without issue.

Which solution will meet these requirements MOST cost-effectively?

- A. Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use On-Demand Instances for the analytics application.
- B. Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use Spot Instances for the analytics application.
- C. Use Spot Instances for the online gaming application and the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.
- D. Use On-Demand Instances for the online gaming application. Use Spot Instances for the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.

Correct Answer: B

Community vote distribution

B (100%)

 **d401c0d** 10 months, 3 weeks ago

Selected Answer: B

B = EC2 instance savings plan since it must always be available. Spot instances for analytics since it can be interrupted and resumed.
upvoted 2 times

 **dankositze** 1 year, 4 months ago

Selected Answer: B

B all the way
upvoted 2 times

 **career360guru** 1 year, 5 months ago

Selected Answer: B

Option B
upvoted 2 times

 **Russ99** 1 year, 7 months ago

Selected Answer: B

B is correct, Spot instances used for the analytical application can be interrupted and resumed at any time.
upvoted 4 times

 **shaaam80** 1 year, 7 months ago

Selected Answer: B

B... use spot instances for Analytics appn and Instance savings for Gaming
upvoted 4 times

 **salazar35** 1 year, 7 months ago

Selected Answer: B

B no doubt
upvoted 3 times

 **cypkir** 1 year, 7 months ago

Selected Answer: B

Correct
upvoted 1 times

Question #337

A company runs applications in hundreds of production AWS accounts. The company uses AWS Organizations with all features enabled and has a centralized backup operation that uses AWS Backup.

The company is concerned about ransomware attacks. To address this concern, the company has created a new policy that all backups must be resilient to breaches of privileged-user credentials in any production account.

Which combination of steps will meet this new requirement? (Choose three.)

- A. Implement cross-account backup with AWS Backup vaults in designated non-production accounts.
- B. Add an SCP that restricts the modification of AWS Backup vaults.
- C. Implement AWS Backup Vault Lock in compliance mode.
- C. Implement least privilege access for the IAM service role that is assigned to AWS Backup.
- D. Configure the backup frequency, lifecycle, and retention period to ensure that at least one backup always exists in the cold tier.
- E. Configure AWS Backup to write all backups to an Amazon S3 bucket in a designated non-production account. Ensure that the S3 bucket has S3 Object Lock enabled.

Correct Answer: ABC

Community vote distribution

ABC (56%)

ACD (26%)

Other

 **ayadmaula**  2 years ago

Selected Answer: ABC

The solution is A, B and C1.

We need to create a Cross Account Backup -> Put it in a Backup Account -> Control modification to the backup account with SCP.

A. Implement cross-account backup with AWS Backup vaults in designated non-production accounts.
<https://docs.aws.amazon.com/aws-backup/latest/devguide/manage-cross-account.html>

B. Add an SCP that restricts the modification of AWS Backup vaults.
<https://aws.amazon.com/blogs/storage/managing-access-to-backups-using-service-control-policies-with-aws-backup/>

C1. Implement AWS Backup Vault Lock in compliance mode.
<https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html>
upvoted 12 times

 **devalenzuela86**  2 years, 1 month ago

Selected Answer: ACE

ACE for sure

A. Implement cross-account backup with AWS Backup vaults in designated non-production accounts. This will allow the company to securely copy their backups to other accounts that are part of their organization for operational or security reasons1.
C. Implement AWS Backup Vault Lock in compliance mode. This will provide an additional layer of protection and immutability to the backup vaults, preventing any user (including the root user) or AWS from deleting or modifying the backups until the retention period is complete2.
E. Configure the backup frequency, lifecycle, and retention period to ensure that at least one backup always exists in the cold tier. This will help the company to avoid accidental or malicious deletion of backups by enforcing a minimum retention period and moving the backups to a lower-cost storage tier2.
upvoted 8 times

 **tiagobs** 2 years ago

ACD you mean?

upvoted 4 times

 **titi_r** 1 year, 8 months ago

A, C1, D you mean.

upvoted 1 times

 **sashenka**  1 year, 1 month ago

In a ransomware scenario where an attacker gains highly privileged access, both B and C2 can be bypassed. However, C2 (least privilege) offers a slightly stronger defense in this specific case. Here's why:

If the attacker compromises an account with permissions to manage backups but not to manage SCPs, least privilege will still restrict their ability to delete or modify backups directly, even if they can't disable the SCP.

An SCP, on the other hand, provides no additional protection if the attacker has the permissions to modify SCPs.

The Verdict:

While both B and C2 are important security practices, C2 (least privilege) is slightly better than B (SCPs) for mitigating the specific risk of ransomware attacks involving privileged credential compromise. However, neither is as effective as C1 (Vault Lock) and A (Cross-account backups).

upvoted 2 times

 **sashenka** 1 year, 1 month ago

Please delete above. Correction to ABC

upvoted 2 times

 **Sin_Dan** 1 year, 2 months ago

Selected Answer: BCD

Why would you store backup of a production environment in a non-production environment? That itself adds a security risk. And in my opinion removes options A and E from my choice. Also, option D it doesn't address the main concern. And options B, C and E look to solve the purpose effectively at least with the given choices and thus those are my choices.

upvoted 3 times

 **vip2** 1 year, 5 months ago

Selected Answer: ACD

A C(C1) D are correct in questions.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: ACD

ACD are correct, that is A, C1 and D in question.

upvoted 1 times

 **Training** 1 year, 6 months ago

Should be BCD. <https://aws.amazon.com/blogs/storage/managing-access-to-backups-using-service-control-policies-with-aws-backup/>

Cross-Account is not feasible. Hundreds of accounts.

upvoted 1 times

 **trungtd** 1 year, 6 months ago

Selected Answer: ACD

A, C1, D

B is incorrect: concern of compromised credentials: SCPs could potentially be modified by a user with sufficient privileges in the organization's master account.

C2: good for ensuring backup availability but does not directly address resilience against breaches of privileged-user credentials.

E: provide similar benefits to using AWS Backup Vault Lock but is more complex to manage. AWS Backup Vault Lock is specifically designed for backup resilience and is more straightforward to implement within AWS Backup's framework.

upvoted 2 times

 **red_panda** 1 year, 7 months ago

Selected Answer: ABC

A, B, C for me.

upvoted 2 times

 **sarlos** 1 year, 7 months ago

ABC1 is the answer

upvoted 1 times

 **paderni** 1 year, 7 months ago

A. Implement cross-account backup with AWS Backup vaults in designated non-production accounts.

C. Implement AWS Backup Vault Lock in compliance mode.

E. Configure AWS Backup to write all backups to an Amazon S3 bucket in a designated non-production account. Ensure that the S3 bucket has S3 Object Lock enabled.

upvoted 2 times

 **seetpt** 1 year, 7 months ago

Selected Answer: ABC

ABC For me

upvoted 2 times

 **hogtrough** 1 year, 9 months ago

Selected Answer: ABC

ABC is definitely the answer.

D. Configuring backup frequency does not do anything to prevent breaches

E. AWS backup does not currently support S3 as a storage location for backups. You can use AWS backup to make a backup of S3 buckets but cannot use it to store backups.

upvoted 6 times

 **arberod** 1 year, 10 months ago

Selected Answer: ACD

ACD for sure

upvoted 3 times

 **chelbsik** 1 year, 10 months ago

Selected Answer: ABC

ABC seems more reasonable over D(E) - as others mentioned, configuring backup doesn't protect from compromised creds attack.

Moderator, please fix the answer letters order

upvoted 4 times

 **tmlong18** 1 year, 11 months ago

Selected Answer: ABC

ABC1 for sure

upvoted 4 times

 **vibzr2023** 1 year, 11 months ago

Answer : ACC (ACD).. there is typo in question second C should be D, D should be E, E should be F.. saying that the other options
B. SCP restricting vault modification: Offers a good layer of protection, but doesn't directly address the concern of compromised credentials in production accounts.
E. Cold Tier backups: Ensures backup accessibility in case of attacks, but doesn't specifically protect against compromised credentials.
F. S3 Object Lock: Provides immutability within the non-production account, but if that account is breached, backups could still be compromised.

upvoted 5 times

Question #338

A company needs to aggregate Amazon CloudWatch logs from its AWS accounts into one central logging account. The collected logs must remain in the AWS Region of creation. The central logging account will then process the logs, normalize the logs into standard output format, and stream the output logs to a security tool for more processing.

A solutions architect must design a solution that can handle a large volume of logging data that needs to be ingested. Less logging will occur outside normal business hours than during normal business hours. The logging solution must scale with the anticipated load. The solutions architect has decided to use an AWS Control Tower design to handle the multi-account logging process.

Which combination of steps should the solutions architect take to meet the requirements? (Choose three.)

- A. Create a destination Amazon Kinesis data stream in the central logging account.
- B. Create a destination Amazon Simple Queue Service (Amazon SQS) queue in the central logging account.
- C. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Kinesis data stream. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a subscription filter for each log group to send data to the Kinesis data stream.
- D. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Simple Queue Service (Amazon SQS) queue. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a single subscription filter for all log groups to send data to the SQS queue.
- E. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the central logging account and to write the logs to the security tool.
- F. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the member accounts and to write the logs to the security tool.

Correct Answer: ACE

Community vote distribution

ACE (100%)

 **shaaam80** Highly Voted 2 years ago

Selected Answer: ACE

Cloud Watch logs -> Kinesis Data Streams -> Lambda -> Security Tool
ACE

upvoted 8 times

 **carpa_jo** Highly Voted 1 year, 12 months ago

A vs B: Kinesis data stream is a possible destination of CloudWatch Logs subscriptions, SQS isn't --> A
C vs. D: As we had to choose Kinesis only C makes sense.
E vs. F: Difference is that E runs the Lambda function in the central logging account while F runs the Lambda function in the member accounts. So clearly E, as we have streamed the logs to the central accounts Kinesis, which easily can use Lambda for the final processing etc.

upvoted 5 times

 **daveshell** Most Recent 1 year, 1 month ago

While SQS does not fit the bill as it is not a direct location to send CW logs, KDS too does not fit the bill because it cannot scale automatically with load and one has to keep adding shards to increase the throughput. The authors themselves are not that knowledgeable. Only KDF seems to be the most correct thing to do(not mentioned in the options) as it can scale automatically as well has the transformation feature.

upvoted 1 times

 **NoDoubkevo** 1 year, 3 months ago

BDE
Why would you write to the member account? makes no sense.
Why would you use kinesis it says nothing about real time. BD
upvoted 1 times

 **ZAK_11** 1 year, 1 month ago

Kinesis data stream is a possible destination of CloudWatch Logs subscriptions, but SQS isn't
upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: ACE

A, C and E

upvoted 1 times

 **yuliaqwerty** 2 years ago

ACE Kinesis for sure

upvoted 1 times

 **salazar35** 2 years, 1 month ago

Selected Answer: ACE

I vote for ACE

upvoted 4 times

 **HunkBunky** 2 years, 1 month ago

Selected Answer: ACE

Definitely - ACE

upvoted 4 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: ACE

ACE for sure

upvoted 4 times

Question #339

Topic 1

A company is migrating a legacy application from an on-premises data center to AWS. The application consists of a single application server and a Microsoft SQL Server database server. Each server is deployed on a VMware VM that consumes 500 TB of data across multiple attached volumes.

The company has established a 10 Gbps AWS Direct Connect connection from the closest AWS Region to its on-premises data center. The Direct Connect connection is not currently in use by other services.

Which combination of steps should a solutions architect take to migrate the application with the LEAST amount of downtime? (Choose two.)

- A. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the database server VM to AWS.
- B. Use VM Import/Export to import the application server VM.
- C. Export the VM images to an AWS Snowball Edge Storage Optimized device.
- D. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the application server VM to AWS.
- E. Use an AWS Database Migration Service (AWS DMS) replication instance to migrate the database to an Amazon RDS DB instance.

Correct Answer: DE

Community vote distribution

DE (58%)	AD (29%)	9%
----------	----------	----

✉️  **salazar35**  2 years ago

Selected Answer: DE

Should be DE "LEAST amount of downtime"

upvoted 9 times

✉️  **Chris_W_1234** 1 month, 3 weeks ago

D - AWS Server Migration Service has been discontinued.

upvoted 1 times

✉️  **water314**  2 years ago

Selected Answer: AD

AD, RDS Database has max size of less than 500TB, cannot use RDS!

upvoted 8 times

✉️  **m1xa** 2 years ago

Where did you get that? 16TB

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html#Concepts.Storage.GeneralSSD

upvoted 1 times

✉️  **water314** 1 year, 12 months ago

on the page you mentioned

Volume size

100 GiB–64 TiB (16 TiB on RDS for SQL Server)

20 GiB–64 TiB (16 TiB on RDS for SQL Server)

20 GiB–64 TiB (16 TiB on RDS for SQL Server)

upvoted 1 times

✉️  **hogtrough** 1 year, 10 months ago

It does not actually say that the DB itself is 500TB, but that its the total size of storage for both VMs. I really do not like this question. The information provided leaves a lot of room for assumptions.

upvoted 5 times

✉️  **Chris_W_1234**  1 month, 3 weeks ago

Selected Answer: C

Has anyone actually done the transfer speed math? The company needs to transfer $2 \times 500\text{GB} = 1000\text{ TB}$ to the cloud. At a max rate of 1.25GByte/s (10Gbit/s) that means it will take 10 or more days to transfer all that data. I imagine, with proper planning and speedy shipping it will take several days less to move data into the cloud using 5 Snowball storage-optimized devices, which is what the question was asking for. However, the question doesn't have any good second answer that would complement a data transfer via Snowball.

upvoted 1 times

✉ **Woody1848** 1 year, 1 month ago

FYI: Server Migration Service (AWS SMS) has been discontinued.

AWS now recommends the AWS Application Migration Service as the primary migration service.

upvoted 4 times

✉ **Danm86** 1 year, 1 month ago

Answer is AD. This is a crazy question with lot of ambiguity, the question prepared just based of one blog with no clear information :)
Reference: <https://aws.amazon.com/blogs/compute/learn-about-hourly-replication-in-server-migration-service-and-the-ability-to-migrate-large-data-volumes/>

upvoted 1 times

✉ **seetpt** 1 year, 7 months ago

Selected Answer: DE

DE for me

upvoted 1 times

✉ **titi_r** 1 year, 8 months ago

Selected Answer: DE

D and E - "LEAST amount of downtime".

upvoted 2 times

✉ **pangchn** 1 year, 8 months ago

Selected Answer: DE

3 limit here:

RDS volume - 16TB

DMS - 30TB

EBS - 64TB

none of them matching the 500TB of size.

so only possible here:

write forgot the size limit but made the question only focus on comparision between DX and Snowball.

Or, the 500TB size of file is no db or not a single file which can be split to different volumes. And in either case above, DE would be the answer that author is looking for, Simple as Do you know what DMS is.

upvoted 3 times

✉ **TonytheTiger** 1 year, 9 months ago

Selected Answer: AC

Option ACE. You need to create a transit gateway, set up at routing table for communication route rules and finally, create a transit gateway attachment to a VPN .

Option E - <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-vpn-attachments.html>

Option A&C - <https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-isolated.html>

upvoted 1 times

✉ **career360guru** 1 year, 9 months ago

Selected Answer: DE

Option D & E

upvoted 2 times

✉ **Dgix** 1 year, 9 months ago

Selected Answer: AD

There is no requirement to migrate to RDS, hence VMs only.

upvoted 1 times

✉ **Dgix** 1 year, 9 months ago

Change of mind: DE.

upvoted 2 times

✉ **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: DE

D, E SMS and DMS

upvoted 3 times

✉ **TheCloudGuruu** 1 year, 10 months ago

Changing to AD

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Limits.html

upvoted 1 times

✉ **hogtrough** 1 year, 10 months ago

That is temporary storage as a staging area until it replicates to the target server. You can replicate more than 30TB to a target VM using DMS.

"The 30,000-GB quota for storage applies to all your AWS DMS replication instances in a given AWS Region. This storage is used to cache changes if a target can't keep up with a source, and for storing log information."

upvoted 1 times

 **dankositze** 1 year, 10 months ago

Selected Answer: DE

I vote DE

upvoted 5 times

 **07c2d2a** 1 year, 10 months ago

A is wrong. For least downtime you will migrate a Database with DMS.

D & E is the correct answer.

upvoted 3 times

 **ele** 1 year, 10 months ago

Selected Answer: AD

<https://www.amazonaws.cn/en/server-migration-service/faqs/>

Q: What is the difference between EC2 VM Import and Amazon Server Migration Service?

Amazon Server Migration Service is a significant enhancement of EC2 VM Import. The Amazon Server Migration Service provides automated, live incremental server replication and Amazon Web Services Console support. For customers using EC2 VM Import for migration, we recommend using Amazon Server Migration Service.

upvoted 1 times

 **vibzr2023** 1 year, 11 months ago

Answer: DE

Both AWS SMS and AWS DMS offer continuous replication, allowing the application and database to be kept in sync with their AWS counterparts during the migration process. This enables a switchover with minimal downtime.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: BE

Migrate application using VM Export/Import

As DB is MS SQL running on VM, use DMS to Migrate to RDS.

upvoted 3 times

Question #340

Topic 1

A company operates a fleet of servers on premises and operates a fleet of Amazon EC2 instances in its organization in AWS Organizations. The company's AWS accounts contain hundreds of VPCs. The company wants to connect its AWS accounts to its on-premises network. AWS Site-to-Site VPN connections are already established to a single AWS account. The company wants to control which VPCs can communicate with other VPCs.

Which combination of steps will achieve this level of control with the LEAST operational effort? (Choose three.)

- A. Create a transit gateway in an AWS account. Share the transit gateway across accounts by using AWS Resource Access Manager (AWS RAM).
- B. Configure attachments to all VPCs and VPNs.
- C. Setup transit gateway route tables. Associate the VPCs and VPNs with the route tables.
- D. Configure VPC peering between the VPCs.
- E. Configure attachments between the VPCs and VPNs.
- F. Setup route tables on the VPCs and VPNs.

Correct Answer: ABC

Community vote distribution

ABC (72%)

ACE (28%)

 **HappyPrince** Highly Voted 2 years ago

Selected Answer: ABC

As transit gateway follows a hub and spoke model connecting all VPCs and VPNs to it makes more sense. Moreover, between VPCs and VPNs is invalid.

upvoted 16 times

 **HunkyBunky** Highly Voted 2 years, 1 month ago

Selected Answer: ACE

I guess ACE. The company wants to control which VPC will communicate with other VPC, that means that we don't need to setup attachment for all VPCs

upvoted 11 times

 **devalenzuela86** 2 years, 1 month ago

Option E proposes configuring attachments between the VPCs and VPNs. This option is necessary to connect the VPCs and VPNs to the transit gateway.

upvoted 3 times

 **Longc** Most Recent 8 months ago

Selected Answer: ACE

ACE

B (Attach "all" VPCs/VPNs): Overly broad and operationally intensive for hundreds of VPCs. Attachments should be configured selectively.

upvoted 1 times

 **Daniel76** 1 year, 1 month ago

why i dont choose:

D - VPC peering not feasible for hundreds of VPCs

E and F, the attachments and route tables should be done on the transit gateways, not on the VPCs and VPNs.

upvoted 3 times

 **Danm86** 1 year, 1 month ago

Answer ABC is correct. Since C has route tables, which gives Organization to control which VPC can communicate

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: ABC

For those who think that, in relation to the requirement "The company wants to control which VPCs can communicate with other VPCs", option E would be correct, in fact this will be possible through letter C, therefore the answer is A, B, C.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: ABC

C is correct instead of E because all VPCs and VPN attach to Transit-GW

upvoted 1 times

✉ **053081f** 1 year, 5 months ago

Selected Answer: ACE

The question and options include (or lack) some typo errors.

E should be "Configure 'transit gateway' attachments between the VPCs and VPNs."

Then, I think ABE is correct, not ABC.

The company wants to control "which VPCs can communicate with other VPCs." It doesn't say "all VPCs and VPNs".

upvoted 1 times

✉ **053081f** 1 year, 5 months ago

Sorry I think ACE is correct, not ABC.

upvoted 1 times

✉ **seetpt** 1 year, 7 months ago

Selected Answer: ABC

ABC for me

upvoted 3 times

✉ **VerRi** 1 year, 9 months ago

Selected Answer: ACE

We don't need "all"

upvoted 3 times

✉ **hogtrough** 1 year, 9 months ago

Selected Answer: ABC

E. You don't configure attachments between VPCs and VPNs, you configure attachments to both VPCs and VPN from the transit gateway, thus B.

upvoted 6 times

✉ **arberod** 1 year, 10 months ago

Selected Answer: ACE

It is ACE

upvoted 1 times

✉ **tmlong18** 1 year, 11 months ago

Selected Answer: ABC

I go ABC

upvoted 4 times

✉ **vibzr2023** 1 year, 11 months ago

My Answer "ACE" Why B is correct? The question asks "The company wants to control which VPCs can communicate with other VPCs" Saying that Option B is "Involves attaching every single VPC and VPN within the organization directly to the Transit Gateway" whereas Option C focuses on "establishing attachments only between the VPCs that need to communicate with each other and the VPN gateway" Can one explain why B is correct?

upvoted 1 times

✉ **vibzr2023** 1 year, 11 months ago

Typo... I mean Option E

Option E... focuses on "establishing attachments only between the VPCs that need to communicate with each other and the VPN gateway"

Can anyone explain why B is correct?

upvoted 1 times

✉ **career360guru** 1 year, 11 months ago

Selected Answer: ABC

Option A, B, C. Option E looks feasible instead of B but that is not a requirement as company only wants to control VPC to VPC communication.

upvoted 6 times

✉ **ayadmawla** 2 years ago

Selected Answer: ABC

ABC - we need to read the answers as a combination of steps.

upvoted 5 times

✉ **ayadmawla** 2 years ago

One issue though that in order to control which VPC talks to which one, we need to setup route tables on each VPC (E) and not on the transit VPC (C) as that needs to be light. So I am thinking that the choice should be ABE and not ABC.

The specific use case is not mentioned here but this link should give an idea of how route tables need to be configured.
https://docs.aws.amazon.com/vpc/latest/tgw/TGW_Scenarios.html

upvoted 1 times

 **ayadmawla** 2 years ago

This article suggests the use of NACL to control inter-vpc traffic but that option is not available in the question (although there is another question that brings it up)

<https://intuitive.cloud/blog/securing-multi-vpc-connectivity-with-aws-transit-gateway-#:~:text=Use%20security%20groups%20and%20NACLs,connected%20to%20the%20Transit%20Gateway.>

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: ABC

Answer - ABC

upvoted 5 times

Question #341

Topic 1

A company needs to optimize the cost of its application on AWS. The application uses AWS Lambda functions and Amazon Elastic Container Service (Amazon ECS) containers that run on AWS Fargate. The application is write-heavy and stores data in an Amazon Aurora MySQL database.

The load on the application is not consistent. The application experiences long periods of no usage, followed by sudden and significant increases and decreases in traffic. The database runs on a memory optimized DB instance that cannot handle the load.

A solutions architect must design a solution that can scale to handle the changes in traffic.

Which solution will meet these requirements MOST cost-effectively?

- A. Add additional read replicas to the database. Purchase Instance Savings Plans and RDS Reserved Instances.
- B. Migrate the database to an Aurora DB cluster that has multiple writer instances. Purchase Instance Savings Plans.
- C. Migrate the database to an Aurora global database. Purchase Compute Savings Plans and RDS Reserved instances.
- D. Migrate the database to Aurora Serverless v1. Purchase Compute Savings Plans.

Correct Answer: D

Community vote distribution

D (96%)	4%
---------	----

✉  **GaryQian**  2 years ago

Selected Answer: D

Aurora Serverless designed to be handling heavy and unpredictable load while Aurora global table is more on low-latency connection
upvoted 8 times

✉  **salazar35**  2 years, 1 month ago

Selected Answer: D

Aurora Serverless v1 provides a relatively simple, cost-effective option for infrequent, intermittent, or unpredictable workloads
upvoted 6 times

✉  **asquared16**  1 year, 4 months ago

Selected Answer: B

I guess this is a very old question; as of today, Aurora Serverless v1 is going EOL by December, 2024. So, invalid question. But if we still had to make a decision with D, it will be B.

upvoted 1 times

✉  **career360guru** 1 year, 11 months ago

Selected Answer: D

Option D. This question looks incomplete as it does not give options for cost savings opportunity for application layer.

upvoted 2 times

✉  **shaaam80** 2 years ago

Selected Answer: D

Answer D

Aurora Serverless can scale better to handle heavy loads

upvoted 2 times

✉  **Russ99** 2 years ago

Selected Answer: D

Per scenario, the application is write intensive and the load varies due to burst. Aurora Serverless with compute saving plans is the correct answer

upvoted 2 times

✉  **devalenzuela86** 2 years, 1 month ago

Selected Answer: D

D for sure

upvoted 3 times

✉  **devalenzuela86** 2 years, 1 month ago

Change to C. Its most cost effective

upvoted 1 times

Question #342

Topic 1

A company migrated an application to the AWS Cloud. The application runs on two Amazon EC2 instances behind an Application Load Balancer (ALB).

Application data is stored in a MySQL database that runs on an additional EC2 instance. The application's use of the database is read-heavy.

The application loads static content from Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. The static content is updated frequently and must be copied to each EBS volume.

The load on the application changes throughout the day. During peak hours, the application cannot handle all the incoming requests. Trace data shows that the database cannot handle the read load during peak hours.

Which solution will improve the reliability of the application?

- A. Migrate the application to a set of AWS Lambda functions. Set the Lambda functions as targets for the ALB. Create a new single EBS volume for the static content. Configure the Lambda functions to read from the new EBS volume. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.
- B. Migrate the application to a set of AWS Step Functions state machines. Set the state machines as targets for the ALB. Create an Amazon Elastic File System (Amazon EFS) file system for the static content. Configure the state machines to read from the EFS file system. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance.
- C. Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create a new single EBS volume for the static content. Mount the new EBS volume on the ECS cluster. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.
- D. Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create an Amazon Elastic File System (Amazon EFS) file system for the static content. Mount the EFS file system to each container. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance.

Correct Answer: D*Community vote distribution*

D (90%) 10%

 **salazar35** Highly Voted 2 years, 1 month ago

Selected Answer: D

Amazon Aurora MySQL Serverless v2 with a reader DB instance will provide heavy-read
upvoted 5 times

 **AzureDP900** Most Recent 1 year, 1 month ago

By containerizing the application using Amazon Elastic Container Service (Amazon ECS) and AWS Fargate, the company can easily scale the application up or down based on demand, reducing downtime during peak hours. Using an Amazon Elastic File System (Amazon EFS) for static content ensures that data is accessible from multiple containers, reducing the need to copy content to each individual container. Configuring AWS Application Auto Scaling on the ECS cluster allows automatic scaling based on CPU utilization or other custom metrics, ensuring that the application can handle increased load during peak hours. Migrating the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance allows for horizontal scalability and eliminates the need for provisioning and managing database instances manually.

upvoted 1 times

 **wmp7039** 1 year, 12 months ago

Selected Answer: D

The question is not clear on the nature of application and assumes that the application is Linux based, all option would be incorrect if this was a windows app. Given the information D is the best bet.

upvoted 3 times

 **JOn102** 2 years ago

Selected Answer: D

Answer: D

upvoted 2 times

 **shaam80** 2 years ago

Selected Answer: D

D is good. Not sure if Static content on EBS will have an issue when DB is multi AZ as EBS cannot span AZs.
upvoted 4 times

✉ **shaaam80** 2 years ago

"Not sure if Static content on EBS will have an issue when DB is multi AZ as EBS cannot span AZs" - This is for Option C
upvoted 1 times

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

just D

upvoted 1 times

✉ **devalenzuela86** 2 years, 1 month ago

Selected Answer: D

D is better than C.
upvoted 4 times

✉ **devalenzuela86** 2 years, 1 month ago

Selected Answer: C

C for sure
upvoted 2 times

✉ **igor12ghsj577** 1 year, 11 months ago

You always say "for sure". Again you're wrong, that's for sure.
upvoted 12 times

✉ **asquared16** 1 year, 4 months ago

Stop saying "for sure"
upvoted 2 times

Question #343

A solutions architect wants to make sure that only AWS users or roles with suitable permissions can access a new Amazon API Gateway endpoint. The solutions architect wants an end-to-end view of each request to analyze the latency of the request and create service maps.

How can the solutions architect design the API Gateway access control and perform request inspections?

- A. For the API Gateway method, set the authorization to AWS_IAM. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Enable the API caller to sign requests with AWS Signature when accessing the endpoint. Use AWS X-Ray to trace and analyze user requests to API Gateway.
- B. For the API Gateway resource, set CORS to enabled and only return the company's domain in Access-Control-Allow-Origin headers. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.
- C. Create an AWS Lambda function as the custom authorizer, ask the API client to pass the key and secret when making the call, and then use Lambda to validate the key/secret pair against the IAM system. Use AWS X-Ray to trace and analyze user requests to API Gateway.
- D. Create a client certificate for API Gateway. Distribute the certificate to the AWS users and roles that need to access the endpoint. Enable the API caller to pass the client certificate when accessing the endpoint. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

Correct Answer: A

Community vote distribution

A (100%)

 **vibzr2023** Highly Voted 1 year, 11 months ago

Answer: A

Keyword "X-ray" AWS X-Ray is used to trace and analyze user requests to API Gateway, providing an end-to-end view of each request and helping analyze latency. This meets the requirement for creating service maps and analyzing request latency.

upvoted 6 times

 **AzureDP900** Most Recent 1 year, 1 month ago

A is right

By setting the authorization to AWS_IAM for the API Gateway method, only users or roles with suitable permissions can access the endpoint. Using execute-api:Invoke permission ensures that only intended resources are accessible. Enabling API callers to sign requests with AWS Signature adds an additional layer of security, ensuring that only authorized parties have access to the resource.

Using AWS X-Ray for tracing and analyzing user requests provides end-to-end visibility into each request, allowing the solutions architect to analyze latency, create service maps, and identify potential issues or bottlenecks in the system. This approach helps maintain a secure, efficient, and manageable API Gateway endpoint.

upvoted 1 times

 **sarlos** 1 year, 7 months ago

Why not C ?

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Because a Lambda custom authorizer can validate tokens or credentials but is more complex than necessary when AWS_IAM authorization is already suitable.

AWS_IAM can directly control access based on IAM roles and policies, making it simpler and more secure for restricting access.

The question specifies using IAM permissions for access control, making AWS_IAM a better fit, so the correct answer is A.

upvoted 3 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: A

Option A - <https://aws.amazon.com/blogs/aws/apigateway-xray/>

upvoted 1 times

 **Maygam** 1 year, 11 months ago

Selected Answer: A

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

upvoted 3 times

 **ayadmawla** 2 years ago

Selected Answer: A

A - See: <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-control-access-using-iam-policies-to-invoke-api.html#api-gateway-who-can-invoke-an-api-method-using-iam-policies>

upvoted 2 times

 **nublit** 2 years ago

Selected Answer: A

A is correct

upvoted 1 times

 **Russs99** 2 years ago

A is correct, use Iam and role for authentication and x-ray for tracing and analyzing

upvoted 1 times

 **salazar35** 2 years, 1 month ago

Selected Answer: A

A - Use X-ray

upvoted 3 times

 **Totoroha** 2 years, 1 month ago

Answer is A

upvoted 3 times

Question #344

Topic 1

A company is using AWS CodePipeline for the CI/CD of an application to an Amazon EC2 Auto Scaling group. All AWS resources are defined in AWS CloudFormation templates. The application artifacts are stored in an Amazon S3 bucket and deployed to the Auto Scaling group using instance user data scripts. As the application has become more complex, recent resource changes in the CloudFormation templates have caused unplanned downtime.

How should a solutions architect improve the CI/CD pipeline to reduce the likelihood that changes in the templates will cause downtime?

- A. Adapt the deployment scripts to detect and report CloudFormation error conditions when performing deployments. Write test plans for a testing team to run in a non-production environment before approving the change for production.
- B. Implement automated testing using AWS CodeBuild in a test environment. Use CloudFormation change sets to evaluate changes before deployment. Use AWS CodeDeploy to leverage blue/green deployment patterns to allow evaluations and the ability to revert changes, if needed.
- C. Use plugins for the integrated development environment (IDE) to check the templates for errors, and use the AWS CLI to validate that the templates are correct. Adapt the deployment code to check for error conditions and generate notifications on errors. Deploy to a test environment and run a manual test plan before approving the change for production.
- D. Use AWS CodeDeploy and a blue/green deployment pattern with CloudFormation to replace the user data deployment scripts. Have the operators log in to running instances and go through a manual test plan to verify the application is running as expected.

Correct Answer: B

Community vote distribution

B (100%)

 **shaaam80** Highly Voted 2 years ago

Selected Answer: B

Use Code Build to run unit/automated testing. Code Deploy for blue/green deployments
upvoted 11 times

 **AzureDP900** Most Recent 1 year, 1 month ago

B is correct
The current CI/CD pipeline has caused unplanned downtime due to recent resource changes in CloudFormation templates. To minimize this risk, implementing automated testing using AWS CodeBuild will help ensure that changes are thoroughly tested in a non-production environment before being deployed to production.

Using CloudFormation change sets allows for evaluating the impact of changes before deployment, reducing the likelihood of unexpected issues during deployment. Adopting a blue/green deployment pattern with AWS CodeDeploy ensures minimal downtime and provides an option to revert changes if needed. By replacing user data scripts with automated deployments using AWS CodeDeploy, operators no longer have to manually log in to instances for testing, further reducing the likelihood of human error during the deployment process.

upvoted 1 times

 **vibzr2023** 1 year, 11 months ago

Answer: B
Key word "blue/green deployment" and not D.. coz manual testing.
upvoted 2 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B
Option B
upvoted 1 times

 **yuliaqwert** 2 years ago

Agree B is the best here
upvoted 1 times

 **awsdaisuki** 2 years, 1 month ago

Selected Answer: B
BBBBBdaswsfasdfasdfsdf
upvoted 3 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 4 times

Question #345

Topic 1

A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us-east-1 Region. The application should dynamically scale to meet user demand and maintain resiliency. Additionally, the application must have disaster recovery capabilities in an active-passive configuration with the us-west-1 Region.

Which steps should a solutions architect take after creating a VPC in the us-east-1 Region?

- A. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.
- B. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions.
- C. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) that spans both VPCs. Deploy EC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB. Create an Amazon Route 53 record that points to the ALB.
- D. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions.

Correct Answer: B

Community vote distribution

B (100%)

 **AzureDP900** 1 year, 1 month ago

B is right

To implement disaster recovery in an active-passive configuration, you should deploy the application infrastructure across multiple Availability Zones (AZs) in each Region with the primary region being us-east-1. By having an Application Load Balancer (ALB) spanning multiple AZs in the us-east-1 Region and EC2 instances as part of an Auto Scaling group served by this ALB, you can achieve dynamic scaling to meet user demand.

To ensure high availability across both Regions, create an Amazon Route 53 record set with a failover routing policy that directs traffic from the us-west-1 Region to the primary infrastructure in the us-east-1 Region when available. Enable health checks for this Route 53 record set to ensure that traffic is directed away from unhealthy endpoints, providing a seamless user experience while ensuring resiliency and disaster recovery capabilities.

upvoted 1 times

 **asquared16** 1 year, 4 months ago

Selected Answer: B

ALB can't span VPCs in different regions, the key statement in B is "Deploy the same solution in us-west-1"

upvoted 1 times

 **tushar321** 1 year, 8 months ago

B. Peering is not needed here as we dont need syncing of environments

upvoted 3 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: B

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

upvoted 2 times

 **vibzr2023** 1 year, 11 months ago

My Answer is also B but i feel D is also same as B.. Only difference is the words.

B "Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions"

D "Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions"

Can someone clarify???

upvoted 1 times

 **pangchn** 1 year, 9 months ago

D missing keyword Failover

upvoted 3 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

 **yuliaqwerty** 2 years ago

B is correct Route 53 failover policy. A and C wrong - ALB can't span VPC which are in different regions. ALB is region specific service

upvoted 2 times

 **shaaam80** 2 years ago

Answer B. ALB + Autoscaling of EC2 instances on both regions. Route53 with Failover routing policy.

upvoted 4 times

 **salazar35** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 3 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 3 times

 **cypkir** 2 years, 1 month ago

Selected Answer: B

B is the correct answer

upvoted 3 times

Question #346

A company has a legacy application that runs on multiple .NET Framework components. The components share the same Microsoft SQL Server database and communicate with each other asynchronously by using Microsoft Message Queueing (MSMQ).

The company is starting a migration to containerized .NET Core components and wants to refactor the application to run on AWS. The .NET Core components require complex orchestration. The company must have full control over networking and host configuration. The application's database model is strongly relational.

Which solution will meet these requirements?

- A. Host the .NET Core components on AWS App Runner. Host the database on Amazon RDS for SQL Server. Use Amazon EventBridge for asynchronous messaging.
- B. Host the .NET Core components on Amazon Elastic Container Service (Amazon ECS) with the AWS Fargate launch type. Host the database on Amazon DynamoDB. Use Amazon Simple Notification Service (Amazon SNS) for asynchronous messaging.
- C. Host the .NET Core components on AWS Elastic Beanstalk. Host the database on Amazon Aurora PostgreSQL Serverless v2. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) for asynchronous messaging.
- D. Host the .NET Core components on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. Host the database on Amazon Aurora MySQL Serverless v2. Use Amazon Simple Queue Service (Amazon SQS) for asynchronous messaging.

Correct Answer: D

Community vote distribution

D (96%)	4%
---------	----

 **heatblur** Highly Voted 2 years, 1 month ago

Selected Answer: D

Option D seems to be the best fit:

Amazon ECS with EC2 offers the needed control and orchestration capabilities.

Amazon Aurora MySQL Serverless v2 can support the relational database model, though it requires adapting from Microsoft SQL Server to MySQL.

Amazon SQS aligns well with the need for asynchronous messaging and can be a suitable replacement for MSMQ.

upvoted 9 times

 **AzureDP900** Most Recent 1 year, 1 month ago

D is right

To meet all of the company's requirements, they should host their .NET Core components on Amazon ECS using the EC2 launch type to gain full control over networking and host configuration. Hosting the database on Amazon Aurora MySQL Serverless v2 allows them to use a strongly relational database model. Since the original application communicates asynchronously by using Microsoft Message Queue (MSMQ), Amazon Simple Queue Service (Amazon SQS) can be used for an alternative solution.

upvoted 1 times

 **nimbus_00** 1 year, 1 month ago

"company must have full control over networking and host configuration" points to EC2.

"database model is strongly relational" points to RDS/Aurora

upvoted 1 times

 **pangchn** 1 year, 8 months ago

Selected Answer: D

A - eventbridge for replacing MSMQ?

B - dynamodb is not relational

C - Amazon Aurora PostgreSQL serverless v2 is not existing

upvoted 2 times

 **jAtlas7** 1 year ago

Amazon Aurora Serverless v2 does appear to support PostgreSQL:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.Aurora_Fea_Regions_DB-eng.Feature.ServerlessV2.html

upvoted 1 times

 **hogtrough** 1 year, 9 months ago

Selected Answer: D

SQS is perfect solution for queue solution replacement.

upvoted 2 times

career360guru 1 year, 11 months ago

Selected Answer: D

Option D

upvoted 1 times

duriselvan 1 year, 12 months ago

D :- Containerization and Orchestration:

Amazon ECS is a fully managed container orchestration service that can seamlessly manage containerized .NET Core components. The EC2 launch type provides full control over the underlying EC2 instances, enabling customization of networking and host configuration as needed.

2. Relational Database:

Amazon RDS for SQL Server is a managed relational database service that natively supports SQL Server, aligning perfectly with the application's strongly relational database model.

3. Asynchronous Messaging:

D is ans

Amazon SQS offers a reliable and scalable managed message queueing service that mirrors the functionality of MSMQ, ensuring smooth integration with the existing application architecture

upvoted 2 times

yuliaqwert 2 years ago

A Moving from SQL Server to RDS is the easiest. RDS allows network control customisation

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/custom-setup-sqlserver.html#custom-setup-sqlserver.iam-vpc> also App Runner is good for .Net code <https://docs.aws.amazon.com/apprunner/latest/dg/service-source-code-net6.html>

upvoted 1 times

shaaam80 2 years ago

Selected Answer: D

Option D. Since the company wants control over host networking, EC2 is the best choice compared to Fargate or Beanstalk. Aurora MySQL is relational.

upvoted 3 times

salazar35 2 years, 1 month ago

Selected Answer: D

D - DB is strongly relational

upvoted 4 times

VasDev 2 years, 1 month ago

Selected Answer: D

Because the DB is strongly relational

upvoted 3 times

devalenzuela86 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 1 times

devalenzuela86 2 years, 1 month ago

Yes; go with D

upvoted 1 times

cypkir 2 years, 1 month ago

Selected Answer: D

D is the correct answer

upvoted 3 times

Question #347

Topic 1

A solutions architect has launched multiple Amazon EC2 instances in a placement group within a single Availability Zone. Because of additional load on the system, the solutions architect attempts to add new instances to the placement group. However, the solutions architect receives an insufficient capacity error.

What should the solutions architect do to troubleshoot this issue?

- A. Use a spread placement group. Set a minimum of eight instances for each Availability Zone.
- B. Stop and start all the instances in the placement group. Try the launch again.
- C. Create a new placement group. Merge the new placement group with the original placement group.
- D. Launch the additional instances as Dedicated Hosts in the placement groups.

Correct Answer: B*Community vote distribution*

B (88%)

13%

✉  **George88** Highly Voted 2 years, 1 month ago

Should be B

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

If you try to add more instances to the placement group later, or if you try to launch more than one instance type in the placement group, you increase your chances of getting an insufficient capacity error.

If you stop an instance in a placement group and then start it again, it still runs in the placement group. However, the start fails if there isn't enough capacity for the instance.

If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all of the instances in the placement group, and try the launch again. Starting the instances may migrate them to hardware that has capacity for all of the requested instances.

upvoted 18 times

✉  **heatblur** 2 years, 1 month ago

I don't know about this -- you would stop all the instances handling a production load? That would immediately induce downtime

upvoted 2 times

✉  **Jay_2pt0_1** 2 years ago

You're right. Straight from the documentation. Thank you for researching this one.

upvoted 2 times

✉  **AzureDP900** Most Recent 1 year, 1 month ago

B is correct, when you try to add more instances to a placement group with insufficient capacity, it might result in an "Insufficient capacity" error. One way to troubleshoot this issue is by recycling (stopping and starting) all existing instances in the placement group. This helps AWS reschedule your instances to accommodate the new ones. Other options do not solve the root cause of the problem.

upvoted 1 times

✉  **TonytheTiger** 1 year, 9 months ago

Selected Answer: B

Option B - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-capacity>
OR

<https://repost.aws/knowledge-center/ec2-insufficient-capacity-errors>

upvoted 1 times

✉  **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 2 times

✉  **yuliaqwerty** 2 years ago

B <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#concepts-placement-groups>:~:text=stop%20and%20start%20all%20of%20the%20instances%20in%20the%20placement%20group%2C%20and%20try%20the%20launch%20again

upvoted 1 times

✉  **JOn102** 2 years ago

Selected Answer: B

Answer is B

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#concepts-placement-groups>

upvoted 1 times

 dutchy1988 2 years ago

I agree with answer B despite the fact that you will have to incur downtime and (obviously) will discuss that before executing the stop and start. This question does not particular state that there must be no downtime. So my advice would be taking appropriate actions and stop/start placement group instead of add Dedicated Host.

upvoted 3 times

 shaaam80 2 years ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/89258-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

 enk 2 years, 1 month ago

Selected Answer: B

George88's article specifically states B as the answer. However, I agree with Heatblur's reply that in a prod load in real life this is unacceptable unless your app is resilient and can afford a handful of servers being rebooted.

upvoted 3 times

 heatblur 2 years, 1 month ago

Selected Answer: D

Using Dedicated Hosts (D) can be a solution if the capacity issue is persistent and critical, and if the cost and complexity of managing Dedicated Hosts are justifiable.

A: Spread Placement might help but doesn't directly address the capacity issue.

B: All the instances are handling traffic -- stopping them surely won't help.

C: You can't merge placement groups.

upvoted 2 times

 salazar35 2 years, 1 month ago

Selected Answer: B

Vote B

upvoted 2 times

 devalenzuela86 2 years, 1 month ago

A forsure

upvoted 1 times

 devalenzuela86 2 years, 1 month ago

Go with B

upvoted 1 times

 cypkir 2 years, 1 month ago

Selected Answer: B

Answer: B

upvoted 3 times

Question #348

Topic 1

A company has used infrastructure as code (IaC) to provision a set of two Amazon EC2 instances. The instances have remained the same for several years.

The company's business has grown rapidly in the past few months. In response, the company's operations team has implemented an Auto Scaling group to manage the sudden increases in traffic. Company policy requires a monthly installation of security updates on all operating systems that are running.

The most recent security update required a reboot. As a result, the Auto Scaling group terminated the instances and replaced them with new, unpatched instances.

Which combination of steps should a solutions architect recommend to avoid a recurrence of this issue? (Choose two.)

- A. Modify the Auto Scaling group by setting the Update policy to target the oldest launch configuration for replacement.
- B. Create a new Auto Scaling group before the next patch maintenance. During the maintenance window, patch both groups and reboot the instances.
- C. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure monitoring to ensure that target group health checks return healthy after the Auto Scaling group replaces the terminated instances.
- D. Create automation scripts to patch an AMI, update the launch configuration, and invoke an Auto Scaling instance refresh.
- E. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure termination protection on the instances.

Correct Answer: CD

Community vote distribution

CD (48%)	AD (37%)	Other
----------	----------	-------

  **LazyAutonomy** Highly Voted 1 year, 11 months ago

Selected Answer: AD

Terrible, terrible question. All answers are technically wrong. But the answer they want is A & D.

C & E - There is nothing in the question to suggest any requirement that warrants the introduction of a load balancer of any kind. Is there any inbound traffic? Maybe, maybe not. Even if the traffic is inbound, what if they've implemented DNS-round-robin "load balancing" directly to the EC2 public/private IPs (ie no need for ELB)?

There's also nothing to suggest that the "traffic" is consistently the same 24x7, which means they may want the ASG to periodically scale-in and scale-out instances dynamically e.g. in response to EC2 CPU usage. Enabling termination protection will also prevent the ASG from replacing genuinely unhealthy instances, defeating the purpose of having an ASG in the first place.

So that leaves us with A, B & D.

upvoted 14 times

  **LazyAutonomy** 1 year, 11 months ago

But why is ASG terminates those instances?

What's happening is that ansible/puppet/chef/whatever IaC processes are causing OS updates to be applied long after the default 300s health check grace period ends, which means new kernel, new glibc, etc packages are installed, requiring a reboot for the change to take effect. During these reboots, EC2 ASG thinks the instances are unhealthy (EC2 ping health checks will fail) and replaces them with new instances instantiated from an old unpatched AMI.

If you still have lingering doubts about eliminating C and E, then consider the fact that deploying an ELB and turning on ELB health checks in the ASG won't make a difference. A rebooting instance will still get terminated by ASG because EC2 + ELB health checks will fail during the reboot. The instances will probably die faster.

So the problem isn't the reboot. The problem is ASG killing rebooting servers and replacing them with unpatched servers.

upvoted 2 times

  **LazyAutonomy** 1 year, 11 months ago

The simplest solution would be to just increase the health check grace period to something large, like 1 hour, and make sure IaC patches & reboots new instances within the grace period. That will buy you a month before the next senseless EC2 massacre. But nothing resembling that option is being offered here.

The next simplest option is to protect individual EC2 instances from scale-in while they're being rebooted. But nothing resembling that option is being offered here either.

So we're left with somehow updating the kernel/glibc/etc that's baked into the AMI itself, thus altogether avoiding the need for new

instances to reboot in the first place (let's just ignore livepatch methods for the moment).

Yes, we all know that launch configs can't technically be updated in place (and AMIs can't be "patched" either), but if we eliminate D for that reason then we're left A & B, neither of which mention new AMIs or launch configs at all.

upvoted 3 times

 **LazyAutonomy** 1 year, 11 months ago

Can we eliminate B? Yes. I can safely assume the intention of B is to create a new ASG with the same old launch config + existing AMI. The behaviour of new ASG will match the old ASG. Any instance rebooted after the health check grace period ends will get terminated, even during a "maintenance window" (which is not a thing).

Option A wants to modify the termination policy of the existing ASG to "Oldest launch configuration". That's unnecessary but harmless. The default termination policy will do this anyway, and AZ re-balancing always takes precedence even when using a non-default termination policy.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-termination-policies.html>

"Amazon EC2 Auto Scaling always balances instances across Availability Zones first, regardless of which termination policy is used"

upvoted 3 times

 **LazyAutonomy** 1 year, 11 months ago

So where does that leave us?

A - does nothing meaningful at all, but at least it's harmless.

B - working instances will all die on reboot during the "maintenance window" (all at the same time? lol)

C - working instances will die faster when rebooted

D - perfect, except it technically isn't possible to "update" launch configs or "patch" AMIs in place. Bummer.

E - broken instances will never get replaced, defeating the purpose of ASGs.

I think it's safe to conclude the author of this question was just really sloppy with how they worded option D.

To avoid a re-occurrence of this issue, I am compelled by common sense to adopt a more relaxed interpretation of D. If I infer that the intent of D is New AMI + New launch config + Invoke ASG refresh, then I don't actually need to do anything else. D will be enough to prevent re-occurrence. But I have to pair it with a second option. So I'll pair it with A, which sounds good but actually does nothing and is harmless.

upvoted 4 times

 **LazyAutonomy** 1 year, 11 months ago

Answer: A + D.

Terrible, terrible, terrible question.

upvoted 3 times

 **yuliaqwerty** Highly Voted  2 years ago

A and C. D is wrong launch config can't be updated <https://docs.aws.amazon.com/autoscaling/ec2/userguide/change-launch-config.html>

upvoted 6 times

 **d401c0d** Most Recent  10 months, 3 weeks ago

Selected Answer: AD

How to implement:

Access your Auto Scaling group: Navigate to your Auto Scaling group in the AWS console.

Edit the update policy: Go to the "Update policy" section within your Auto Scaling group settings.

Select "oldest" option: Choose the option that specifies to target the oldest launch configuration for replacement when scaling activities occur.

upvoted 1 times

 **deepakR20** 11 months, 3 weeks ago

Selected Answer: AD

A and D

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

A D for me.

Here's why:

A: Modifying the Auto Scaling group to target the oldest launch configuration for replacement ensures that the most recent instance replacements do not reuse unpatched images. This approach helps maintain the security of the newly patched instances.

D: Creating automation scripts to patch an AMI, update the launch configuration, and invoke an Auto Scaling instance refresh enables a more streamlined process for updating instances with the latest security patches. Automation can help ensure consistency in the patching process, reducing the risk of human error.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: CD

The recommended steps to avoid the issue are:

D. Create automation scripts to patch AMI, update launch configuration, and invoke Auto Scaling instance refresh. C. Create ELB in front of Auto Scaling group. Configure monitoring for target group health checks after instance replacement.

Explanation:

- D. Automation scripts ensure new instances launched by Auto Scaling group are patched and secure.
- C. ELB distributes traffic to healthy instances. Monitoring ensures new instances are ready before terminating old ones, maintaining availability during refresh.

upvoted 2 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: CD

D should get the job done.
The rest are redundant. But C seems to be not hurting to do anyway

upvoted 2 times

 **053081f** 1 year, 5 months ago

Selected Answer: AD

While options A and D are considered the most suitable (and safest) answers to the question's requirements, they may not completely solve the problem. For example, if there are 10 instances in an Auto Scaling group (No.1, No.2, No.3 ... No.10), and two of them are unpatched, the Oldest Launch setting would prioritize replacing the older unpatched instances. However, there's a possibility that only No.10 might be scaled in, leaving No.9 still unpatched and active in the group.

upvoted 1 times

 **seetpt** 1 year, 7 months ago

Selected Answer: CD

CD i think
upvoted 2 times

 **titi_r** 1 year, 8 months ago

Selected Answer: AC

A and C.
upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: AD

Sometimes I really hate the AWS exam writers. This questions is on a level to which even they shouldn't plumb.

All of the alternatives are wrong in some way. So you have to guess. Whoever wrote this should be fired.

D, since it addresses the AMI (though "update" is not what you do with an AMI). And then A, for the reasons LazyAutonomy gives.

But wow do I sometimes hate the exam writers. It's one thing to force us to focus on minute details; it's quite another to subject us to their own sloppiness.

upvoted 2 times

 **adelyn|||||||** 1 year, 10 months ago

Answer: A, C

<https://docs.aws.amazon.com/systems-manager/latest/userguide/automation-tutorial-update-patch-windows-ami-autoscaling.html>
upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: CD

Option C and D
upvoted 3 times

 **JMAN1** 1 year, 11 months ago

Selected Answer: DE

A and C does not prevent EC2 to be terminated by security patch. B is very burdened(create new group each time?).
D is poorly worded as it says 'update configuration'.
But I will go with D E.

upvoted 1 times

 **JMAN1** 1 year, 11 months ago

Sorry. E does not prevent terminating from patch.Let me go with C D.

upvoted 1 times

 **Atown** 1 year, 12 months ago

Selected Answer: CD

CD
Answer is worded a bit poorly but this is correct.
upvoted 4 times

 **awsamar** 2 years ago

Selected Answer: AC

D is out

AC then

upvoted 2 times

 **awsamar** 2 years ago

Option D is out because it says to "update launch configuration"

AWS Auto Scaling launch configurations cannot be updated directly. Once a launch configuration is created, it cannot be modified; instead, a new one must be created to reflect any changes

upvoted 2 times

Question #349

Topic 1

A team of data scientists is using Amazon SageMaker instances and SageMaker APIs to train machine learning (ML) models. The SageMaker instances are deployed in a VPC that does not have access to or from the internet. Datasets for ML model training are stored in an Amazon S3 bucket. Interface VPC endpoints provide access to Amazon S3 and the SageMaker APIs.

Occasionally, the data scientists require access to the Python Package Index (PyPI) repository to update Python packages that they use as part of their workflow. A solutions architect must provide access to the PyPI repository while ensuring that the SageMaker instances remain isolated from the internet.

Which solution will meet these requirements?

- A. Create an AWS CodeCommit repository for each package that the data scientists need to access. Configure code synchronization between the PyPI repository and the CodeCommit repository. Create a VPC endpoint for CodeCommit.
- B. Create a NAT gateway in the VPC. Configure VPC routes to allow access to the internet with a network ACL that allows access to only the PyPI repository endpoint.
- C. Create a NAT instance in the VPC. Configure VPC routes to allow access to the internet. Configure SageMaker notebook instance firewall rules that allow access to only the PyPI repository endpoint.
- D. Create an AWS CodeArtifact domain and repository. Add an external connection for public:pypi to the CodeArtifact repository. Configure the Python client to use the CodeArtifact repository. Create a VPC endpoint for CodeArtifact.

Correct Answer: D

Community vote distribution

D (100%)

 **salazar35** Highly Voted 2 years, 1 month ago

Selected Answer: D

CodeArtifact allows you to store artifacts using popular package managers and build tools like Maven, Gradle, npm, Yarn, Twine, pip, NuGet, and SwiftPM

upvoted 8 times

 **aka1177** Most Recent 1 month ago

Selected Answer: D

D for sure

upvoted 1 times

 **svenkata18** 1 year, 8 months ago

Why not C , can use NAT gateway and Sagemaker instance notebook rules as there were not asking for cost-effective
upvoted 1 times

 **Daniel76** 1 year, 4 months ago

Requirement is to isolate Sagemaker instances from the Internet

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: D

Option D

upvoted 1 times

 **vibzr2023** 1 year, 11 months ago

Answer : D

Not option C

By using CodeArtifact, you can effectively meet the requirements of providing access to PyPI while maintaining isolation, security, and cost-efficiency for the SageMaker instances. NAT are additional costs... which you can avoid

upvoted 2 times

 **carpa_jo** 1 year, 12 months ago

Selected Answer: D

<https://aws.amazon.com/blogs/machine-learning/private-package-installation-in-amazon-sagemaker-running-in-internet-free-mode/>

upvoted 3 times

 **heatblur** 2 years ago

Selected Answer: D

D is the answer.

It can't be A -- CodeCommit is primarily a source control service and does not directly synchronize with external repositories like PyPI. This option requires significant overhead in maintaining the sync.

upvoted 2 times

  **devalenzuela86** 2 years, 1 month ago**Selected Answer: D**

D for sure

upvoted 2 times

  **cypkir** 2 years, 1 month ago**Selected Answer: D**

Answer: D

upvoted 1 times

Question #350

A solutions architect works for a government agency that has strict disaster recovery requirements. All Amazon Elastic Block Store (Amazon EBS) snapshots are required to be saved in at least two additional AWS Regions. The agency also is required to maintain the lowest possible operational overhead.

Which solution meets these requirements?

- A. Configure a policy in Amazon Data Lifecycle Manager (Amazon DLM) to run once daily to copy the EBS snapshots to the additional Regions.
- B. Use Amazon EventBridge to schedule an AWS Lambda function to copy the EBS snapshots to the additional Regions.
- C. Setup AWS Backup to create the EBS snapshots. Configure Amazon S3 Cross-Region Replication to copy the EBS snapshots to the additional Regions.
- D. Schedule Amazon EC2 Image Builder to run once daily to create an AMI and copy the AMI to the additional Regions.

Correct Answer: A
Community vote distribution

A (89%)

11%

 **heatblur** Highly Voted 2 years ago

Selected Answer: A

The best answer is A: configuring Amazon Data Lifecycle Manager to automate the copying of EBS snapshots to additional regions, is the most suitable solution. It meets the requirement of minimal operational overhead while ensuring that snapshots are stored in multiple regions for disaster recovery. This approach is straightforward and leverages AWS's native capabilities for snapshot management.

Can't be C...EBS snapshots are not stored in S3 in a direct manner that would allow the use of S3 Cross-Region Replication. This option seems to misunderstand the nature of EBS snapshots and S3 integration.

upvoted 8 times

 **titi_r** 1 year, 8 months ago

Indeed, you can do a cross-Region snapshot copy with AWS Backup, but ans "C" states to do a local-Region copy, then from the S3 console to run a S3 cross-Region replication, which is NOT possible. See the text and link below.

"EBS snapshots are stored in Amazon S3, in S3 buckets that you CAN'T access directly. You can create and manage your snapshots using the Amazon EC2 console or the Amazon EC2 API. You can't access your snapshots using the Amazon S3 console or the Amazon S3 API."

<https://docs.aws.amazon.com/ebs/latest/userguide/ebs-snapshots.html>

So, correct ans is "A".

upvoted 2 times

 **ftaws** 1 year, 11 months ago

EBS snapshot are stored in S3.

upvoted 1 times

 **mark_232323** Most Recent 1 year, 5 months ago

Selected Answer: A

CRR is a feature in AWS S3 that automatically replicates data from one S3 bucket in one AWS region to another S3 bucket in a different region.

the requirements here to send backup to two regions

upvoted 1 times

 **mark_232323** 1 year, 5 months ago

Selected Answer: A

AWS Backup does not store snapshots in Amazon S3: AWS Backup stores the EBS snapshots in the same AWS Region where the EBS volumes reside. It does not store the snapshots in Amazon S3 buckets.

upvoted 1 times

 **titi_r** 1 year, 8 months ago

Selected Answer: A

"A" - correct.

upvoted 1 times

 **SAExamTaker** 1 year, 10 months ago

"You can now copy snapshots across regions using Data Lifecycle Manager (DLM). You can enable policies which, along with create, can now also copy snapshots to one or more AWS region(s). Copies can be scheduled for up to three regions from a single policy and retention periods are set for each region separately."

<https://aws.amazon.com/about-aws/whats-new/2019/12/amazon-data-lifecycle-manager-enables-automation-snapshot-copy-via-policies/>

upvoted 3 times

✉ **Russs99** 1 year, 10 months ago

Selected Answer: C

A (Amazon Data Lifecycle Manager) could work, but it's more suitable for lifecycle management tasks such as creating, retaining, and deleting EBS snapshots based on defined policies. It doesn't inherently handle cross-region replication.

upvoted 1 times

✉ **career360guru** 1 year, 11 months ago

Selected Answer: A

Option A. EBS Data Lifecycle manager supports automated cross region snapshot.

<https://aws.amazon.com/about-aws/whats-new/2019/12/amazon-data-lifecycle-manager-enables-automation-snapshot-copy-via-policies/>

upvoted 2 times

✉ **Maygam** 1 year, 11 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>

It help's - Create disaster recovery backup policies that back up data to isolated Regions or accounts.

upvoted 2 times

✉ **duriselvan** 1 year, 12 months ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-ami-policy.html>

upvoted 1 times

✉ **duriselvan** 1 year, 12 months ago

C ans

a IS not correct

Snapshots must be archived in the same Region in which they were created. If you enabled cross-Region copy and snapshot archiving, Amazon Data Lifecycle Manager does not archive the snapshot copy.

upvoted 1 times

✉ **yuliaqwerty** 2 years ago

C Amazon data lifecycle manager can't copy snapshots. AWS backup has cross-Region copy feature [https://aws.amazon.com/getting-started/hands-on/amazon-ebs-backup-and-restore-using-aws-backup/#:~:text=same%20AWS%20Region%20\(-,however%2C%20see%20step%203.2%20for%20information%20on%20cross%2DRegion%20copy,-\).%20This%20tutorial%20uses](https://aws.amazon.com/getting-started/hands-on/amazon-ebs-backup-and-restore-using-aws-backup/#:~:text=same%20AWS%20Region%20(-,however%2C%20see%20step%203.2%20for%20information%20on%20cross%2DRegion%20copy,-).%20This%20tutorial%20uses)

upvoted 1 times

✉ **Jay_2pt0_1** 1 year, 12 months ago

Since 2019, DLM can copy to other regions. See <https://aws.amazon.com/about-aws/whats-new/2019/12/amazon-data-lifecycle-manager-enables-automation-snapshot-copy-via-policies/> I'm pretty sure the answer is A

upvoted 1 times

✉ **knark446** 2 years ago

Selected Answer: A

For me A would be the solution.

C will imply copying the ebs snapshots to s3, why not using directly the AWS Backup cross-region backup copy feature?

upvoted 1 times

✉ **dutchy1988** 2 years ago

<https://aws.amazon.com/about-aws/whats-new/2020/12/amazon-data-lifecycle-manager-now-automates-copying-ebs-snapshots-across-accounts/>

fully automated and no overhead. Answer A

upvoted 2 times

✉ **jpes** 2 years, 1 month ago

Selected Answer: C

Answer is C

upvoted 1 times

✉ **Leo0802** 2 years, 1 month ago

should be C

upvoted 1 times

✉ **Totoroha** 2 years, 1 month ago

Answer is C. Therefore, option C is the most efficient and cost-effective solution that aligns with the agency's strict disaster recovery requirements while minimizing operational complexity.

upvoted 2 times

✉ **salazar35** 2 years, 1 month ago

How AWS Backup create Snapshot?

upvoted 1 times

✉ **Totoroha** 2 years ago

yes. i'm researching and saw that: <https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/new-ebs-volume-backups.html#amazon-dlm>

upvoted 1 times

Question #351

A company has a project that is launching Amazon EC2 instances that are larger than required. The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT. The company wants to allow only the launch of t3.small EC2 instances by developers in the project's account. These EC2 instances must be restricted to the us-east-2 Region.

What should a solutions architect do to meet these requirements?

- A. Create a new developer account. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company's organization in AWS Organizations. Enforce a tagging policy that denotes Region affinity.
- B. Create an SCP that denies the launch of all EC2 instances except t3.small EC2 instances in us-east-2. Attach the SCP to the project's account.
- C. Create and purchase a t3.small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag.
- D. Create an IAM policy that allows the launch of only t3.small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the project's account.

Correct Answer: D*Community vote distribution*

D (91%)	9%
---------	----

 **George88** Highly Voted  1 year, 7 months ago

Should be D.

Question says "The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT"

You need organisation for SCP.

upvoted 14 times

 **trungtd** Most Recent  1 year ago

Selected Answer: D

only possible way

upvoted 1 times

 **svenkata18** 1 year, 1 month ago

C

Why not C as developers has to select only T3.small. why can't we purchase RI with only T3.small

upvoted 1 times

 **Russ99** 1 year, 4 months ago

Selected Answer: D

option D is the only answer. the scenario clearly stated the IT team in this project cannot be part of the organization.

upvoted 2 times

 **career360guru** 1 year, 5 months ago

Selected Answer: D

Option D

upvoted 1 times

 **vibzr2023** 1 year, 5 months ago

Answer D:

Option B: An SCP can manage IAM permissions across an organization, but the project account isn't part of the organization.

upvoted 1 times

 **ayadmawla** 1 year, 6 months ago

Selected Answer: D

SCP can be applied only to those users and roles which are managed by accounts that are part of any organization

See: <https://digitalcloud.training/aws-scp-mastering-aws-service-control-policies/#:~:text=SCP%20can%20be%20applied%20only,including%20the%20account's%20root%20user>.

upvoted 1 times

 **Russ99** 1 year, 6 months ago

Selected Answer: D

D meets the needs with an IAM-based access control policy specific to the standalone project account and its developers' roles/groups.

upvoted 1 times

 **Maygam** 1 year, 7 months ago

Selected Answer: B

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_ec2.html#example-ec2-1

upvoted 1 times

 **albert_kuo** 9 months, 3 weeks ago

due to policy restrictions to keep this activity outside of corporate IT

upvoted 1 times

 **cypkir** 1 year, 7 months ago

Selected Answer: D

Answer: D

upvoted 4 times

Question #352

Topic 1

A scientific company needs to process text and image data from an Amazon S3 bucket. The data is collected from several radar stations during a live, time-critical phase of a deep space mission. The radar stations upload the data to the source S3 bucket. The data is prefixed by radar station identification number.

The company created a destination S3 bucket in a second account. Data must be copied from the source S3 bucket to the destination S3 bucket to meet a compliance objective. This replication occurs through the use of an S3 replication rule to cover all objects in the source S3 bucket.

One specific radar station is identified as having the most accurate data. Data replication at this radar station must be monitored for completion within 30 minutes after the radar station uploads the objects to the source S3 bucket.

What should a solutions architect do to meet these requirements?

- A. Setup an AWS DataSync agent to replicate the prefixed data from the source S3 bucket to the destination S3 bucket. Select to use all available bandwidth on the task, and monitor the task to ensure that it is in the TRANSFERRING status. Create an Amazon EventBridge rule to initiate an alert if this status changes.
- B. In the second account, create another S3 bucket to receive data from the radar station with the most accurate data. Set up a new replication rule for this new S3 bucket to separate the replication from the other radar stations. Monitor the maximum replication time to the destination. Create an Amazon EventBridge rule to initiate an alert when the time exceeds the desired threshold.
- C. Enable Amazon S3 Transfer Acceleration on the source S3 bucket, and configure the radar station with the most accurate data to use the new endpoint. Monitor the S3 destination bucket's TotalRequestLatency metric. Create an Amazon EventBridge rule to initiate an alert if this status changes.
- D. Create a new S3 replication rule on the source S3 bucket that filters for the keys that use the prefix of the radar station with the most accurate data. Enable S3 Replication Time Control (S3 RTC). Monitor the maximum replication time to the destination. Create an Amazon EventBridge rule to initiate an alert when the time exceeds the desired threshold.

Correct Answer: D*Community vote distribution*

D (100%)

 **devalenzuela86** Highly Voted 1 year, 7 months ago

Selected Answer: D

D for sure
upvoted 8 times

 **vibzr2023** Highly Voted 1 year, 5 months ago

Answer: D
Not C....
Feature | S3 RTC | S3 Transfer Acceleration

Purpose | Faster replication | Faster uploads/downloads
Scope | Replication across buckets | Individual file transfers
Performance | SLA for 15-minute replication | Up to 50-500% speed improvement
Cost | Additional charge | Additional charge
upvoted 5 times

 **career360guru** Most Recent 1 year, 5 months ago

Selected Answer: D
Option D
upvoted 1 times

 **yuliaqwerty** 1 year, 6 months ago

D <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-time-control.html>
upvoted 2 times

 knark446 1 year, 7 months ago

Selected Answer: D

C would also be ok, but its additional overhead of configuring the additional bucket and modifying the sensor to send data to it, so my option is D

upvoted 2 times

Question #353

Topic 1

A company wants to migrate its on-premises data center to the AWS Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers, SAN storage, Java and PHP applications with MySQL, and Oracle databases. There are many dependent services hosted either in the same data center or externally. The technical documentation is incomplete and outdated. A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration.

Which tools or services should the solutions architect use to plan the cloud migration? (Choose three.)

- A. AWS Application Discovery Service
- B. AWS SMS
- C. AWS X-Ray
- D. AWS Cloud Adoption Readiness Tool (CART)
- E. Amazon Inspector
- F. AWS Migration Hub

Correct Answer: ADF

Community vote distribution

ADF (65%)	ACF (15%)	12%	8%
-----------	-----------	-----	----

 **cypkir** Highly Voted 2 years, 1 month ago

Selected Answer: ADF

Answer: ADF

upvoted 9 times

 **aka1177** Most Recent 1 month ago

Selected Answer: ADF

Since AWS X-Ray is more cloud tool and not dedicated for on-prem infrastructure analysis. I will go with ADF. B is outdated service and E is not for on-prem.

upvoted 1 times

 **Chris_W_1234** 1 month, 3 weeks ago

Selected Answer: ACF

CART won't help the architect in any way to determine cost or how the current system is structured, so no D. SMS has been discontinued in 2022, so no B. I read Amazon Inspector doesn't run on-prem, so no E. That leaves A, C, F. X-Ray can be installed on-prem and it helps determining dependencies between services, which is part of what the architect is tasked to do.

upvoted 2 times

 **Chungies** 1 year, 3 months ago

ADF is correct

upvoted 1 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: ADF

Option ADF not B - As of March 31, 2022, Amazon Web Services will discontinue Server Migration Service (Amazon Web Services SMS). Going forward, we recommend Amazon Web Services Application Migration Service (Amazon Web Services MGN)

AWS CART - <https://aws.amazon.com/blogs/publicsector/get-migration-ready-aws-cloud-adoption-readiness-tool/>
upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: ADF

A, D, F

upvoted 2 times

 **vibzr2023** 1 year, 11 months ago

Answer: ADF sure...

B. AWS SMS was discontinued on March 31, 2022. AWS recommends using alternative solutions for server migration, such as: AWS Application Migration Service (AMS), AWS Database Migration Service (DMS), AWS Transfer Family
<https://awscli.amazonaws.com/v2/documentation/api/2.4.19/reference/sms/index.html>

upvoted 3 times

 **JMAN1** 1 year, 11 months ago

Selected Answer: ABF

D. CART is just some of questioner tool to assess and find any gap of people, organization, process between on-premise and AWS Cloud for migration. It is not directly needed or aimed for system.

upvoted 2 times

 **MegalodonBolado** 1 year, 11 months ago

Selected Answer: ACF

A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration.

- A. AWS Application Discovery Service (ok): gathers information about your source servers to support the migration planning.
- B. AWS SMS (?): Isn't it AWS Application Migration Service?
- C. AWS X-Ray (ok): AWS X-Ray provides a complete view of requests as they travel through your application
- D. AWS (CART) (out): Strategic planning tool, focused on Public Sector**
- E. Amazon Inspector (out): Doesn't work on premises
- F. AWS Migration Hub (ok): Migration Hub monitors the status of your migrations in all AWS Regions

ADS helps understand machines, X-ray maps relationships in an undocumented env, and Hub tracks migration data.

upvoted 2 times

 **yuliaqwerty** 2 years ago

Agree ADF

upvoted 2 times

 **andyo** 2 years ago

ADF -- D and not B because one requirement is "estimate the cloud resource costs after the migration"

upvoted 1 times

 **J0n102** 2 years ago

Selected Answer: ABF

I believe the answer is ABF - SMS Server Migration Service seems to be more essential than CART. Servers migrations are mention which SMS is great for. CART should be used before migration when you're just assessing an organization's readiness for cloud adoption

upvoted 1 times

 **GoKhe** 2 years ago

The question is about before migration

upvoted 1 times

 **tfl** 2 years ago

Selected Answer: ADF

ADF for sure

upvoted 2 times

 **shaaam80** 2 years ago

Selected Answer: ADF

ADF correct

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: ABD

ABD for sure

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Yes. ADF is the correct one

upvoted 2 times

Question #354

A solutions architect is reviewing an application's resilience before launch. The application runs on an Amazon EC2 instance that is deployed in a private subnet of a VPC. The EC2 instance is provisioned by an Auto Scaling group that has a minimum capacity of 1 and a maximum capacity of 1. The application stores data on an Amazon RDS for MySQL DB instance. The VPC has subnets configured in three Availability Zones and is configured with a single NAT gateway.

The solutions architect needs to recommend a solution to ensure that the application will operate across multiple Availability Zones.

Which solution will meet this requirement?

- A. Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to a Multi-AZ configuration. Configure the Auto Scaling group to launch the instances across Availability Zones. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.
- B. Replace the NAT gateway with a virtual private gateway. Replace the RDS for MySQL DB instance with an Amazon Aurora MySQL DB cluster. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.
- C. Replace the NAT gateway with a NAT instance. Migrate the RDS for MySQL DB instance to an RDS for PostgreSQL DB instance. Launch a new EC2 instance in the other Availability Zones.
- D. Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to turn on automatic backups and retain the backups for 7 days. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Keep the minimum capacity and the maximum capacity of the Auto Scaling group at 1.

Correct Answer: A

Community vote distribution

A (100%)

 **duriselvan** Highly Voted 1 year, 6 months ago

A ans

Best practices

If your resources span multiple Availability Zones (AZ) , then create one NAT gateway per AZ. This helps to avoid a single point of failure and zone data transfer charges.

Data that's transferred between Amazon EC2 and Elastic Network Interfaces in the same AZ is free. However, data that's transferred to and from Amazon EC2 and Elastic Network Interfaces across multiple AZs in the same AWS Region is charged. The charges depend on the data transfer rates for the Region.

<https://repost.aws/knowledge-center/nat-gateway-vpc-private-subnet>

upvoted 6 times

 **AI8282** Most Recent 5 months, 3 weeks ago

Selected Answer: A

This question made me wonder if I'm doing drugs. A.

upvoted 2 times

 **career360guru** 1 year, 5 months ago

Selected Answer: A

Option A

upvoted 1 times

 **knark446** 1 year, 7 months ago

Selected Answer: A

A.

all the other options make no sense in this scenario

upvoted 3 times

 **shaaam80** 1 year, 7 months ago

Selected Answer: A

A...other answers don't make sense

upvoted 2 times

 **devalenzuela86** 1 year, 7 months ago

Selected Answer: A

A for sure

upvoted 1 times

 **cypkir** 1 year, 7 months ago

Selected Answer: A

Answer: A

upvoted 1 times

Question #355

Topic 1

A company is planning to migrate its on-premises transaction-processing application to AWS. The application runs inside Docker containers that are hosted on VMs in the company's data center. The Docker containers have shared storage where the application records transaction data.

The transactions are time sensitive. The volume of transactions inside the application is unpredictable. The company must implement a low-latency storage solution that will automatically scale throughput to meet increased demand. The company cannot develop the application further and cannot continue to administer the Docker hosting environment.

How should the company migrate the application to AWS to meet these requirements?

- A. Migrate the containers that run the application to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon S3 to store the transaction data that the containers share.
- B. Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic File System (Amazon EFS) file system. Create a Fargate task definition. Add a volume to the task definition to point to the EFS file system.
- C. Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic Block Store (Amazon EBS) volume. Create a Fargate task definition. Attach the EBS volume to each running task.
- D. Launch Amazon EC2 instances. Install Docker on the EC2 instances. Migrate the containers to the EC2 instances. Create an Amazon Elastic File System (Amazon EFS) file system. Add a mount point to the EC2 instances for the EFS file system.

Correct Answer: B

Community vote distribution

B (100%)

 **thotwielder**  1 year, 11 months ago

Selected Answer: B

To mount an Amazon EFS file system on a Fargate task or container, you must first create a task definition. Then, make that task definition available to the containers in your task across all Availability Zones in your AWS Region. Then, your Fargate tasks use Amazon EFS to automatically mount the file system to the tasks that you specify in your task definition.

<https://repost.aws/knowledge-center/ecs-fargate-mount-efs-containers-tasks>

upvoted 6 times

 **kgpoj**  1 year, 4 months ago

Selected Answer: B

I was thinking between B and C.

But according to AWS doc: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/using_data_volumes.html

Amazon EBS volumes provide cost-effective, durable, high-performance block storage for data-intensive containerized workloads.

Amazon EFS volumes support concurrency and are useful for containerized applications that scale horizontally and need storage functionalities like low latency, high throughput, and read-after-write consistency.

So should be B

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

 **yuliaqwerty** 2 years ago

answer B

upvoted 1 times

 **JOn102** 2 years ago

Selected Answer: B

Answer: B Fargate+EFS

upvoted 1 times

 **Russ99** 2 years ago

Selected Answer: B

B is the correct answer for the given scenario

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 3 times

 **cypkir** 2 years, 1 month ago

Selected Answer: B

Answer: B

upvoted 3 times

Question #356

A company is planning to migrate to the AWS Cloud. The company hosts many applications on Windows servers and Linux servers. Some of the servers are physical, and some of the servers are virtual. The company uses several types of databases in its on-premises environment. The company does not have an accurate inventory of its on-premises servers and applications.

The company wants to rightsize its resources during migration. A solutions architect needs to obtain information about the network connections and the application relationships. The solutions architect must assess the company's current environment and develop a migration plan.

Which solution will provide the solutions architect with the required information to develop the migration plan?

- A. Use Migration Evaluator to request an evaluation of the environment from AWS. Use the AWS Application Discovery Service Agentless Collector to import the details into a Migration Evaluator Quick Insights report.
- B. Use AWS Migration Hub and install the AWS Application Discovery Agent on the servers. Deploy the Migration Hub Strategy Recommendations application data collector. Generate a report by using Migration Hub Strategy Recommendations.
- C. Use AWS Migration Hub and run the AWS Application Discovery Service Agentless Collector on the servers. Group the servers and databases by using AWS Application Migration Service. Generate a report by using Migration Hub Strategy Recommendations.
- D. Use the AWS Migration Hub import tool to load the details of the company's on-premises environment. Generate a report by using Migration Hub Strategy Recommendations.

Correct Answer: B

Community vote distribution

B (100%)

 **saggy4** Highly Voted 1 year, 4 months ago

Selected Answer: B

Always remember. If you want to find data for migration that is related to

1. Network, system performance, running process, etc
2. The current on-prem load that you need to find has physical servers in it.

Always use an Application discovery agent.

so A and C are out (since they use agentless discovery which is only used for on-prem VMs)

Between B and D: D is wrong the question itself mentions we are not aware of the current load so import data is not possible.

Correct ans is B

upvoted 11 times

 **ayadmawla** Highly Voted 1 year, 6 months ago

Selected Answer: B

The Discovery Agent captures system configuration, system performance, running processes, and details of the network connections between systems.

The Agentless Collector is only installed as an OVA on the VMware vCenter so it doesn't apply to all servers.

<https://aws.amazon.com/application-discovery/faqs/>

upvoted 5 times

 **thotwielder** Most Recent 1 year, 4 months ago

Why not D?

AWS Migration Hub (Migration Hub) import allows you to import details of your on-premises environment directly into Migration Hub without using the Application Discovery Service Agentless Collector (Agentless Collector) or AWS Application Discovery Agent (Discovery Agent)

<https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-import.html>

upvoted 1 times

 **pangchn** 1 year, 3 months ago

coz the company don't have a detailed list of servers to be imported

upvoted 3 times

 **career360guru** 1 year, 5 months ago

Selected Answer: B

Option B

upvoted 1 times

 **career360guru** 1 year, 5 months ago

Selected Answer: B

Option B

upvoted 1 times

  **J0n102** 1 year, 6 months ago**Selected Answer: B**

Answer: B

upvoted 1 times

  **shaaam80** 1 year, 7 months ago**Selected Answer: B**

Answer B. Application Discovery service agent installed on all servers and VMs to gather information.

upvoted 2 times

  **devalenzuela86** 1 year, 7 months ago**Selected Answer: B**

B for sure

upvoted 3 times

  **cypkir** 1 year, 7 months ago**Selected Answer: B**

Answer: B

upvoted 3 times

Question #357

A financial services company sells its software-as-a-service (SaaS) platform for application compliance to large global banks. The SaaS platform runs on AWS and uses multiple AWS accounts that are managed in an organization in AWS Organizations. The SaaS platform uses many AWS resources globally.

For regulatory compliance, all API calls to AWS resources must be audited, tracked for changes, and stored in a durable and secure data store.

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

- A. Create a new AWS CloudTrail trail. Use an existing Amazon S3 bucket in the organization's management account to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 bucket.
- B. Create a new AWS CloudTrail trail in each member account of the organization. Create new Amazon S3 buckets to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 buckets.
- C. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket with versioning turned on to store the logs. Deploy the trail for all accounts in the organization. Enable MFA delete and encryption on the S3 bucket.
- D. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket to store the logs. Configure Amazon Simple Notification Service (Amazon SNS) to send log-file delivery notifications to an external management system that will track the logs. Enable MFA delete and encryption on the S3 bucket.

Correct Answer: C*Community vote distribution*

C (96%)	4%
---------	----

 **Totoroha** Highly Voted 2 years, 1 month ago

i thinks C is correct answer

upvoted 11 times

 **Dgix** Highly Voted 1 year, 9 months ago

Selected Answer: C

C is correct. Do not get fooled by the phrase "deploy the trail for all accounts" to think that a trail is created in each account – it means that the new organisational-level trail is _configured_ to capture data for all accounts.

upvoted 10 times

 **juanife** 10 months, 2 weeks ago

thanks for that info, someone tends to be misled by those phrases.

upvoted 1 times

 **Curious76** Most Recent 6 months, 1 week ago

Selected Answer: C

S3 with Versioning:

Ensures that logs cannot be overwritten or lost — important for compliance and auditing.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option C: Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket with versioning turned on to store the logs. Deploy the trail for all accounts in the organization. Enable MFA delete and encryption on the S3 bucket. The management account can act as a central hub for logging and auditing.

Using an existing S3 bucket in the management account reduces operational overhead compared to creating multiple buckets across different accounts.

Versioning turned on ensures that old log versions are not automatically deleted, providing an additional layer of compliance.

upvoted 1 times

 **Chungies** 1 year, 2 months ago

I will go with D as the correct answer because C has versioning turned on which is not necessary in this case. You can configure a trail to use Amazon SNS topic and be notified when cloud trail publishes new log files to the Amazon S3 bucket.

upvoted 1 times

 **dv1** 1 year ago

Yes, S3 versioning is not necessary for the org trail to function, but it is a good practice to have in case of accidental deletion of events in the bucket. Option D with SNS is irrelevant.

upvoted 1 times

career360guru 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 1 times

MegalodonBolado 1 year, 11 months ago

Selected Answer: C

A: Should always create new bucket for cloudtrail

B: When you create an organization trail, a trail with the name that you give it is created in every AWS account that belongs to your organization.

C: Correct

D: For several reasons, use SNS only to notify admin, not to use email as a external mgmt system

upvoted 3 times

duriselvan 1 year, 12 months ago

D ans :- <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/configure-sns-notifications-for-cloudtrail.html>

upvoted 1 times

J0n102 2 years ago

Selected Answer: C

Answer: C

upvoted 1 times

ProMax 2 years, 1 month ago

Selected Answer: C

C is correct

upvoted 3 times

oomwowww 2 years, 1 month ago

Selected Answer: C

i thinks C is correct answer

upvoted 3 times

devalenzuela86 2 years, 1 month ago

Selected Answer: A

A for sure

upvoted 1 times

devalenzuela86 2 years, 1 month ago

Yes, C is the correct

upvoted 3 times

Question #358

A company is deploying a distributed in-memory database on a fleet of Amazon EC2 instances. The fleet consists of a primary node and eight worker nodes. The primary node is responsible for monitoring cluster health, accepting user requests, distributing user requests to worker nodes, and sending an aggregate response back to a client. Worker nodes communicate with each other to replicate data partitions.

The company requires the lowest possible networking latency to achieve maximum performance.

Which solution will meet these requirements?

- A. Launch memory optimized EC2 instances in a partition placement group.
- B. Launch compute optimized EC2 instances in a partition placement group.
- C. Launch memory optimized EC2 instances in a cluster placement group.
- D. Launch compute optimized EC2 instances in a spread placement group.

Correct Answer: C

Community vote distribution

C (100%)

 **shaaam80** Highly Voted 2 years ago

Selected Answer: C

Answer C. Memory optimized in Cluster placement group for low latency replication between worker nodes.
upvoted 7 times

 **Totoroha** Highly Voted 2 years, 1 month ago

Option C.

upvoted 5 times

 **AzureDP900** Most Recent 1 year, 1 month ago

C is right

Cluster placement groups (CPGs) are designed to place related resources into the same Availability Zone (AZ), which reduces latency and improves network performance. Since this is a distributed in-memory database with multiple nodes that need to communicate quickly, using a CPG for memory-optimized EC2 instances would be an ideal solution.

By launching memory-optimized EC2 instances in a cluster placement group:

You can reduce latency by minimizing network hops between nodes

You can improve communication efficiency between nodes

upvoted 2 times

 **kgp0j** 1 year, 4 months ago

Selected Answer: C

God I wish all SCP questions are like this.

Easy to read.

Easy to answer.

Easy to move on to next question without spending extra time to read through all comments, ask google/chatGPT and read AWS doc to make sure the community vote is correct

upvoted 3 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 1 times

 **Russ99** 2 years ago

Selected Answer: C

C is the correct answer for sure

upvoted 1 times

 **JOn102** 2 years ago

Selected Answer: C

Answer: C, I guess memory optimized is the obvious way to go and

Cluster placement group provides the lowest possible networking latency

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: C

C is ok

upvoted 3 times

Question #359

A company maintains information on premises in approximately 1 million.csv files that are hosted on a VM. The data initially is 10 TB in size and grows at a rate of 1 TB each week. The company needs to automate backups of the data to the AWS Cloud.

Backups of the data must occur daily. The company needs a solution that applies custom filters to back up only a subset of the data that is located in designated source directories. The company has set up an AWS Direct Connect connection.

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

- A. Use the Amazon S3 CopyObject API operation with multipart upload to copy the existing data to Amazon S3. Use the CopyObject API operation to replicate new data to Amazon S3 daily.
- B. Create a backup plan in AWS Backup to back up the data to Amazon S3. Schedule the backup plan to run daily.
- C. Install the AWS DataSync agent as a VM that runs on the on-premises hypervisor. Configure a DataSync task to replicate the data to Amazon S3 daily.
- D. Use an AWS Snowball Edge device for the initial backup. Use AWS DataSync for incremental backups to Amazon S3 daily.

Correct Answer: C

Community vote distribution

C (83%)	B (17%)
---------	---------

 **VasDev** Highly Voted 2 years, 1 month ago

Selected Answer: C

Because of: The company needs a solution that applies custom filters to back up only a subset of the data that is located in designated source directories.

upvoted 14 times

 **PAUGURU** 2 years ago

The only problem with C is that a data sync is not a backup. If you delete a file, the sync will delete the file on AWS, but with backups you can restore it from yesterday's backup. So I think it's B.

upvoted 2 times

 **vibzr2023** 1 year, 11 months ago

I agree AWS DataSync is not a dedicated backup solution but it can be used for data replication that serves as a backup, it's essential to understand its limitations and distinctions compared to a comprehensive backup service:
When to Use DataSync for Backup-Like Purposes:

Initial Data Transfer: It's efficient for bulk migration of large datasets to AWS storage services.

Incremental Updates: It excels at replicating ongoing changes to keep a copy of data in AWS, serving as a near-real-time backup.

Cost-Effective Replication: It's often more cost-effective than traditional backup tools for ongoing data replication, especially for large datasets.

upvoted 2 times

 **ayadmawla** Highly Voted 2 years ago

Selected Answer: C

For me there are two cues:

- 1- "custom filters" which are available in Datasync
- 2- AWS Backup does not back up to S3, rather to a Storage Vault.

upvoted 6 times

 **eesa** Most Recent 9 months, 1 week ago

Selected Answer: C

Automatización: DataSync permite programar tareas periódicas, como respaldos diarios.

Filtros personalizados: Puedes configurar filtros para incluir solo ciertos archivos o directorios específicos.

Compatibilidad: DataSync está diseñado para grandes cantidades de archivos (como 1 millón de archivos .csv).

Rendimiento: Se integra con Direct Connect, aprovechando la conexión de alta capacidad.

Bajo overhead operativo: Solo debes instalar un agente una vez y definir tareas desde la consola de AWS. Es administrado completamente por AWS.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option C is a good choice for this scenario.

Using AWS DataSync to replicate the data to Amazon S3 daily (Option C) meets all the requirements:

It provides an automated solution for backing up data to the cloud.

It allows you to apply custom filters to back up only a subset of the data located in designated source directories.

Since DataSync is designed for scalable and efficient data transfer, it should provide better performance for large datasets.

Here are some benefits of using AWS DataSync:

Easy setup and configuration

Automatic replication to Amazon S3

Scalable and efficient data transfer

Supports custom filters for selective data backup

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: C

Option C: How To

<https://docs.aws.amazon.com/datasync/latest/userguide/create-s3-location.html>

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C - Due to filtering requirement.

upvoted 2 times

 **vibzr2023** 1 year, 11 months ago

Answer: C

Option B: AWS Backup offers centralized backup management, but it might not support custom filtering for specific files or directories as granularly as DataSync.

upvoted 1 times

 **yuliaqwert** 2 years ago

B AWS Backup can do backup from on-premise (<https://aws.amazon.com/backup/faqs/> Can I use AWS Backup to back up on-premises data?)

upvoted 1 times

 **motica0418** 2 years ago

based on the FQA, AWS Backup can only back up on-premises "Storage Gateway" volumes and "VMware virtual machines".

upvoted 1 times

 **awsamar** 2 years ago

Selected Answer: B

B correct. Because Datasync is not for backup

upvoted 3 times

 **Russs99** 2 years ago

Selected Answer: C

as to option B, AWS Backup doesn't natively support direct backups of on-premises data into Amazon S3.

upvoted 2 times

 **J0n102** 2 years ago

Selected Answer: C

Answer: C

upvoted 2 times

 **shaaam80** 2 years ago

Selected Answer: C

Answer C - with Datasync custom filters can be created to select what data needs to be backed up / replicated.

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 3 times

 **igor12ghsj577** 1 year, 11 months ago

For sure you ate wrong.

upvoted 4 times

Question #360

Topic 1

A financial services company has an asset management product that thousands of customers use around the world. The customers provide feedback about the product through surveys. The company is building a new analytical solution that runs on Amazon EMR to analyze the data from these surveys. The following user personas need to access the analytical solution to perform different actions:

- Administrator: Provisions the EMR cluster for the analytics team based on the team's requirements
- Data engineer: Runs ETL scripts to process, transform, and enrich the datasets
- Data analyst: Runs SQL and Hive queries on the data

A solutions architect must ensure that all the user personas have least privilege access to only the resources that they need. The user personas must be able to launch only applications that are approved and authorized. The solution also must ensure tagging for all resources that the user personas create.

Which solution will meet these requirements?

- Create IAM roles for each user persona. Attach identity-based policies to define which actions the user who assumes the role can perform. Create an AWS Config rule to check for noncompliant resources. Configure the rule to notify the administrator to remediate the noncompliant resources.
- Setup Kerberos-based authentication for EMR clusters upon launch. Specify a Kerberos security configuration along with cluster-specific Kerberos options.
- Use AWS Service Catalog to control the Amazon EMR versions available for deployment, the cluster configuration, and the permissions for each user persona.
- Launch the EMR cluster by using AWS CloudFormation. Attach resource-based policies to the EMR cluster during cluster creation. Create an AWS Config rule to check for noncompliant clusters and noncompliant Amazon S3 buckets. Configure the rule to notify the administrator to remediate the noncompliant resources.

Correct Answer: C

Community vote distribution

C (84%)	A (16%)
---------	---------

 **career360guru** Highly Voted 1 year, 11 months ago

Selected Answer: C

Option C. Option A does not provide control over deployment of resources and configurations.
upvoted 5 times

 **eesa** Most Recent 9 months, 1 week ago

Selected Answer: C

AWS Service Catalog permite definir plantillas preaprobadas para lanzar EMR clusters con configuraciones controladas (versiones, aplicaciones, seguridad).

Se pueden definir permisos por rol (por persona o grupo de IAM) para controlar qué acciones puede realizar cada usuario.

Se pueden forzar políticas de etiquetado obligatorio mediante plantillas y restricciones de uso.

Garantiza el principio de menor privilegio, ya que los usuarios no tienen acceso completo a EMR sino sólo a lo autorizado por Service Catalog.

Ideal para ambientes empresariales donde se necesita control centralizado, gobernanza y cumplimiento
upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Using AWS Service Catalog (Option C) to control the Amazon EMR versions available for deployment, the cluster configuration, and the permissions for each user persona meets all the requirements:

It provides a centralized management interface for IT services

It allows you to define and enforce policies for resource provisioning and access control

It enables you to manage multiple instances of an application (in this case, EMR clusters) from a single console

upvoted 1 times

✉ **AloraCloud** 1 year, 2 months ago

Why not Option A is because it involves creating IAM roles and attaching identity-based policies, which is solid. But it relies on AWS Config rules to ensure compliance, which adds an extra layer of management and potential lag in remediation.

AWS Service Catalog, on the other hand, simplifies control over EMR versions, configurations, and permissions, and it also enforces resource tagging directly during deployment, making it more efficient and streamlined for managing access and compliance.

upvoted 1 times

✉ **gfhbox0083** 1 year, 5 months ago

Selected Answer: C

C, for sure.

AWS Service Catalog ensures that all resources created are compliant with the organization's policies, including mandatory tagging.

upvoted 1 times

✉ **JMAN1** 1 year, 11 months ago

Selected Answer: C

C because tagging ensured by Service Catalogue.

upvoted 3 times

✉ **vibzr2023** 1 year, 11 months ago

Selected Answer: C

Option A: While IAM roles and identity-based policies offer user-level control, they lack the functionality for managing EMR deployment options and configurations centrally.

upvoted 1 times

✉ **awsamar** 2 years ago

Selected Answer: C

keyword here are: "...only applications that are approved and authorized..."

Only C provides this

upvoted 4 times

✉ **ayadmawla** 2 years ago

Selected Answer: A

A - IAM Roles define actions Service Catalog is about resources (EMR)

upvoted 4 times

✉ **ayadmawla** 2 years ago

it seems that I was wrong and C is the approach as per: <https://aws.amazon.com/blogs/big-data/build-a-self-service-environment-for-each-line-of-business-using-amazon-emr-and-aws-service-catalog/>

upvoted 5 times

✉ **shaaam80** 2 years ago

Please vote your answers rather than just commenting. It skews the vote % for someone who doesn't read all the comments.

upvoted 1 times

✉ **dutchy1988** 2 years ago

It seems that AWS is upselling AWS Service Catalog here with this question. Some key parts in this question:

1. Least privilege access
2. launch only approved and authorized applications
3. ensure tagging.

upvoted 2 times

✉ **dutchy1988** 2 years ago

due to point 3, all options with AWS config rule are out since it only measures if you are compliant, so that means tagging is not ensured upfront. A and D are out!

B doesn't fulfill the requirement for tagging and even more, is kerberos really helpful here?

upvoted 2 times

✉ **dutchy1988** 2 years ago

Leaves only C,

quote from <https://aws.amazon.com/servicecatalog/>

Create, organize, and govern a curated catalog of AWS resources that can be shared at the permissions level so you can quickly provision approved cloud resources without needing direct access to the underlying AWS services. -> meets only allowed and authorized application launch.

AutoTag fulfills the requirement to tag resources with creator -> aws:servicecatalog:provisioningPrincipalArn - The ARN of the provisioning principal (user) who created the provisioned product.

this can only be AWS Server Catalog.

and please stop seeding GPT answers! do your own research.

upvoted 4 times

✉ **PouyaK** 2 years ago

Answer A -

The answers from Chat GPT are inaccurate and untrustable.

upvoted 3 times

 **shaam80** 2 years ago

Selected Answer: C

From GPT: AWS Service Catalog allows you to control and manage access to resources by defining portfolios and products with specific permissions. Allows you to create portfolios with approved and authorized applications, ensuring that only the specified applications are launched. AWS Service Catalog can enforce tagging on provisioned resources, ensuring that all resources created by the user personas are appropriately tagged.

upvoted 3 times

 **heatblur** 2 years, 1 month ago

Selected Answer: C

C is correct: AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. This is ideal for controlling which Amazon EMR versions and cluster configurations are available to users. Specific cluster configurations and permissions can be set for each user persona, ensuring they have only the access they need. This meets the least privilege principle. The Service Catalog can be configured to allow users to launch only certain applications, ensuring adherence to company policies on approved and authorized software. It also supports resource tagging.

upvoted 3 times

 **devalenzuela86** 2 years, 1 month ago

A is correct

Aws:

To ensure that all user personas have least privilege access to only the resources they need, can launch only approved and authorized applications, and ensure tagging for all resources that the user personas create, a solutions architect can consider the following steps:

1. IAM roles for each user persona. Attach identity-based policies to define which actions the user who assumes the role can perform.
- 2.Create an AWS Config rule to check for noncompliant resources. Configure the rule to notify the administrator to remediate the noncompliant resources.

upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: C

Answer: C

upvoted 1 times

Question #361

A software as a service (SaaS) company uses AWS to host a service that is powered by AWS PrivateLink. The service consists of proprietary software that runs on three Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in private subnets in multiple Availability Zones in the eu-west-2 Region. All the company's customers are in eu-west-2.

However, the company now acquires a new customer in the us-east-1 Region. The company creates a new VPC and new subnets in us-east-1. The company establishes inter-Region VPC peering between the VPCs in the two Regions.

The company wants to give the new customer access to the SaaS service, but the company does not want to immediately deploy new EC2 resources in us-east-1.

Which solution will meet these requirements?

- A. Configure a PrivateLink endpoint service in us-east-1 to use the existing NLB that is in eu-west-2. Grant specific AWS accounts access to connect to the SaaS service.
- B. Create an NLB in us-east-1. Create an IP target group that uses the IP addresses of the company's instances in eu-west-2 that host the SaaS service. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.
- C. Create an Application Load Balancer (ALB) in front of the EC2 instances in eu-west-2. Create an NLB in us-east-1. Associate the NLB that is in us-east-1 with an ALB target group that uses the ALB that is in eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.
- D. Use AWS Resource Access Manager (AWS RAM) to share the EC2 instances that are in eu-west-2. In us-east-1, create an NLB and an instance target group that includes the shared EC2 instances from eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

Correct Answer: A

Community vote distribution

A (54%)

B (46%)

 **devalenzuela86** Highly Voted 2 years, 1 month ago

Selected Answer: A

A

Explanation:

- * Configuring a PrivateLink endpoint service in us-east-1 to use the existing NLB that is in eu-west-2 will allow the new customer to access the SaaS service without deploying new EC2 resources in us-east-1.
 - * Granting specific AWS accounts access to connect to the SaaS service will ensure that only authorized users can access the service.
- upvoted 18 times

 **abhitricanada** 1 year, 11 months ago

Answer is A because ... VPC peering between the VPCs in the two Regions already done & company does not want to immediately deploy new EC2 resources in us-east-1, later on company will change the architecture

upvoted 2 times

 **Pilot** 2 years ago

Network Load Balancers now support connections from clients to IP-based targets in peered VPCs across different AWS Regions. Previously, access to Network Load Balancers from an inter-region peered VPC was not possible. With this launch, you can now have clients access Network Load Balancers over an inter-region peered VPC. Network Load Balancers can also load balance to IP-based targets that are deployed in an inter-region peered VPC. This support on Network Load Balancers is available in all AWS Regions.

<https://aws.amazon.com/about-aws/whats-new/2018/10/network-load-balancer-now-supports-inter-region-vpc-peering/>

NLB support client from different region, I think A is correct.

upvoted 5 times

 **heatblur** Highly Voted 2 years ago

Selected Answer: B

The best option among these is B. While it introduces some complexity, it's the most viable solution that aligns with AWS capabilities and the company's requirements. Creating an NLB in us-east-1 and targeting the IP addresses of the existing instances in eu-west-2 is a feasible approach. This setup allows the company to use their existing infrastructure in eu-west-2 while providing access to the customer in us-east-1 through the PrivateLink endpoint service in us-east-1. This avoids the immediate need to deploy new EC2 resources in the us-east-1 region.

It can't be A because AWS PrivateLink endpoint services cannot span regions. They are region-specific, so an endpoint service in us-east-1 cannot directly use an NLB located in eu-west-2.

upvoted 17 times

 **ayadmawla** 2 years ago

But the company has establishing Inter-Region VPC Peering so the endpoint would work

upvoted 2 times

 **SKS** 1 year, 8 months ago

Wrong on part where private link support for inter region vpc peering .

<https://aws.amazon.com/about-aws/whats-new/2018/10/aws-privatelink-now-supports-access-over-inter-region-vpc-peering/>

upvoted 4 times

 **pk0619** 1 year ago

This is saying you can access privatelink in us-east-1 from ec2 instance in eu-west-1. It does not say that you can create a privatelink in us-east-1 for a resource like NLB in eu-west-1.

upvoted 1 times

 **liquen14** 1 year, 9 months ago

I was unable to find documentation saying that an AWS PrivateLink endpoint requires the NLB to be in the same region but if you go to the console for instance here:

<https://eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateVpcEndpointServiceConfiguration>:

try to create an endpoint service and you don't have a NLB there the console explicitly states:

"No Network Load Balancers or Gateway Load Balancers available in this Region." so for me A is invalid

upvoted 4 times

 **aka1177** Most Recent 1 month ago

Selected Answer: B

Be careful answer is B !!

PrivateLink is used only within a single region or between VPCs in the same region !!!

upvoted 1 times

 **D_dee** 2 months, 2 weeks ago

Selected Answer: B

A is incorrect bcos An AWS PrivateLink endpoint service must use an NLB in the same Region. You cannot associate an endpoint service in us-east-1 with an NLB in eu-west-2

upvoted 1 times

 **Blair77** 2 months, 3 weeks ago

Selected Answer: B

B ! Why not A? You cannot configure a PrivateLink endpoint service in one region (us-east-1) to directly use a load balancer in another region (eu-west-2). An endpoint service must be in the same region as its associated NLB.

upvoted 1 times

 **fa6d93f** 3 months, 1 week ago

Selected Answer: B

AWS PrivateLink does not support cross-Region endpoint services directly, so customers in us-east-1 cannot connect to a PrivateLink endpoint service running in eu-west-2 without a localized endpoint/NLB in their Region.

Option B leverages inter-Region VPC peering to create an NLB in us-east-1; this NLB can forward traffic to the EC2 instances in eu-west-2 by using an IP target group with their private IPs.

This setup does not require any new EC2 instances in us-east-1, satisfying the company's requirement to avoid immediate new deployments in that Region.

upvoted 3 times

 **ce0b8b3** 4 months, 1 week ago

Selected Answer: B

A - Not possible. An endpoint service is regional and can only point to an NLB in the same region. You cannot directly associate a PrivateLink service in us-east-1 with an NLB in eu-west-2.

upvoted 2 times

 **AI8282** 5 months, 2 weeks ago

Selected Answer: A

As of Dec 2024 A is right:

"With the launch of native cross-region connectivity for AWS PrivateLink, you can now share and access VPC endpoint services across different Regions."

It's less complex and fully supported.

<https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-cross-region-connectivity-for-aws-privatelink/#:~:text=Overview,a%20variety%20of%20use%2Dcases>

upvoted 2 times

 **strike3test** 5 months, 3 weeks ago

Selected Answer: A

"Configure a PrivateLink endpoint service in us-east-1 to use the existing NLB in eu-west-2" — This matches the cross-region PrivateLink model, where the endpoint service is hosted in eu-west-2 but accessible from us-east-1 via PrivateLink endpoints. The service provider grants access to specific AWS accounts. This is exactly the new cross-region PrivateLink feature.

upvoted 2 times

 **dfd5668** 6 months, 2 weeks ago

Selected Answer: A

Now A is the answer

upvoted 2 times

 **kyo** 10 months, 2 weeks ago

Selected Answer: B

This question was written before AWS PrivateLink supported cross-region connectivity. At that time, the only way to give a customer in us-east-1 access to a service in eu-west-2 without deploying resources in us-east-1 was the complex workaround described in Option B. This involved creating an NLB in us-east-1 and using an IP target group pointing back to the instances in eu-west-2. It was a complicated solution, but it was the only way to achieve the desired outcome given the limitations at the time. Therefore, B was the correct answer for the question as it was originally written.

But now the answer has changed to A.

upvoted 5 times

 **Spike2020** 1 year ago

Selected Answer: B

As of November 2024, AWS PrivateLink supports native cross-region connectivity. However, since this exam question appears to be set before this feature was available, we need to consider the solution using the previous architecture patterns.

Option A: Not viable because PrivateLink endpoint services must be in the same region as the NLB

upvoted 3 times

 **TomTom** 1 year ago

Selected Answer: A

Answer A is correct (now) Recently AWS announce, Now PrivateLink endpoint supports native cross-region connectivity.

<https://aws.amazon.com/about-aws/whats-new/2024/11/aws-privatelink-across-region-connectivity/>

upvoted 2 times

 **altonh** 10 months, 2 weeks ago

A is still incorrect. Note that A requires creating an ENDPOINT SERVICE in us-east-1 that points to an NLB in us-west-2. This is not possible. What you can do is create an endpoint service in us-west-2 that points to the NLB in us-west-2 and then make the endpoint service cross-region. Then, in us-east-1, you can create an ENDPOINT that points to the ENDPOINT SERVICE in us-east-1.

upvoted 1 times

 **alexbraila** 1 year ago

The article refers to Interface VPC endpoints connectivity to VPC endpoint services, but this is not the use case here. The comment of liquen14 is still valid, I tested today 3rd of Dec 2024. When creating an endpoint service, you can only select load balancers in the same region. Hence for the current use case we must create an NLB in us-east-1, which will be able to connect to the EC2 instances over the peered VPC due to the link in Pilot's comment (however, his comment is not right, A does not work):

<https://aws.amazon.com/about-aws/whats-new/2018/10/network-load-balancer-now-supports-inter-region-vpc-peering/>

upvoted 1 times

 **alexbraila** 1 year ago

Bottom line, A does not work, B does

upvoted 1 times

 **youonebe** 1 year, 1 month ago

Selected Answer: B

Creating an NLB in us-east-1 with IP target group pointing to the existing eu-west-2 instances is the most efficient solution because: IP target groups can route traffic across VPC peering connections

This configuration allows the use of existing EC2 instances while providing local access in us-east-1

PrivateLink endpoint service can be configured with the new NLB to provide secure access

upvoted 2 times

 **0b43291** 1 year, 1 month ago

Selected Answer: B

The correct solution is Option B: Create an NLB in us-east-1. Create an IP target group that uses the IP addresses of the company's instances in eu-west-2 that host the SaaS service. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

Option A is not possible because PrivateLink endpoint services cannot span across AWS Regions. The existing NLB in eu-west-2 cannot be directly used for a PrivateLink endpoint service in us-east-1.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

correct answer : A

Using an existing NLB in eu-west-2 as the basis for a PrivateLink endpoint service in us-east-1 allows the company to quickly provide access to its SaaS service without having to create new EC2 resources or configure complex networking setups.

upvoted 1 times

 **Woody1848** 1 year, 2 months ago

Selected Answer: A

"An interface endpoint is essentially a service-level ENI. The service is attached straight to the VPC subnet through the ENI. This allows us to assign a private IP address from the subnet pool directly to the service." (AWS Certified Advanced Networking - Specialty Exam Guide pg. 36)

There is no need to create EC2 resources in us-east-1 when creating a PrivateLink endpoint.

upvoted 2 times

Question #362

A company needs to monitor a growing number of Amazon S3 buckets across two AWS Regions. The company also needs to track the percentage of objects that are encrypted in Amazon S3. The company needs a dashboard to display this information for internal compliance teams.

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

- A. Create a new 3 Storage Lens dashboard in each Region to track bucket and encryption metrics. Aggregate data from both Region dashboards into a single dashboard in Amazon QuickSight for the compliance teams.
- B. Deploy an AWS Lambda function in each Region to list the number of buckets and the encryption status of objects. Store this data in Amazon S3. Use Amazon Athena queries to display the data on a custom dashboard in Amazon QuickSight for the compliance teams.
- C. Use the S3 Storage Lens default dashboard to track bucket and encryption metrics. Give the compliance teams access to the dashboard directly in the S3 console.
- D. Create an Amazon EventBridge rule to detect AWS CloudTrail events for S3 object creation. Configure the rule to invoke an AWS Lambda function to record encryption metrics in Amazon DynamoDB. Use Amazon QuickSight to display the metrics in a dashboard for the compliance teams.

Correct Answer: C*Community vote distribution*

C (71%)	A (23%)	6%
---------	---------	----

 **cypkir** Highly Voted 2 years, 1 month ago

Selected Answer: C

Answer: C

upvoted 10 times

 **OtisB** Most Recent 1 month ago

Selected Answer: A

Organization-level dashboards can be scoped only to a single AWS Region

https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens_basics_metrics_recommendations.html
upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 4 months ago

Selected Answer: C

S3 Storage Lens already provides built-in metrics for bucket and encryption status in a default dashboard. You don't need to build or maintain any extra Lambda, Athena, or QuickSight pipelines. Just give the compliance team access to the console dashboard → least operational overhead

upvoted 1 times

 **4845c28** 4 months, 1 week ago

Selected Answer: A

Default storage lens dashboard is scoped to one account and this cannot be changed
https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens_editing.html

And organization wide dashboards can only be scope to regional scope

https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens_basics_metrics_recommendations.html
upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

C is right

This solution requires the least operational overhead because it leverages the existing S3 Storage Lens feature, which provides a pre-built dashboard for monitoring bucket and encryption metrics.

The compliance teams can access this dashboard directly in the S3 console without requiring additional setup or configuration.

This solution also eliminates the need to set up and manage multiple AWS resources (e.g., Lambda functions, Athena queries) or aggregate data from separate dashboards.

upvoted 1 times

 **trungtd** 1 year, 7 months ago

Selected Answer: A

This use-case is really too rare to learn about on your own
upvoted 3 times

✉️ **TonytheTiger** 1 year, 9 months ago

Selected Answer: C

Option C: Not A because the requirement is asking for "Least Operation Overhead" w/ S3 Storage Lens has a default dashboard. If you include QuicSight you are adding additional operational overhead, now you have to build your dashboard.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens_basics_metrics_recommendations.html#storage_lens_basics_default_dashboard

upvoted 4 times

✉️ **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 1 times

✉️ **vibzr2023** 1 year, 11 months ago

Answer: C

Storage Lens is a built-in S3 feature that automatically collects and aggregates storage metrics, eliminating the need for custom development or infrastructure management.

Option A: While Storage Lens supports multiple dashboards, creating and aggregating regional dashboards in QuickSight adds complexity and maintenance overhead.

Option B: Involves custom Lambda development, data storage in S3, Athena queries, and QuickSight integration, increasing operational complexity and costs.

Option D: Requires EventBridge rule configuration, Lambda function development, DynamoDB table management, and QuickSight integration, adding significant overhead.

upvoted 2 times

✉️ **GoKhe** 2 years ago

C

I was leaning towards A but it says in each region so that is wrong since Storage Lens gives you a view of all the regions. Someone has chosen B which is wrong b/c it has operational overhead.

upvoted 4 times

✉️ **GaryQian** 2 years ago

Selected Answer: C

I doubt B as the question is asking for LEAST operational choice instead of Best choice. The lambda function needs developer to write code.

upvoted 1 times

✉️ **shaaam80** 2 years ago

Selected Answer: C

Answer C.

Storage Lens metrics include % of encrypted objects

upvoted 1 times

✉️ **J0n102** 2 years ago

Selected Answer: C

Answer: C, S3 Storage Lens default=free metrics which offers encryption tracking. It's easy to set up and least overhead.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens_metrics_glossary.html

upvoted 3 times

✉️ **heatblur** 2 years ago

Selected Answer: C

C is the best answer -- it's the most straightforward and involves the least operational overhead. It directly addresses the need to monitor S3 buckets and track encryption status without the need for additional setup or custom integrations. While it may not offer the same level of customization as some of the other options, it should suffice for most internal compliance requirements and is the most efficient choice in terms of minimizing operational complexity.

upvoted 1 times

✉️ **pic1** 2 years ago

Selected Answer: A

Given the scenario specifics, it's the only option that answers the need to aggregate data from two regions in a dashboard for compliance teams.

upvoted 1 times

✉️ **pic1** 2 years ago

On second thought, I'm switching to option B. It appears to be the lightest between the candidates.

upvoted 1 times

✉️ **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B is ok.

To monitor a growing number of Amazon S3 buckets across two AWS Regions and track the percentage of objects that are encrypted in Amazon S3 with the least operational overhead, a solutions architect can consider the following steps:

Deploy an AWS Lambda function in each Region to list the number of buckets and the encryption status of objects. Store this data in

Amazon S3.

Use Amazon Athena queries to display the data on a custom dashboard in Amazon QuickSight for the compliance teams
upvoted 2 times

Question #363

Topic 1

A company's CISO has asked a solutions architect to re-engineer the company's current CI/CD practices to make sure patch deployments to its application can happen as quickly as possible with minimal downtime if vulnerabilities are discovered. The company must also be able to quickly roll back a change in case of errors.

The web application is deployed in a fleet of Amazon EC2 instances behind an Application Load Balancer. The company is currently using GitHub to host the application source code, and has configured an AWS CodeBuild project to build the application. The company also intends to use AWS CodePipeline to trigger builds from GitHub commits using the existing CodeBuild project.

What CI/CD configuration meets all of the requirements?

- A. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for in-place deployment. Monitor the newly deployed code, and, if there are any issues, push another code update
- B. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue/green deployments. Monitor the newly deployed code, and, if there are any issues, trigger a manual rollback using CodeDeploy.
- C. Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks. Monitor the newly deployed code, and, if there are any issues, push another code update.
- D. Configure the CodePipeline with a deploy stage using AWS OpsWorks and in-place deployments. Monitor the newly deployed code, and, if there are any issues, push another code update.

Correct Answer: B

Community vote distribution

B (100%)

 **heatblur** Highly Voted 2 years ago

Selected Answer: B

B is the best choice. Using a B/G approach aligns with the requirements for quick patch deployments and minimal downtime. In the event of an issue, the company can quickly revert to the previous version, meeting the need for a fast rollback process. This method offers a balance of speed, reliability, and safety for critical updates.

upvoted 8 times

 **AzureDP900** Most Recent 1 year, 1 month ago

B is right

Blue/green deployments allow for multiple instances of the application to be deployed simultaneously, one in production and one in a standby state (the "blue" instance). This approach provides several benefits, including:

Minimal downtime: If an issue arises with the production instance, users can quickly switch to the standby instance without disrupting the application.

Easy rollbacks: If issues cannot be resolved, blue/green deployments allow for a quick rollback to the previous version of the application.

upvoted 1 times

 **Daniel76** 1 year, 4 months ago

Manual code rollback in CodeDeploy:

<https://docs.aws.amazon.com/codedeploy/latest/userguide/deployments-rollback-and-redeploy.html#:~:text=a%20deployment%20group.-,Manual%20rollbacks,gotten%20into%20an%20unknown%20state.>

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

 **GaryQian** 2 years ago

Selected Answer: B

AWS like green/blue deployment for new code & roll back scenario

upvoted 2 times

 **JOn102** 2 years ago

Selected Answer: B

Answer: B

upvoted 1 times

 PouyaK 2 years ago

Answer B

upvoted 2 times

 shaaam80 2 years ago

Selected Answer: B

Answer B

upvoted 2 times

 devalenzuela86 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 3 times

 cypkir 2 years, 1 month ago

Selected Answer: B

Answer: B

upvoted 2 times

Question #364

Topic 1

A company is managing many AWS accounts by using an organization in AWS Organizations. Different business units in the company run applications on Amazon EC2 instances. All the EC2 instances must have a BusinessUnit tag so that the company can track the cost for each business unit.

A recent audit revealed that some instances were missing this tag. The company manually added the missing tag to the instances.

What should a solutions architect do to enforce the tagging requirement in the future?

A. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned off. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the root of the organization.

B. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned on. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the organization's management account.

C. Create an SCP and attach the SCP to the root of the organization. Include the following statement in the SCP:

```
{
  "Sid": "DenyEC2Creation",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/BusinessUnit": "true"
    }
  }
}
```

D. Create an SCP and attach the SCP to the organization's management account. Include the following statement in the SCP:

```
{
  "Sid": "DenyEC2Creation",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/BusinessUnit": "false"
    }
  }
}
```

Correct Answer: C

Community vote distribution

C (75%)

B (19%)

6%

 **ayadmaWla** Highly Voted  2 years ago

Selected Answer: C

Answer is C. To those that are getting confused between a Management Account vs Root of the Organisation here is my two pennies:

Management Account is where you create accounts, management payments, create organisation, etc.

Root of Organisation is where you apply the policies

See: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html

upvoted 15 times

 **marszalekm** 1 year, 10 months ago

You apply SCP in root account and tag policy in management account, but I think crucial issue here is to "enforce the tagging requirement in the future", only SCP can do that.

<https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>
"SCPs can be used along-side tag policies to ensure that the tags are applied at the resource creation time and remain attached to the

resource."

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html

"When you sign in to the organization's management account, you use Organizations to enable the tag policies feature. [...] in the organization's management account. Then you can create tag policies and attach them to the organization entities to put those tagging rules in effect. "

upvoted 3 times

✉ **MegalodonBolado** Highly Voted 1 year, 11 months ago

Selected Answer: C

From repost:

* Use tag policies to prevent tagging on existing resources

* Use SCPs to prevent tagging for creating new resources

<https://repost.aws/knowledge-center/organizations-scp-tag-policies>

What should a solutions architect do to enforce the tagging requirement in the future?

You can use SCPs to prevent the creation of new AWS resources that aren't tagged for your Organization's tagging restriction guidelines. To make sure that the AWS resources are created only if a certain tag is present, use the example SCP policy to require a tag on specified created resources:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html#example-require-tag-on-create

upvoted 7 times

✉ **MegalodonBolado** 1 year, 11 months ago

Looks like I can't post json code here, so follow the last link to find the policy

upvoted 1 times

✉ **AI8282** Most Recent 5 months, 3 weeks ago

Selected Answer: C

C. D has a typo (e2:RunInstances rather than ec2 which wont work) and the null condition is true where it needs to be false.

upvoted 1 times

✉ **AzureDP900** 1 year, 1 month ago

C is correct

upvoted 1 times

✉ **053081f** 1 year, 5 months ago

Selected Answer: C

Option A and B is incorrect:

Tag policies with capitalization control provide the following regulation:

For example, if the "BusinessUnit" tag requires case sensitivity, creating resources with tags like "BusineSSUnit" or "businessunit" will fail, while creating resources with the "Business" tag will be allowed.

Case sensitivity enforces rules within the same string, but does not fulfill the requirements of this question.

upvoted 1 times

✉ **053081f** 1 year, 5 months ago

Selected Answer: A

Correct answer is A, rather than B.

C: While this SCP would prevent instances from being created without the tag, it's a more restrictive approach than using tag policies. SCPs are better suited for broad permission management rather than enforcing tagging.

upvoted 1 times

✉ **red_panda** 1 year, 7 months ago

Selected Answer: C

For me it's C.

Here we have to note that when the AWS Organization Units are mentioned, for the most we need to use SCP or RAM at the exams. Just little tips.

A part of this, C seems most correct answer in my point of view :)

upvoted 2 times

✉ **tushar321** 1 year, 8 months ago

C. "true": This means that the condition will evaluate to true (and thus the policy statement will be in effect) if the Project tag is not present in the request.

condition states that the policy statement is in effect when the Project tag is not included in the request. If the Project tag is present, the condition will evaluate to false

upvoted 2 times

✉ **VerRi** 1 year, 9 months ago

Selected Answer: C

Tag policies take control of auto-tagging but do not "enforce" the tagging requirement.

upvoted 1 times

✉ **TonytheTiger** 1 year, 9 months ago

Selected Answer: C

Option C - SCP for tagging resources

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html#example-require-tag-on-create

upvoted 1 times

 **pangchn** 1 year, 9 months ago

Selected Answer: C

C

Did a recent project which is similar to this question.

B D out since they apply to management account which is wrong.

For C, SCP will deny the resource creation, if it is missing the tag

For A, tagging policy will deny tag creation if the tag key is not matching the name

For this question asked, it is C

If question is asking that resource must be have tag key ABC=***, and can't not have tag key CBA=*** then A would be the answer.

For a real world restriction, you may have both A and C setup

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 1 times

 **Laercio96** 1 year, 11 months ago

Selected Answer: C

After you create a tagging policy, you can put your tagging rules into effect. To do this, attach the policy to the organization root, organizational units (OUs), AWS Accounts within the organization, or a combination of organization entities.

https://docs.aws.amazon.com/pt_br/organizations/latest/userguide/orgs_manage_policies_tag-policies-create.html

Option B asks to attach the management account, but the question informs you that you have several accounts.

That's why I'll go with "C"

upvoted 1 times

 **NOZOMI** 1 year, 12 months ago

The answer is c. Tag policies control the key and value when a tag is applied, but they cannot prevent the application of tags themselves.

upvoted 1 times

 **duriselman** 1 year, 12 months ago

<https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>

upvoted 1 times

 **duriselman** 1 year, 12 months ago

ANs :

<https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>

upvoted 1 times

 **water314** 1 year, 12 months ago

Selected Answer: A

Implement a tag policy that specifically requires the BusinessUnit tag on EC2 instances. This policy can be enforced across the organization, ensuring that all EC2 instances carry the mandatory tag. Compliance with tag key capitalization can be turned off to allow flexibility in how the tag key is formatted. Once the policy is created, it should be attached to the root of the organization, which ensures that it is applied across all accounts within the organization.

upvoted 1 times

Question #365

Topic 1

A company is running a workload that consists of thousands of Amazon EC2 instances. The workload is running in a VPC that contains several public subnets and private subnets. The public subnets have a route for 0.0.0.0/0 to an existing internet gateway. The private subnets have a route for 0.0.0.0/0 to an existing NAT gateway.

A solutions architect needs to migrate the entire fleet of EC2 instances to use IPv6. The EC2 instances that are in private subnets must not be accessible from the public internet.

What should the solutions architect do to meet these requirements?

- A. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Update all the VPC route tables, and add a route for ::/0 to the internet gateway.
- B. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Update the VPC route tables for all private subnets, and add a route for ::/0 to the NAT gateway.
- C. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Create an egress-only internet gateway. Update the VPC route tables for all private subnets, and add a route for ::/0 to the egress-only internet gateway.
- D. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Create a new NAT gateway, and enable IPv6 support. Update the VPC route tables for all private subnets, and add a route for ::/0 to the IPv6-enabled NAT gateway.

Correct Answer: C

Community vote distribution

C (92%)

8%

 **George88** Highly Voted 2 years, 1 month ago

Answer: C

<https://repost.aws/knowledge-center/configure-private-ipv6-subnet>

upvoted 13 times

 **cypkir** Highly Voted 2 years, 1 month ago

Selected Answer: C

Answer: C

upvoted 6 times

 **AzureDP900** Most Recent 1 year, 1 month ago

C is correct

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Associating an Amazon-provided IPv6 CIDR block with the VPC and all subnets ensures that the EC2 instances in the VPC can use IPv6 without requiring additional configuration.

Creating an egress-only internet gateway allows traffic from the public internet to exit the VPC, but prevents incoming traffic (ingress) from reaching the VPC. This meets the requirement that EC2 instances in private subnets must not be accessible from the public internet.

Updating the VPC route tables for all private subnets and adding a route for ::/0 to the egress-only internet gateway ensures that traffic destined for IPv6 addresses outside the VPC can exit through the egress-only internet gateway.

upvoted 1 times

 **juanife** 10 months, 1 week ago

I think you wrote it incorrectly, precisely in the part in which you say ' allows traffic from the public internet to exit the VPC'. Did you mean 'allows traffic from the VPC to the public internet', right?

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 1 times

 **yuliaqwerty** 2 years ago

[C https://docs.aws.amazon.com/vpc/latest/userguide/vpc-migrate-ipv6.html](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-migrate-ipv6.html)

upvoted 3 times

✉  **GaryQian** 2 years ago

Selected Answer: C

IPv6 can only be used by Egress only gateway
upvoted 6 times

✉  **ayadmawla** 2 years ago

Selected Answer: C

IP6 --> Egress GW
upvoted 3 times

✉  **J0n102** 2 years ago

Selected Answer: C

Answer: C
upvoted 1 times

✉  **shaaam80** 2 years ago

Selected Answer: C

Answer C. No NAT gateway for IPv6 subnets. Only Egress-only Internet gateway to allow only outbound traffic from private subnets.
upvoted 6 times

✉  **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

Answer: B

Explanation:

* Updating the existing VPC and associating an Amazon-provided IPv6 CIDR block with the VPC and all subnets will enable the EC2 instances to use IPv6
* Updating the VPC route tables for all private subnets and adding a route for ::/0 to the NAT gateway will ensure that the EC2 instances that are in private subnets are not accessible from the public internet
upvoted 2 times

✉  **Jahangeer_17** 2 years ago

NAT gateway does not support IPv6.
You should use egress-only internet gateway in-place of NAT gateway for IPv6.
<https://repost.aws/knowledge-center/configure-private-ipv6-subnet>
upvoted 2 times

✉  **vibzr2023** 1 year, 11 months ago

My Answer is C because of ease and cost effective... NAT gateway do support IPv6 indirectly which is NAT64 and DNS64 provide a workaround for IPv6-to-IPv4 communication
<https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-nat64-dns64.html>
upvoted 1 times

✉  **igor12ghsj577** 1 year, 11 months ago

Be careful ! This guy gives wrong answers on purpose...
upvoted 3 times

Question #366

Topic 1

A company is using Amazon API Gateway to deploy a private REST API that will provide access to sensitive data. The API must be accessible only from an application that is deployed in a VPC. The company deploys the API successfully. However, the API is not accessible from an Amazon EC2 instance that is deployed in the VPC.

Which solution will provide connectivity between the EC2 instance and the API?

- A. Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows apigateway:* actions. Disable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC. Use the VPC endpoint's DNS name to access the API.
- B. Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows the execute-api:Invoke action. Enable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC endpoint. Use the API endpoint's DNS names to access the API.
- C. Create a Network Load Balancer (NLB) and a VPC link. Configure private integration between API Gateway and the NLB. Use the API endpoint's DNS names to access the API.
- D. Create an Application Load Balancer (ALB) and a VPC Link. Configure private integration between API Gateway and the ALB. Use the ALB endpoint's DNS name to access the API.

Correct Answer: B

Community vote distribution

B (100%)

 **cypkir** Highly Voted 2 years, 1 month ago

Selected Answer: B

Answer: B

upvoted 6 times

 **AzureDP900** Most Recent 1 year, 1 month ago

B is correct

Creating an interface VPC endpoint for API Gateway allows the EC2 instance to access the API without having to traverse the internet. Attaching an endpoint policy that allows the execute-api:Invoke action enables the EC2 instance to invoke the API, but only if it has the necessary permissions and credentials.

Enabling private DNS naming for the VPC endpoint ensures that the EC2 instance can use the endpoint's DNS name to access the API. Configuring an API resource policy that allows access from the VPC endpoint enables the EC2 instance to access the API without having to authenticate again.

upvoted 1 times

 **tushar321** 1 year, 8 months ago

C. Why not C here ?

upvoted 2 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

 **ayadmaawla** 2 years ago

Selected Answer: B

Answer B. Enable Private naming for VPC Endpoint

upvoted 3 times

 **shaaam80** 2 years ago

Selected Answer: B

Answer B. Enable Private naming for VPC Endpoint

upvoted 3 times

 **nublit** 2 years ago

Selected Answer: B

B is correct

upvoted 2 times

Question #367

A large payroll company recently merged with a small staffing company. The unified company now has multiple business units, each with its own existing AWS account.

A solutions architect must ensure that the company can centrally manage the billing and access policies for all the AWS accounts. The solutions architect configures AWS Organizations by sending an invitation to all member accounts of the company from a centralized management account.

What should the solutions architect do next to meet these requirements?

- A. Create the OrganizationAccountAccess IAM group in each member account. Include the necessary IAM roles for each administrator.
- B. Create the OrganizationAccountAccessPolicy IAM policy in each member account. Connect the member accounts to the management account by using cross-account access.
- C. Create the OrganizationAccountAccessRole IAM role in each member account. Grant permission to the management account to assume the IAM role.
- D. Create the OrganizationAccountAccessRole IAM role in the management account. Attach the AdministratorAccess AWS managed policy to the IAM role. Assign the IAM role to the administrators in each member account.

Correct Answer: C

Community vote distribution

C (92%)	8%
---------	----

 **heatblur**  2 years, 1 month ago

Selected Answer: C

C is the Answer:

This setup enables centralized management of member accounts from the management account. Administrators in the management account can assume the OrganizationAccountAccessRole in member accounts to perform necessary actions, aligning with AWS best practices for Organizations. It simplifies the management and auditing of various accounts and ensures a standardized role exists across all accounts for consistent access control.

upvoted 11 times

 **yuliaqwert**  2 years ago

C https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html#orgs_manage_accounts_create-cross-account-role

upvoted 5 times

 **JMAN1** 1 year, 11 months ago

Thank you!

upvoted 2 times

 **AzureDP900**  1 year, 1 month ago

Option C is correct

By creating an IAM role in each member account, you can define the specific permissions and controls for access to resources within that account.

Granting permission to the management account to assume the IAM role allows administrators in one account to take control of another account, while still maintaining a centralized level of control.

Option C is correct because it provides a way to:

Centralize access to resources across multiple accounts

Define specific permissions and controls for each account

Allow administrators in one account to assume control of another account

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: C

Option C

upvoted 1 times

 **ftaws** 1 year, 11 months ago

Is it possible C ? Role in the each member account and management account just grant assume the role. How to implement it? @@

upvoted 1 times

 **ayadmawla** 2 years ago

Selected Answer: C

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

upvoted 3 times

 **J0n102** 2 years ago

Selected Answer: C

Answer: C

upvoted 2 times

 **shaam80** 2 years ago

Selected Answer: C

OrganizationAccountAccessRole is created in the member accounts and this role can be assumed by IAM users in the Management account to perform any actions in member accounts. Answer C.

upvoted 3 times

 **George88** 2 years, 1 month ago

Answer: C

https://fullbacksystems.com/aws_organizations/

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Answer D. Be is not correct

To centrally manage the billing and access policies for all the AWS accounts of a company that has multiple business units, each with its own existing AWS account, the following steps can be taken:

- 1.Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the strongly recommended controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- 2.Create the OrganizationAccountAccessRole IAM role in the management account. Attach the AdministratorAccess AWS managed policy to the IAM role. Assign the IAM role to the administrators in each member account

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

Option B is the correct solution because it creates the OrganizationAccountAccessPolicy IAM policy in each member account and connects the member accounts to the management account by using cross-account access. This will ensure that the company can centrally manage the billing and access policies for all the AWS accounts.

upvoted 2 times

 **cypkir** 2 years, 1 month ago

Selected Answer: C

Answer: C

upvoted 3 times

Question #368

A company has application services that have been containerized and deployed on multiple Amazon EC2 instances with public IPs. An Apache Kafka cluster has been deployed to the EC2 instances. A PostgreSQL database has been migrated to Amazon RDS for PostgreSQL. The company expects a significant increase of orders on its platform when a new version of its flagship product is released.

What changes to the current architecture will reduce operational overhead and support the product release?

- A. Create an EC2 Auto Scaling group behind an Application Load Balancer. Create additional read replicas for the DB instance. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.
- B. Create an EC2 Auto Scaling group behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.
- C. Deploy the application on a Kubernetes cluster created on the EC2 instances behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.
- D. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate and enable auto scaling behind an Application Load Balancer. Create additional read replicas for the DB instance. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

Correct Answer: D*Community vote distribution*

D (88%)	8%
---------	----

 **J0n102**  2 years ago

Selected Answer: D

Option D with Fargate can potentially provide a more serverless-like experience, emphasizing ease of use and reduced operational responsibilities

upvoted 9 times

 **AzureDP900**  1 year, 1 month ago

Option D is the best choice because it provides a scalable and highly available architecture that can handle increased traffic during the product release.

By deploying on Amazon EKS with AWS Fargate, the company can take advantage of managed container services, auto-scaling, and load balancing, which reduces operational overhead.

Creating additional read replicas for the DB instance ensures high availability and reduces the load on the primary instance.

Deploying the Kafka cluster as an Amazon Managed Streaming for Apache Kafka cluster provides a managed and scalable service that can handle large volumes of data.

Storing static content in Amazon S3 behind an Amazon CloudFront distribution reduces the load on the application services and provides faster content delivery.

upvoted 1 times

 **michele_scar** 1 year, 6 months ago

Selected Answer: B

It's not specified if there are in pipe a refactoring or rearchitecting and how many time you have to rearchitect before going to prod. I will go with B because D should increment the delay to go in prod; instead with B it's immediate the production deploy.

upvoted 2 times

 **career360guru** 1 year, 9 months ago

Selected Answer: D

Option D

upvoted 2 times

 **AC1984** 1 year, 11 months ago

Selected Answer: C

Why do you need fargate when you are hosting on kubernetes

upvoted 1 times

 **AC1984** 1 year, 11 months ago

Modified my answer to D. Fargate will handle unexpected load.

upvoted 3 times

 **thotwielder** 1 year, 11 months ago

Selected Answer: D

cloudfront for static content.
Then aws kubernetes over kubernetes on ec2.
upvoted 2 times

✉ **yuliaqwerty** 2 years ago

My answer is C. I don't agree with D "significant increase of orders " means more data, read replicas will not resolve this
upvoted 2 times

✉ **MegalodonBolado** 1 year, 11 months ago

On C, the number of EC2 instances is fixed, so can't provide elasticity beyond this limit. Could be another history if ASG was mentioned.
upvoted 1 times

✉ **shaaam80** 2 years ago

Selected Answer: D

Answer - D
upvoted 3 times

✉ **devalenzuela86** 2 years, 1 month ago

Selected Answer: D

D for sure
upvoted 3 times

✉ **cypkir** 2 years, 1 month ago

Selected Answer: D

Answer: D
upvoted 3 times

Question #369

Topic 1

A company hosts a VPN in an on-premises data center. Employees currently connect to the VPN to access files in their Windows home directories. Recently, there has been a large growth in the number of employees who work remotely. As a result, bandwidth usage for connections into the data center has begun to reach 100% during business hours.

The company must design a solution on AWS that will support the growth of the company's remote workforce, reduce the bandwidth usage for connections into the data center, and reduce operational overhead.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Create an AWS Storage Gateway Volume Gateway. Mount a volume from the Volume Gateway to the on-premises file server.
- B. Migrate the home directories to Amazon FSx for Windows File Server.
- C. Migrate the home directories to Amazon FSx for Lustre.
- D. Migrate remote users to AWS Client VPN.
- E. Create an AWS Direct Connect connection from the on-premises data center to AWS.

Correct Answer: BD

Community vote distribution

BD (100%)

 **AzureDP900** 1 year, 1 month ago

Option B is correct because migrating home directories to Amazon FSx for Windows File Server allows employees to access their files from anywhere, without the need to connect through a VPN or to an on-premises file server. This reduces the bandwidth usage and operational overhead associated with connecting to a VPN.

Option D is also correct because migrating remote users to AWS Client VPN provides a secure and scalable way for employees to access company resources and files from anywhere. This solution reduces the need for employees to connect through a VPN or to an on-premises file server, which in turn reduces bandwidth usage and operational overhead.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: BD

Option B and D

upvoted 1 times

 **yuliaqwerty** 2 years ago

BC For Migrating existing file storage to FSx for Windows File Server is needed Direct Connect
<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-fsx.html>

upvoted 1 times

 **yuliaqwerty** 2 years ago

I mean BE

upvoted 2 times

 **ayadmawla** 2 years ago

Selected Answer: BD

Agreed: Answer: B & D

upvoted 2 times

 **srv321** 2 years ago

Why not direct connect ? the question did not mention about cost but rather it mentions "reduce the bandwidth usage for connections into the data center" . any thoughts ?

upvoted 1 times

 **GoKhe** 2 years ago

Key is "... a large growth in the number of employees who work remotely." These users are connecting from home to their data centre over VPN. They now need to be diverted to AWS. It therefore makes sense VPN Client here, not DX

upvoted 9 times

 **vibzr2023** 1 year, 11 months ago

Agree...My answer is B&D

AWS Client VPN allows remote users to securely connect to AWS resources, including Amazon FSx for Windows File Server, without the need for a VPN connection to the on-premises data center. Migrating remote users to AWS Client VPN can help reduce bandwidth usage for connections into the on-premises data center, as users will access resources directly from AWS. This approach

is more scalable and can be managed with less operational overhead compared to maintaining a VPN infrastructure in the on-premises data center.

upvoted 4 times

 **J0n102** 2 years ago

Selected Answer: BD

Answer: B & D

upvoted 2 times

 **shaaam80** 2 years ago

Selected Answer: BD

B & D are correct

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: BD

BD for sure

upvoted 2 times

 **cypkir** 2 years, 1 month ago

Selected Answer: BD

Answer: BD

upvoted 2 times

Question #370

Topic 1

A company has multiple AWS accounts. The company recently had a security audit that revealed many unencrypted Amazon Elastic Block Store (Amazon EBS) volumes attached to Amazon EC2 instances.

A solutions architect must encrypt the unencrypted volumes and ensure that unencrypted volumes will be detected automatically in the future. Additionally, the company wants a solution that can centrally manage multiple AWS accounts with a focus on compliance and security.

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

- A. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the strongly recommended controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- B. Use the AWS CLI to list all the unencrypted volumes in all the AWS accounts. Run a script to encrypt all the unencrypted volumes in place.
- C. Create a snapshot of each unencrypted volume. Create a new encrypted volume from the unencrypted snapshot. Detach the existing volume, and replace it with the encrypted volume.
- D. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the mandatory controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- E. Turn on AWS CloudTrail. Configure an Amazon EventBridge rule to detect and automatically encrypt unencrypted volumes.

Correct Answer: AC

Community vote distribution

AC (84%) AE (16%)

 **J0n102**  2 years ago

Selected Answer: AC

A: strongly recommended controls - detects whether the Amazon EBS volumes attached to an Amazon EC2 instance are encrypted
C: Best way to encrypt an unencrypted volume

upvoted 6 times

 **Russ99**  2 years ago

Selected Answer: AC

the appropriate guardrail is: A
Strongly recommended guardrail: Detect Whether Encryption is Enabled for Amazon EBS Volumes Attached to Amazon EC2 Instances.

This guardrail continuously monitors your environment and detects any EC2 instances with unencrypted EBS volumes attached
upvoted 5 times

 **AzureDP900**  1 year, 1 month ago

Option A is correct because setting up an organization with AWS Control Tower will help centrally manage multiple AWS accounts and ensure compliance and security. Joining all accounts to the organization ensures that encryption is enforced across all accounts.

Option C is also correct because creating snapshots of each unencrypted volume, encrypting them, and replacing the original volumes with encrypted ones is a more efficient and automated way to handle the encryption.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: AC

A and C are correct according to

<https://docs.aws.amazon.com/controlltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>
upvoted 2 times

 **kejam** 1 year, 11 months ago

Selected Answer: AC

<https://docs.aws.amazon.com/controlltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>
upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: AC

Option A & C
upvoted 1 times

 **ayadmawla** 2 years ago

Selected Answer: AC

Answer A+C
upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: AC
Answer AC
upvoted 2 times

 **tfl** 2 years ago

Selected Answer: AC
AC for sure. Unencrypted EBS detection is part of strongly recommended guardrails, and you cannot encrypt a volume or snapshot in place. You need to create a new encrypted volume from an unencrypted snapshot, and attach it to the instance.
upvoted 5 times

 **shaaam80** 2 years ago

Selected Answer: AE
"and ensure that unencrypted volumes will be detected automatically in the future. " - to automatically detect unencrypted volumes, we need CloudTrail and Eventbridge to detect and encrypt unencrypted volumes automatically.
upvoted 3 times

 **shaaam80** 2 years ago

Changing to A&C.
upvoted 2 times

 **pic1** 2 years ago

Selected Answer: AE
"...centrally manage multiple AWS accounts with a focus on compliance and security", and "...ensure that unencrypted volumes will be detected automatically..."
upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

BD for sure
upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Change to BE

Creating an organization in AWS Organizations, setting up AWS Control Tower, and turning on the mandatory controls (guardrails) (Option D) is not required since the strongly recommended controls (guardrails) are sufficient
upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: AC
Answer: A C
upvoted 4 times

 **devalenzuela86** 2 years, 1 month ago

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>

Creating a snapshot of each unencrypted volume, creating a new encrypted volume from the unencrypted snapshot, detaching the existing volume, and replacing it with the encrypted volume (Option C) is not required since the volumes can be encrypted in place
upvoted 1 times

 **heatblur** 2 years, 1 month ago

The volumes can not be encrypted in place -- see the steps (copy/pasted from the link you shared):
1. AWS Config detects an unencrypted EBS volume.
2. An administrator uses AWS Config to send a remediation command to Systems Manager.
3. The Systems Manager automation takes a snapshot of the unencrypted EBS volume.
4. The Systems Manager automation uses AWS KMS to create an encrypted copy of the snapshot.
5. The Systems Manager automation does the following: Stops the affected EC2 instance if it is running. Attaches the new, encrypted copy of the volume to the EC2 instance. Returns the EC2 instance to its original state.

Also, under the Limitations section: "When you remediate existing, unencrypted EBS volumes, ensure that the EC2 instance is not in use. This automation shuts down the instance in order to detach the unencrypted volume and attach the encrypted one. There is downtime while the remediation is in progress."

upvoted 1 times

Question #371

Topic 1

A company hosts an intranet web application on Amazon EC2 instances behind an Application Load Balancer (ALB). Currently, users authenticate to the application against an internal user database.

The company needs to authenticate users to the application by using an existing AWS Directory Service for Microsoft Active Directory directory. All users with accounts in the directory must have access to the application.

Which solution will meet these requirements?

- A. Create a new app client in the directory. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule. Configure the listener rule with the appropriate issuer, client ID and secret, and endpoint details for the Active Directory service. Configure the new app client with the callback URL that the ALB provides.
- B. Configure an Amazon Cognito user pool. Configure the user pool with a federated identity provider (IdP) that has metadata from the directory. Create an app client. Associate the app client with the user pool. Create a listener rule for the ALB. Specify the authenticate-cognito action for the listener rule. Configure the listener rule to use the user pool and app client.
- C. Add the directory as a new IAM identity provider (IdP). Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Configure the new role as the default authenticated user role for the IdP. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule.
- D. Enable AWS IAM Identity Center (AWS Single Sign-On). Configure the directory as an external identity provider (IdP) that uses SAML. Use the automatic provisioning method. Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Attach the new role to all groups. Create a listener rule for the ALB. Specify the authenticate-cognito action for the listener rule.

Correct Answer: B

Community vote distribution

B (66%)	D (28%)	6%
---------	---------	----

 **gustori99**  1 year, 8 months ago

Selected Answer: B

D is complete nonsense. Don't know why so many people are voting for it.

"Configure a role policy that allows access to the ALB" - Come on, guys. ALB is accessed via http or https. You can restrict access via security groups not roles. Also cognito is mentioned in D but cognito is not connected to the SAML provider. So B is the correct answer.
upvoted 12 times

 **ayadmawla**  2 years ago

Selected Answer: B

There are two options either via Cognito or Auth0 and then attach an IDP to one of them.

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

<https://aws.amazon.com/blogs/aws/built-in-authentication-in-alb/>

upvoted 8 times

 **AzureDP900**  1 year, 1 month ago

Option B is right because:

Cognito provides a federated identity provider that can integrate with the directory, making it easy to authenticate users against the application.

By configuring the user pool with the metadata from the directory, you can leverage the existing authentication mechanism in the directory.

Creating an app client and associating it with the user pool allows you to use Cognito as the authentication provider for the ALB. Specifying the authenticate-cognito action for the listener rule enables Cognito-based authentication for the ALB.

upvoted 1 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: B

Option B focuses more on user identity management for web and mobile applications, providing rich user management features and flexible authentication processes. If the company's main requirement is to manage user identities and data for applications, then option B may be more appropriate.

Option D focuses more on providing single sign on access to AWS accounts and applications for organizational employees, as well as integration with external identity providers through SAML. If the company wishes to integrate its existing identity management system

(such as Microsoft Active Directory) with AWS accounts and applications, and wants employees to easily access these resources, then option D may be more appropriate.

upvoted 2 times

kgp0j 1 year, 4 months ago

Selected Answer: B

IAM Identity Center is primarily designed for single sign-on (SSO) access to AWS accounts, applications, and services that are integrated with AWS. It provides centralized identity management for users accessing these resources.

In contrast, the requirement here is for web application authentication directly tied to an intranet web application hosted on EC2 instances, not for general access to AWS resources.

upvoted 3 times

vip2 1 year, 5 months ago

Selected Answer: B

ALB Authenticate users through corporate identities, using SAML, OpenID Connect (OIDC), or OAuth, through the user pools supported by Amazon Cognito.

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

upvoted 1 times

9f02c8d 1 year, 6 months ago

Option B

upvoted 1 times

seetpt 1 year, 7 months ago

Selected Answer: B

B vote

upvoted 2 times

seetpt 1 year, 7 months ago

Selected Answer: B

B vote

upvoted 2 times

seetpt 1 year, 7 months ago

I vote for B

upvoted 1 times

TonytheTiger 1 year, 8 months ago

Selected Answer: D

Option D: Per AWS doc " An Amazon Cognito user pool is a user directory for web and mobile app authentication and authorization. ". The question states " The company hosts an intranet web application". So, you can't select Cognito

<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html>

upvoted 1 times

VerRi 1 year, 9 months ago

Selected Answer: B

A: The Active Directory directory does not use OIDC.

B: Make sense.

C: Cannot add the directory as a new IAM IdP.

D: Why "authenticate-cognito action"

upvoted 5 times

Dgix 1 year, 9 months ago

Selected Answer: B

A: Doesn't support OIDC directly.

B: ALBs can interface directly to Cognito. The correct answer.

C: Rubbish, as IAM doesn't directly interface to any AD.

D: Mixes things up royally.

upvoted 6 times

JOKERO 1 year, 9 months ago

Attach the new role to all groups ???

upvoted 1 times

career360guru 1 year, 9 months ago

Selected Answer: D

Option D

upvoted 2 times

ftaws 1 year, 11 months ago

refer to below.

I am on the Amazon Cognito team.

Amazon Cognito is our identity management solution for developers building B2C or B2B apps for their customers, which makes it a customer-targeted IAM and user directory solution.

AWS SSO is focused on SSO for employees accessing AWS and business apps, initially with Microsoft AD as the underlying employee directory.

We plan to integrate Cognito User Pools and AWS SSO as part of our roadmap.

upvoted 2 times

 **ftaws** 1 year, 11 months ago

Selected Answer: D

They have already AD so we have to use SSO.

upvoted 4 times

Question #372

Topic 1

A company has a website that serves many visitors. The company deploys a backend service for the website in a primary AWS Region and a disaster recovery (DR) Region.

A single Amazon CloudFront distribution is deployed for the website. The company creates an Amazon Route 53 record set with health checks and a failover routing policy for the primary Region's backend service. The company configures the Route 53 record set as an origin for the CloudFront distribution. The company configures another record set that points to the backend service's endpoint in the DR Region as a secondary failover record type. The TTL for both record sets is 60 seconds.

Currently, failover takes more than 1 minute. A solutions architect must design a solution that will provide the fastest failover time.

Which solution will achieve this goal?

- A. Deploy an additional CloudFront distribution. Create a new Route 53 failover record set with health checks for both CloudFront distributions.
- B. Set the TTL to 4 second for the existing Route 53 record sets that are used for the backend service in each Region.
- C. Create new record sets for the backend services by using a latency routing policy. Use the record sets as an origin in the CloudFront distribution.
- D. Create a CloudFront origin group that includes two origins, one for each backend service Region. Configure origin failover as a cache behavior for the CloudFront distribution.

Correct Answer: D*Community vote distribution*

D (100%)

  **ayadmaWla** Highly Voted  2 years ago**Selected Answer: D**

In summary, CloudFront Origin Failover fails over immediately when it detects a failure from the origin. However, it may also introduce latency as it tries to forward every request to the primary origin first.

Route53 DNS Failover offers more stability, but it requires more time to detect failure from the origin. However, you can combine both solutions to increase availability without affecting performance. See: <https://aws.amazon.com/blogs/networking-and-content-delivery/improve-web-application-availability-with-cloudfront-and-route53-hybrid-origin-failover/#:~:text=In%20summary%2C%20CloudFront%20Origin%20Failover,detect%20failure%20from%20the%20origin.>
upvoted 10 times

  **shaaam80** Highly Voted  2 years ago**Selected Answer: D**

Answer - D. Create a Cloud origin group with both Primary and DR origin and configure Origin failover in the Cache behavior. Reducing TTL might impact performance as all or most of the requests will be authoritative and place heavy load on DNS.

upvoted 5 times

  **AzureDP900** Most Recent  1 year, 1 month ago

D is right

The current solution uses health checks and failover routing policy, which can take more than 1 minute to fail over.

By creating an origin group with two origins (one for each backend service region), you can ensure that the CloudFront distribution will automatically switch to the other origin when the primary origin becomes unavailable.

Setting the TTL to 4 seconds for the existing record sets (option B) would not significantly improve failover time, as it's still a health check-based approach.

Deploying an additional CloudFront distribution and creating new Route 53 record sets with health checks (option A) is unnecessary and would add complexity.

Creating new record sets using latency routing policy (option C) might help distribute traffic between the two origins, but it wouldn't improve failover time.

upvoted 1 times

  **career360guru** 1 year, 11 months ago**Selected Answer: D**

Option D

upvoted 1 times

 **yuliaqwerty** 2 years ago

D see:<https://aws.amazon.com/blogs/networking-and-content-delivery/improve-web-application-availability-with-cloudfront-and-route53-hybrid-origin-failover/>

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: D

D for sure

upvoted 4 times

enforce service restrictions, this SCP must be removed or replaced with a custom SCP.

E - Organizational Units (OUs) help manage multiple accounts together

upvoted 1 times

 **titi_r** 1 year, 2 months ago

Selected Answer: ABE

Isn't this called IAM Access Analyzer instead of Advisor?

upvoted 2 times

 **igor12ghsj577** 1 year, 5 months ago

With a deny list strategy a default SCP allows all services and deny lists must be implemented for any specific services that must be restricted.

upvoted 1 times

 **career360guru** 1 year, 5 months ago

Selected Answer: ABE

A, B and E

upvoted 1 times

 **ayadmawla** 1 year, 6 months ago

Selected Answer: ABE

Agreed E+B+A in that order :)

upvoted 2 times

 **dutchy1988** 1 year, 7 months ago

manage as single unit ->OU's is out of scope (answer e)

deny some of the AWS services -> remove the default FullAWSAccess

allow current in use services -> access advisor to determine recently used services

Use deny list strategy to allow only services that are required

leaves only valid answer: ABD

upvoted 1 times

 **dutchy1988** 1 year, 6 months ago

I have to rectify one answer,

You can use organizational units (OUs) to group accounts together to administer as a single unit.

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

So E is correct, D is incorrect

Answer must be ABE

upvoted 3 times

 **shaaam80** 1 year, 7 months ago

Selected Answer: BDE

To administer multiple accounts together as a single unit - Create OU's with member accounts

Remove blanket Allow on OUs - Remove the default FullAWSAccess SCP from OU's

Review Access Advisor to view which services have been in use or accessed by users / roles

Answer BDE

upvoted 1 times

 **shaaam80** 1 year, 7 months ago

There is no DenyAWSAccess SCP created by default on OUs during creation.

upvoted 2 times

 **shaaam80** 1 year, 6 months ago

correction - ABE

D is wrong, removal of FullAccessSCP without replacing it with a custom SCP is not correct.

A is correct, using a Deny list to restrict access to specific services

upvoted 2 times

 **devalenzuela86** 1 year, 7 months ago

Selected Answer: ABE

ABE for sure

upvoted 1 times

Question #374

A live-events company is designing a scaling solution for its ticket application on AWS. The application has high peaks of utilization during sale events. Each sale event is a one-time event that is scheduled. The application runs on Amazon EC2 instances that are in an Auto Scaling group. The application uses PostgreSQL for the database layer.

The company needs a scaling solution to maximize availability during the sale events.

Which solution will meet these requirements?

- A. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Serverless v2 Multi-AZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.
- B. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL Multi-AZ DB instance with automatically scaling read replicas. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger read replica before a sale event. Fail over to the larger read replica. Create another EventBridge rule that invokes another Lambda function to scale down the read replica after the sale event.
- C. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL MultiAZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.
- D. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Multi-AZ DB cluster. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger Aurora Replica before a sale event. Fail over to the larger Aurora Replica. Create another EventBridge rule that invokes another Lambda function to scale down the Aurora Replica after the sale event.

Correct Answer: D

Community vote distribution

D (100%)

 **heatblur** Highly Voted 2 years ago

Selected Answer: D

D is the best answer.

It leverages scheduled scaling for EC2 instances, which is ideal for handling predictable, high-traffic event peaks. Amazon Aurora PostgreSQL is a high-performance database solution that provides the reliability needed for such critical operations. The use of a larger Aurora Replica during the event and scaling down afterward allows for efficient resource utilization, aligning the database capacity with the fluctuating demand.

While it introduces some complexity in terms of manual replica management, this approach offers a good balance between performance, reliability, and cost-effectiveness, making it well-suited for the described scenario.

upvoted 8 times

 **cypkir** Highly Voted 2 years, 1 month ago

Selected Answer: D

Answer: D

upvoted 5 times

 **AzureDP900** Most Recent 1 year, 1 month ago

D is best option

upvoted 1 times

 **gfhbox0083** 1 year, 6 months ago

D for sure.

upvoted 1 times

 **duriselvan** 1 year, 10 months ago

key point is Create an Amazon EventBridge - Monitor Application Auto Scaling events with Amazon EventBridge
Amazon EventBridge, formerly called CloudWatch Events, helps you monitor events that are specific to Application Auto Scaling and initiate target actions that use other AWS services. Events from AWS services are delivered to EventBridge in near real time.
<https://docs.aws.amazon.com/autoscaling/application/userguide/monitoring-eventbridge.html>

upvoted 2 times

 **bjexamprep** 1 year, 11 months ago

Selected Answer: D

Bad question design.

Aurora support auto scaling, so the answer should have Aurora autoscaling. But the predictive scaling for ASG in A and C is obviously wrong. And B is using Lambda function to fail over while Aurora already has this feature. Which leaves D the only possible answer. Who the hell designed this stupid answers.

upvoted 4 times

✉ **tmlong18** 1 year, 11 months ago

Aurora auto scaling requires some time to adjust, and cannot handle sudden spikes in traffic.

Auto scaling is more suitable for gradually increasing traffic.

upvoted 3 times

✉ **career360guru** 1 year, 11 months ago

Selected Answer: D

B or D are the possible choices. D is better choice as it uses Aurora engine that has better availability and scaling performance.

upvoted 1 times

✉ **J0n102** 2 years ago

Selected Answer: D

leverages scheduled scaling and Aurora PostgreSQL is high-performance database

upvoted 2 times

✉ **devalenzuela86** 2 years, 1 month ago

Selected Answer: D

Answer D

upvoted 4 times

Question #375

A company runs an intranet application on premises. The company wants to configure a cloud backup of the application. The company has selected AWS Elastic Disaster Recovery for this solution.

The company requires that replication traffic does not travel through the public internet. The application also must not be accessible from the internet. The company does not want this solution to consume all available network bandwidth because other applications require bandwidth.

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

- A. Create a VPC that has at least two private subnets, two NAT gateways, and a virtual private gateway.
- B. Create a VPC that has at least two public subnets, a virtual private gateway, and an internet gateway.
- C. Create an AWS Site-to-Site VPN connection between the on-premises network and the target AWS network.
- D. Create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network.
- E. During configuration of the replication servers, select the option to use private IP addresses for data replication.
- F. During configuration of the launch settings for the target servers, select the option to ensure that the Recovery instance's private IP address matches the source server's private IP address.

Correct Answer: ADE

Community vote distribution

ADE (50%)	DEF (26%)	14%	5%
-----------	-----------	-----	----

 **heatblur**  2 years, 1 month ago

Selected Answer: ADE

ADE

Option D: Create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network.

Option E: During configuration of the replication servers, select the option to use private IP addresses for data replication.

Option A: could be considered if the private subnets are used without the NAT gateways, ensuring internal-only network access
upvoted 10 times

 **MegalodonBolado**  1 year, 11 months ago

Selected Answer: DEF

<https://docs.aws.amazon.com/drs/latest/userguide/quick-start-guide-gs.html>

(E) Data routing and throttling controls how data flows from the external server to the replication servers. If you choose not to use a private IP, your replication servers will be automatically assigned a public IP and data will flow over the public internet. Check "Use private IP for data replication".

(F) On Default DRS launch settings, check "Copy private IP". This way all other servers can transparently reach the recovered server.

(D) Architects could use VPN or AWS DC, but "...The company does not want this solution to consume all available network bandwidth because other applications require bandwidth.", preferably use AWS Direct Connect.

upvoted 8 times

 **Deztroyer88**  7 months, 2 weeks ago

Selected Answer: ACE

A and E are a given but I would chose C over D simply because its more cost effective and easier to implement than AWS direct connect.
upvoted 2 times

 **0dc6cac** 6 months ago

nope, site-to-site still goes through the internet, so it doesn't work here

upvoted 2 times

 **Deztroyer88** 9 months, 2 weeks ago

Selected Answer: CDE

C - This ensures that replication traffic does not travel over the public internet, meeting the security requirement.

D- Direct Connect provides a dedicated, high-bandwidth, and lower-latency connection to AWS, ensuring replication traffic does not consume all available internet bandwidth.

E- Ensures that replication occurs over private connectivity rather than the public internet, aligning with the security requirement.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: ADE

By following these steps, you can meet the requirements of configuring a cloud backup of the on-premises intranet application using AWS Elastic Disaster Recovery, ensuring that replication traffic does not travel through the public internet, preventing the application from being accessible from the internet (since it's deployed in private subnets), and not consuming all available network bandwidth (since you're using a dedicated Direct Connect connection).

upvoted 1 times

✉ **that1guy** 1 year, 2 months ago

Selected Answer: DEF

> By default, data is sent from the source servers to the replication servers over the public internet, using the public IP that was automatically assigned to the replication servers. Transferred data is always encrypted in transit.

> Choose the box to the left of the Use private IP for data replication... option if you want to route the replicated data from your source servers to the staging area subnet through a private network with a VPN, AWS Direct Connect, VPC peering, or another type of existing private connection.

upvoted 1 times

✉ **AloraCloud** 1 year, 2 months ago

Why it cannot be the following:

- A. Create a VPC that has at least two private subnets, two NAT gateways, and a virtual private gateway. - NAT Gateway not necessary
- B. Create a VPC that has at least two public subnets, a virtual private gateway, and an internet gateway. - IGW not required
- C. Create an AWS Site-to-Site VPN connection between the on-premises network and the target AWS network. - You need bandwidth so that teh solution does not impact other applications

upvoted 1 times

✉ **Syre** 1 year, 3 months ago

Selected Answer: ACE

Direct Connect is an overkill for such a solution. You cant set it all up just to do DR.

upvoted 3 times

✉ **ShenYuing** 1 year, 3 months ago

Regarding Option A, I'm not sure why there should be at least 2 subnets in the VPC. When configuring the Elastic Disaster Recovery, you only need to choose 1 subnet as target area. Besides, NAT is not needed here.

For Option F, you can choose "Copy private IP" to match source server's IP address, but this is not a must, it is an optional choice, you don't need to choose it to meet the question's requirement.

I'm really confused

upvoted 2 times

✉ **asquared16** 1 year, 4 months ago

Those who picked A, why would you need the NAT gateways?!

upvoted 1 times

✉ **kgpoj** 1 year, 4 months ago

I am super confused about A

A says Virtual Private Gateway, which is for Site-to-Site VPNs. Why do we need this ???

upvoted 1 times

✉ **vip2** 1 year, 5 months ago

Selected Answer: DEF

replication traffic does not travel through the public internet. --> Not A
must not be accessible from the internet --> Not B

The company does not want this solution to consume all available network bandwidth --> not C, it requires D as dedicated network E and F during the Disaster Recovery step 3 and 4 as described as link below,
<https://docs.aws.amazon.com/drs/latest/userguide/quick-start-guide-gs.html>

upvoted 2 times

✉ **ftaws** 1 year, 11 months ago

We don't need to connect internet, why we need NAT gateway in A?

upvoted 4 times

✉ **marszalekm** 1 year, 10 months ago

<https://docs.aws.amazon.com/drs/latest/userguide/Network-Requirements.html>

There are two ways to establish direct connectivity to the Internet for the VPC of the staging area, as described in the VPC FAQ

1. Public IP address + Internet gateway
2. Private IP address + NAT instance

upvoted 1 times

✉ **marszalekm** 1 year, 10 months ago

Thats the only info I found, however this doesn't exactly answer your question.

upvoted 1 times

✉ **drake2020** 1 year, 8 months ago

the question says not accessible from internet

NAT gateway is for inbound to internet and not internet -> inbound

upvoted 2 times

 **zhooon** 1 year, 11 months ago

How about A,C,E?

A. Create an intranet application and other application in a private subnet.

Intranet applications connect to a private gateway(one).

Other applications connect to the NAT gateway(one).

Eliminates traffic interference.

C. Site-to-Site VPN connect to private gateway.

E. Replicates private IP.

upvoted 4 times

 **zhooon** 1 year, 11 months ago

Can not backup for other application through Site-to-Site VPN.

It is correct Option D. 'Direct Connect gateway'

A, D, E

upvoted 1 times

 **zhooon** 1 year, 11 months ago

Can other applications communicate with the Internet through the NAT gateway?

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: ADE

A, D and E

upvoted 2 times

 **yuliaqwerty** 2 years ago

Answer ADE

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: ADE

Answer ADE

upvoted 2 times

Question #376

Topic 1

A company that provides image storage services wants to deploy a customer-facing solution to AWS. Millions of individual customers will use the solution. The solution will receive batches of large image files, resize the files, and store the files in an Amazon S3 bucket for up to 6 months.

The solution must handle significant variance in demand. The solution must also be reliable at enterprise scale and have the ability to rerun processing jobs in the event of failure.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Step Functions to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.
- B. Use Amazon EventBridge to process the S3 event that occurs when a user uploads an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.
- C. Use S3 Event Notifications to invoke an AWS Lambda function when a user stores an image. Use the Lambda function to resize the image in place and to store the original file in the S3 bucket. Create an S3 Lifecycle policy to move all stored images to S3 Standard-Infrequent Access (S3 Standard-IA) after 6 months.
- D. Use Amazon Simple Queue Service (Amazon SQS) to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image and stores the resized file in an S3 bucket that uses S3 Standard-Infrequent Access (S3 Standard-IA). Create an S3 Lifecycle policy to move all stored images to S3 Glacier Deep Archive after 6 months.

Correct Answer: D

Community vote distribution

D (51%)	B (33%)	Other
---------	---------	-------

 **thala** Highly Voted 2 years, 1 month ago

Selected Answer: B

Considering the requirements, Option B (Amazon EventBridge with AWS Lambda and S3 Lifecycle Expiration Policy) seems to be the most cost-effective and appropriate solution. It combines the scalability and flexibility of AWS Lambda for image processing with the straightforward event handling of Amazon EventBridge, and appropriately manages the image lifecycle with an S3 expiration policy. While Option C is also a strong contender, the misalignment of the lifecycle policy with the requirement makes Option B a better fit. Option A might be more suitable for complex workflows but is likely not needed for this scenario, and Option D includes unnecessary long-term archival steps.

upvoted 18 times

 **AzureDP900** 1 year, 1 month ago

Agreed with B
using Amazon EventBridge, you can meet the company's requirements most cost-effectively:
handle significant variance in demand
Be reliable at enterprise scale
Rerun processing jobs in the event of failure (not explicitly required but ensures reliability)
Move stored images to a colder storage class after 6 months to reduce costs.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

How do you rerun for failure with option B?

SQS can handle "rerun", hence D

upvoted 4 times

 **yuliaqwert** Highly Voted 2 years ago

B is for sure
A no because Step Function is not in list of s3 event destinations <https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html>
C and D has option for storing data longer than 6 months which is not required

upvoted 12 times

 **AloraCloud** 1 year, 2 months ago

Yes it is
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/EventBridge.html>

upvoted 4 times

ak1177 Most Recent 1 month ago

Selected Answer: B

Option B is the best answer. Answer D is not, since it includes to keep files in deep archive which is not cost effective.
upvoted 1 times

vinalt 1 month ago

Selected Answer: B

why store data after 6 months also there is no mention of using any preferred or required s3 storage tier. cannot simply associate cost-effect to S3-IA
upvoted 1 times

Curious76 5 months, 4 weeks ago

Selected Answer: D

The solution will receive batches of large image files, resize the files, and store the files in an Amazon S3 bucket for up to 6 months. It doesn't mean delete after 6 months.
Option D preserves this logic:
Receives the original image and stores it in S3.

Lambda resizes it and stores another copy (the resized one).

You now have both files.

S3 lifecycle rules manage cost:

Store in Standard-IA initially, then move to Glacier Deep Archive if needed, or delete after 6 months.
upvoted 2 times

ak1177 1 month ago

it means that after 6 months files are not needed anymore. so why keep them and increase cost ?

upvoted 1 times

0dc6cac 6 months, 1 week ago

Selected Answer: B

it's definitely not D, there's no point in archiving the data past 6 months.
upvoted 1 times

Chakanetsa 11 months, 4 weeks ago

Selected Answer: B

Option B (Amazon EventBridge with AWS Lambda and S3 Lifecycle Expiration Policy) seems to be the most cost-effective and appropriate solution. It combines the scalability and flexibility of AWS Lambda for image processing with the straightforward event handling of Amazon EventBridge, and appropriately manages the image lifecycle with an S3 expiration policy.
upvoted 1 times

SIJUTHOMASP 1 year ago

Selected Answer: D

Invoking Lambda directly won't give any resiliency - so C is not a choice. Since the Event Bridge solution tries to replace original file - its rule out. Step function can't be destined from S3 - A is out. Hence the right answer is D through SQS meeting the need for re-run.
upvoted 3 times

ak1177 1 month ago

There is no requirement stating that you cannot replace the image. In the end, you only need the resized image, so B is the right choice
upvoted 1 times

henrikhmkharyan59 1 year ago

Selected Answer: D

Options A and B imply replacing the original image, which will cause an execution loop.
Option C doesn't allow rerunning failed jobs.
Therefore, only option D meets all the requirements.
upvoted 2 times

Spike2020 1 year ago

Selected Answer: D

This is a very malformed question. It should be D because SQS can handle failure. But then the archiving policy is not requested. So all options are not optimal in my opinion.
upvoted 4 times

nimbus_00 1 year ago

Selected Answer: B

Archiving and replaying events with Amazon EventBridge
<https://aws.amazon.com/blogs/compute/archiving-and-replaying-events-with-amazon-eventbridge/>
upvoted 1 times

TomTom 1 year ago

Selected Answer: D

Option D is most cost effective
upvoted 2 times

 **youonebe** 1 year ago

Selected Answer: D

need to rerun failed jobs, so D
upvoted 2 times

 **0b43291** 1 year, 1 month ago

Selected Answer: D

Difficult one. Both options B and D meet the specific requirement of storing the files in an Amazon S3 bucket for up to 6 months.

However, when considering the additional requirements of being reliable at enterprise scale, having the ability to rerun processing jobs in the event of failure, and being the most cost-effective solution, option D with Amazon SQS, AWS Lambda, and the S3 Lifecycle policy to transition to Glacier Deep Archive is still the better choice.

No Rerun of jobs with B. Only D
upvoted 2 times

 **Halliphax** 1 year, 1 month ago

Selected Answer: B

"Store the images in S3 for six months" - leaves only option B.

Options C & D mean keeping the images in S3 forever and that's not the more cost effective option compared to just deleting the files as the question implies is a requirement.

upvoted 1 times

 **nimbus_00** 1 year, 1 month ago

Selected Answer: D

You've got to have a buffer for reruns!
For those concerned about the 6 months TTL in S3 remember glacier isn't S3.
upvoted 3 times

 **Daniel76** 1 year, 1 month ago

Selected Answer: B

C and D are out, for keeping data more than 6 months.
A is out, due to S3 event destination does not include step function, which is anyway seldom use for one step action.
Eventbridge does support retry if event fail to go off:
upvoted 1 times

Question #377

A company has an organization in AWS Organizations that includes a separate AWS account for each of the company's departments. Application teams from different departments develop and deploy solutions independently.

The company wants to reduce compute costs and manage costs appropriately across departments. The company also wants to improve visibility into billing for individual departments. The company does not want to lose operational flexibility when the company selects compute resources.

Which solution will meet these requirements?

- A. Use AWS Budgets for each department. Use Tag Editor to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.
- B. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use SCPs to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.
- C. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use Tag Editor to apply tags to appropriate resources. Purchase Compute Savings Plans.
- D. Use AWS Budgets for each department. Use SCPs to apply tags to appropriate resources. Purchase Compute Savings Plans.

Correct Answer: C*Community vote distribution*

C (90%)	10%
---------	-----

 **heatblur** Highly Voted 2 years, 1 month ago

Selected Answer: C

C appears to be the most suitable solution. The combination of consolidated billing, a comprehensive tagging strategy using Tag Editor, and the purchase of Compute Savings Plans provides a balanced approach. This solution offers a centralized view and management of costs, ensures accurate cost allocation through tagging, and maintains flexibility in compute resource selection with the Compute Savings Plans. The Compute Savings Plans are particularly beneficial as they provide savings not only on EC2 instances but also on AWS Fargate and AWS Lambda, offering a broader range of applicability than EC2 Instance Savings Plans.

upvoted 9 times

 **barracouto** Most Recent 9 months ago

Selected Answer: C

The answers are annoying because billing is automatically consolidated with Organizations

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

c is right

By configuring AWS Organizations to use consolidated billing, implementing a tagging strategy, using Tag Editor to apply tags (although it's not strictly necessary), and purchasing Compute Savings Plans, you can meet the company's requirements of reducing compute costs, managing costs effectively, and improving visibility into billing for individual departments while maintaining operational flexibility.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C.

upvoted 2 times

 **vibzr2023** 1 year, 11 months ago

Answer: C

Option A: Lacks consolidated billing, limiting cost visibility and potential discounts.

Option B: SCPs are primarily for compliance enforcement, not tag application.

Option D: Misses consolidated billing's benefits for cost visibility and management.

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: C

Answer C. Compute Savings plan. Tagging resources in each account using Tag editor & Consolidated Billing to view billing across the accounts.

upvoted 2 times

 **HunkBunk** 2 years, 1 month ago

Selected Answer: C

Answer: C

Because for apply Tags to already created resources - you need to use Tag editor.

upvoted 4 times

✉️ **HunkyBunky** 2 years, 1 month ago

Compute Savings Plans - cover Amazon EC2, AWS Lambda, and AWS Fargate usage = operational flexibility

upvoted 2 times

✉️ **George88** 2 years, 1 month ago

Answer: C

Compute Savings Plans covers more resources than EC2 Instance Savings Plans.

You use Tag Editor to apply tags, not SCPs.

upvoted 4 times

✉️ **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 2 times

Question #378

A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket. The company requires that only authenticated users are allowed to post content. The application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB.

What can a solutions architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?

- A. Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using a COGNITO_USER_POOLS authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.
- B. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using an AWS Lambda authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.
- C. Enable an S3 Transfer Acceleration endpoint on the S3 bucket. Use the endpoint when generating the presigned URL. Have the browser interface upload the objects to this URL using the S3 multipart upload API.
- D. Configure an Amazon CloudFront distribution for the destination S3 bucket. Enable PUT and POST methods for the CloudFront cache behavior. Update the CloudFront origin to use an origin access identity (OAI). Give the OAI user 3: PutObject permissions in the bucket policy. Have the browser interface upload objects using the CloudFront distribution.

Correct Answer: C*Community vote distribution*

C (82%)

Other

 **tmlong18** Highly Voted 1 year, 11 months ago

Selected Answer: C

A is wrong.

The limit of API Gateway payload is 10MB

upvoted 6 times

 **MegalodonBolado** Highly Voted 1 year, 11 months ago

Selected Answer: C

<https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

(C)

upvoted 5 times

 **874def1** Most Recent 8 months, 2 weeks ago

Selected Answer: C

A, B out because API gateway cannot handle 100MB, they can handle 10MB limits.

C => faster uploads = S3 transfer acceleration. I assume that user is authenticated separately.

D is out because - Cloudfront does support uploads. However, Cloudfront is for caching the content at the edge and uploads to Cloudfront would not use S3 transfer acceleration as per this option. Faster upload = S3 transfer acceleration which is not mentioned here.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

C is right

S3 Transfer Acceleration: This feature can significantly improve the performance of large file uploads by leveraging AWS' global network and caching capabilities.

Presigned URL with S3 Transfer Acceleration: By including the S3 Transfer Acceleration endpoint in the presigned URL, you can take advantage of the acceleration to reduce upload times.

S3 multipart upload API: Using the S3 multipart upload API allows for resumable uploads, which is essential for large files that may be interrupted during transfer.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: C

C

"Most users are reporting slow upload times for objects larger than 100 MB."

Straight to S3 Transfer Acceleration.

upvoted 2 times

 **nharaz** 1 year, 10 months ago

Selected Answer: D

Presigned URLs still ensure that only authenticated users can upload content, as the generation of a presigned URL requires valid AWS credentials. The URL is temporary and grants the bearer permission to perform the action defined in the URL, in this case, a PUT operation to upload an object

upvoted 1 times

 **nharaz** 1 year, 10 months ago

Sorry I mean = C

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 1 times

 **carpa_jo** 1 year, 12 months ago

C has the most votes currently. How does C ensure that only authenticated users are allowed to post content?

upvoted 1 times

 **MegalodonBolado** 1 year, 11 months ago

S3TA supports presigned URL. The only problem the architect must solve is the slow upload. Multipart upload can overcome TCP speed limitations and S3TA reduces latency.

See the link in my vote

upvoted 2 times

 **yuliaqwert** 2 years ago

C is the easiest

upvoted 1 times

 **ayadmawla** 2 years ago

Selected Answer: A

Answer is A to secure the API.

<https://aws.amazon.com/blogs/compute/uploading-to-amazon-s3-directly-from-a-web-or-mobile-application/#:~:text=Adding%20authentication%20to%20the%20upload%20process&text=You%20can%20restrict%20access%20to,as%20Amazon%20Cognito%20or%20Auth0.>

upvoted 4 times

 **shaam80** 2 years ago

Selected Answer: C

Answer C

upvoted 1 times

 **thala** 2 years, 1 month ago

Selected Answer: C

Considering the primary concern of improving upload performance for large files while maintaining secure access for authenticated users, Option C (Enable S3 Transfer Acceleration and use it in the presigned URL) is the most suitable solution. It directly addresses the issue of slow uploads for large objects by leveraging CloudFront's edge locations for accelerated data transfer to S3, and it works seamlessly with the existing mechanism of generating presigned URLs for authenticated users.

upvoted 5 times

 **cypkir** 2 years, 1 month ago

Selected Answer: C

Answer: C

upvoted 2 times

Question #379

A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS account that supports both development and test environments. New accounts to support production workloads will be needed soon.

The finance department requires a centralized method for payment but must maintain visibility into each group's spending to allocate costs.

The security team requires a centralized mechanism to control IAM usage in all the company's accounts.

What combination of the following options meets the company's needs with the LEAST effort? (Choose two.)

- A. Use a collection of parameterized AWS CloudFormation templates defining common IAM permissions that are launched into each account. Require all new and existing accounts to launch the appropriate stacks to enforce the least privilege model.
- B. Use AWS Organizations to create a new organization from a chosen payer account and define an organizational unit hierarchy. Invite the existing accounts to join the organization and create new accounts using Organizations.
- C. Require each business unit to use its own AWS accounts. Tag each AWS account appropriately and enable Cost Explorer to administer chargebacks.
- D. Enable all features of AWS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts.
- E. Consolidate all of the company's AWS accounts into a single AWS account. Use tags for billing purposes and the IAM's Access Advisor feature to enforce the least privilege model.

Correct Answer: BD

Community vote distribution

BD (71%)

BC (29%)

 dv1 1 year ago

Selected Answer: BC

Question says "what COMBINATION of options", so the combination is 1. AWS org creation and 2. let business units operate as required.
upvoted 1 times

 AzureDP900 1 year, 1 month ago

B and D correct

Option B: Using AWS Organizations to create a new organization from a chosen payer account and defining an organizational unit hierarchy invites existing accounts to join the organization. This allows for centralized management of IAM usage across all accounts, meeting the security team's requirement. Additionally, this approach enables cost allocation and visibility into spending for each group, which meets the finance department's requirement.

Option D: Enabling all features of AWS Organizations and establishing service control policies that filter IAM permissions for sub-accounts provides a comprehensive solution for centralized IAM control. This approach allows for fine-grained control over access and security across all accounts.

upvoted 3 times

 TonytheTiger 1 year, 8 months ago

Selected Answer: BD

Option BD not C: The management account has the responsibilities of a payer account and is responsible for paying all charges that are accrued by the member accounts. You can't change an organization's management account.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html

upvoted 3 times

 TonytheTiger 1 year, 9 months ago

Selected Answer: BD

Option BD - You need to use Service Control Policies (SCP) for the Security Team requirements.

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

upvoted 4 times

 a54b16f 1 year, 10 months ago

Selected Answer: BD

C is wrong: since it didn't mention Organization at all.

We can get each group's cost by utilizing OU.

upvoted 3 times

 Russ99 1 year, 10 months ago

Selected Answer: BC

options B and C offers a balance between centralized management, cost visibility, and minimal disruption during the migration process. The company can leverage AWS Organizations to establish a central structure and implement security controls later, while maintaining separate accounts for business units with tagging and Cost Explorer to ensure cost allocation. i maybe wrong, but these are my picks upvoted 4 times

 **anubha.agrahari** 1 year, 6 months ago

Agreed

upvoted 1 times

 **alexandercamachop** 1 year, 10 months ago

Selected Answer: BC

BC

We need AWS Organization and we need tagging for cost allocation.

Those are the only answers viable.

upvoted 1 times

 **bjexamprep** 1 year, 10 months ago

Selected Answer: BC

"Centralized method for payment" maps to AWS organization. So B is one of the answer.

"maintain visibility into each group's spending to allocate costs" means all resources need to be tagged for Cost Explorer to provide visibility into each group's spending. So, C is one of the answer

I don't think D is a good answer, coz SCP is not a good way for IAM permission control. The usual way is to create different roles and allow different users/groups to assume different roles.

A is wrong because there isn't so called common IAM permissions; and least privilege model is a best practice rather than a detailed template, so there is nothing to enforce.

E Consolidating accounts into one single account is obviously not a good solution.

upvoted 2 times

 **rajkanch** 1 year, 11 months ago

Why not B,C? It looks good to me.

upvoted 2 times

 **career360guru** 1 year, 11 months ago

Selected Answer: BD

Option B and D

upvoted 2 times

 **yuliaqwerty** 2 years ago

Also vote for B and D

upvoted 1 times

 **shaaam80** 2 years ago

B & D - Create Organizations in AWS Organizations from a chosen payer account and invite all member accounts and create new accounts as a part of the Organizations. Enable All features and create appropriate SCPs for services access control.

upvoted 2 times

 **thala** 2 years, 1 month ago

Selected Answer: BD

Options B and D offers a centralized, efficient, and scalable solution that meets both the finance department's and the security team's requirements.

upvoted 4 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: BD

BD for sure

upvoted 2 times

 **cypkir** 2 years, 1 month ago

Selected Answer: BD

Answer: B D

upvoted 2 times

Question #380

Topic 1

A company has a solution that analyzes weather data from thousands of weather stations. The weather stations send the data over an Amazon API Gateway REST API that has an AWS Lambda function integration. The Lambda function calls a third-party service for data pre-processing. The third-party service gets overloaded and fails the pre-processing, causing a loss of data.

A solutions architect must improve the resiliency of the solution. The solutions architect must ensure that no data is lost and that data can be processed later if failures occur.

What should the solutions architect do to meet these requirements?

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue as the dead-letter queue for the API.
- B. Create two Amazon Simple Queue Service (Amazon SQS) queues: a primary queue and a secondary queue. Configure the secondary queue as the dead-letter queue for the primary queue. Update the API to use a new integration to the primary queue. Configure the Lambda function as the invocation target for the primary queue.
- C. Create two Amazon EventBridge event buses: a primary event bus and a secondary event bus. Update the API to use a new integration to the primary event bus. Configure an EventBridge rule to react to all events on the primary event bus. Specify the Lambda function as the target of the rule. Configure the secondary event bus as the failure destination for the Lambda function.
- D. Create a custom Amazon EventBridge event bus. Configure the event bus as the failure destination for the Lambda function.

Correct Answer: B

Community vote distribution

B (90%) 5%

 **heatblur** Highly Voted 2 years, 1 month ago

Selected Answer: B

B is the best solution. It uses two Amazon SQS queues to ensure that incoming data is not lost and can be processed later in case of failures. The primary queue acts as the initial landing point for data from the API Gateway, and the secondary queue serves as a dead-letter queue, capturing data that could not be processed due to third-party service failures or other issues. This setup maintains data integrity and allows for later processing, effectively improving the solution's resiliency.

upvoted 7 times

 **aka1177** Most Recent 2 weeks, 6 days ago

Selected Answer: A

Why not A?

upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 4 months ago

Selected Answer: B

B is correct because using a primary SQS queue with a DLQ ensures that messages are durably stored and can be retried if the third-party service fails, preventing data loss.

upvoted 1 times

 **pk0619** 1 year ago

Selected Answer: B

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-dead-letter-queue.html>

Amazon SQS does not create the dead-letter queue automatically. You must first create the queue before using it as a dead-letter queue. For instructions on creating a queue to use as a dead letter queue, see [Create a queue using the Amazon SQS console](#).

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

B is right

By creating two Amazon SQS queues (primary and secondary) and configuring the secondary queue as a dead-letter queue for the primary queue, you can ensure that failed messages are not lost.

The primary queue will receive successful messages and be used as the main processing queue.

The secondary queue will serve as a catch-all for failed messages, allowing them to be processed later if the failure is temporary or recoverable.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B is most suitable. Eventbridge can not be target for API Gateway

upvoted 2 times

 **career360guru** 1 year, 11 months ago

API gateway will need to do http post to post an event to Eventbridge bus and a single eventbus has throttle limits on events/sec. SQS will be a better and more scalable in this case.

upvoted 2 times

 **shaam80** 2 years ago

Selected Answer: B

Answer - B. Create 2 SQS queues, one for tasks and second as DLQ. Create Lambda as target invocation.

upvoted 3 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 4 times

 **cypkir** 2 years, 1 month ago

Selected Answer: C

Answer: C

upvoted 1 times

Question #381

A company built an ecommerce website on AWS using a three-tier web architecture. The application is Java-based and composed of an Amazon CloudFront distribution, an Apache web server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database.

Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts. The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics. Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis.

Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events? (Choose three.)

- A. Configure the Aurora MySQL DB cluster to publish slow query and error logs to Amazon CloudWatch Logs.
- B. Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2 instances and implement tracing of SQL queries with the X-Ray SDK for Java.
- C. Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis.
- D. Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs.
- E. Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora
- F. Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-Ray.

Correct Answer: ABD

Community vote distribution

ABD (100%)

 thala Highly Voted 2 years, 1 month ago

Selected Answer: ABD

Publishing slow query and error logs to CloudWatch Logs will allow for better analysis of database performance issues. It helps in identifying slow-running queries that might be contributing to the application's performance problems.

Integrating AWS X-Ray SDK into the application will enable tracing of incoming HTTP requests on the EC2 instances. Tracing SQL queries with the X-Ray SDK for Java will provide insights into how database queries are impacting application performance. X-Ray can give a detailed analysis of both service-level and database-level operations, which is essential for diagnosing performance bottlenecks.

Integrating AWS X-Ray SDK into the application will enable tracing of incoming HTTP requests on the EC2 instances. Tracing SQL queries with the X-Ray SDK for Java will provide insights into how database queries are impacting application performance. X-Ray can give a detailed analysis of both service-level and database-level operations, which is essential for diagnosing performance bottlenecks.

upvoted 9 times

 AzureDP900 Most Recent 1 year, 1 month ago

selecting options AB and D would provide good visibility into the application's performance, including:

Database performance (A): Publishing slow query and error logs from Aurora to CloudWatch Logs will help identify bottlenecks in the database.

Web server performance (B): Implementing AWS X-Ray to trace incoming HTTP requests on EC2 instances will help identify issues with the web server layer, such as high latency or timeouts.

Web server logs (D): Installing and configuring an Amazon CloudWatch Logs agent on the EC2 instances will provide visibility into web server logs, which can help identify performance issues with the web server.

upvoted 1 times

 career360guru 1 year, 11 months ago

Selected Answer: ABD

A, B and D

upvoted 2 times

 yuliaqwerty 2 years ago

Answer ABD

upvoted 1 times

 ayadmawla 2 years ago

Selected Answer: ABD

ABD - Effectively we need to collect logs (from DB, Instance) and Trace the Request <-> Response from the calls using XRay to understand what is happening.

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_LogAccess.Concepts.MySQL.html#USER_LogAccess.MySQLDB.PublishAuroraMySQLtoCloudWatchLogs
<https://aws.amazon.com/blogs/mt/simplifying-apache-server-logs-with-amazon-cloudwatch-logs-insights/>
<https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-dotnet-messagehandler.html>
<https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-java-sqlclients.html>

upvoted 2 times

 **JOn102** 2 years ago

Selected Answer: ABD

Answer: ABD

upvoted 1 times

 **GabrielDeBiasi** 2 years ago

Selected Answer: ABD

Answer ABD

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: ABD

Answer ABD

upvoted 2 times

 **cypkir** 2 years, 1 month ago

Selected Answer: ABD

Answer: A B D

upvoted 2 times

Question #382

A company that provisions job boards for a seasonal workforce is seeing an increase in traffic and usage. The backend services run on a pair of Amazon EC2 instances behind an Application Load Balancer with Amazon DynamoDB as the datastore. Application read and write traffic is slow during peak seasons.

Which option provides a scalable application architecture to handle peak seasons with the LEAST development effort?

- A. Migrate the backend services to AWS Lambda. Increase the read and write capacity of DynamoDB.
- B. Migrate the backend services to AWS Lambda. Configure DynamoDB to use global tables.
- C. Use Auto Scaling groups for the backend services. Use DynamoDB auto scaling.
- D. Use Auto Scaling groups for the backend services. Use Amazon Simple Queue Service (Amazon SQS) and an AWS Lambda function to write to DynamoDB.

Correct Answer: C

Community vote distribution

C (100%)

 **AzureDP900** 1 year, 1 month ago

C is right

Using Auto Scaling groups allows you to scale your backend services automatically based on demand, which can help improve performance during peak seasons.

Using DynamoDB auto scaling provides a built-in way to scale the database dynamically, which can help improve read and write performance during periods of high traffic.

This solution is highly scalable and efficient, as it allows AWS to manage the scaling and provisioning of resources automatically.
upvoted 1 times

 **alexandercamachop** 1 year, 10 months ago

Selected Answer: C

Is the correct answer.

Normally B would be right but it says the Least development effort, which would be required in B to re-write the app for Lambda,

Therefore configuring scaling groups, allows to scale to handle the peak season traffic
upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 3 times

 **yuliaqwerty** 2 years ago

C is the best

upvoted 1 times

 **JOn102** 2 years ago

Selected Answer: C

C has the least development effort

upvoted 4 times

 **shaaam80** 2 years ago

Answer C. Autoscaling

upvoted 3 times

 **GabrielDeBiasi** 2 years ago

LEAST development effort -> Answer C

upvoted 2 times

 **thala** 2 years, 1 month ago

Selected Answer: C

Auto scaling

upvoted 4 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: C

C for sure
upvoted 4 times

 **cypkir** 2 years, 1 month ago

Selected Answer: C

Answer: C
upvoted 4 times

Question #383

A company is migrating to the cloud. It wants to evaluate the configurations of virtual machines in its existing data center environment to ensure that it can size new Amazon EC2 instances accurately. The company wants to collect metrics, such as CPU, memory, and disk utilization, and it needs an inventory of what processes are running on each instance. The company would also like to monitor network connections to map communications between servers.

Which would enable the collection of this data MOST cost effectively?

- A. Use AWS Application Discovery Service and deploy the data collection agent to each virtual machine in the data center.
- B. Configure the Amazon CloudWatch agent on all servers within the local environment and publish metrics to Amazon CloudWatch Logs.
- C. Use AWS Application Discovery Service and enable agentless discovery in the existing virtualization environment.
- D. Enable AWS Application Discovery Service in the AWS Management Console and configure the corporate firewall to allow scans over a VPN.

Correct Answer: A

Community vote distribution

A (91%) 6%

 **cypkir** Highly Voted 2 years, 1 month ago

Selected Answer: A

Answer: A

upvoted 9 times

 **Maygam** Highly Voted 2 years, 1 month ago

To get details on network connections, you would need a agent-based discovery. AWS documentation does mention it.
<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>

upvoted 9 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Option A is correct

AWS Application Discovery Service is a free service that allows you to discover and catalog your resources in the cloud. By deploying the data collection agent to each virtual machine, you can collect metrics such as CPU, memory, disk utilization, network connections, and processes running on each instance.

This approach provides a comprehensive inventory of your virtual machines, which is essential for accurate sizing of new Amazon EC2 instances. Option B is not cost effective

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: A

Option A

upvoted 1 times

 **MegalodonBolado** 1 year, 12 months ago

Selected Answer: A

Agentless doesn't support to collect running process data and network inbound/outbound connections information.

<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html#compare-tools>
upvoted 7 times

 **JOn102** 2 years ago

Selected Answer: A

Network connections requires a discovery agent.

<https://tutorialsdojo.com/aws-application-discovery-service/>

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: A

According to this link, VM utilization metrics are picked up by Agentless and not Agent-based. - <https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html#Database%20Discovery>.

At the same time, network connections are pickedup by Agent-based and not Agentless.

Was pretty confident about A, but now i see A doesn't suffice all criteria nor does C.

upvoted 2 times

 **salazar35** 2 years, 1 month ago

Selected Answer: A

agentless discovery supports VMWare only. The question didn't mention VMWare.

upvoted 6 times

 **heatblur** 2 years, 1 month ago

Selected Answer: A

A is the right answer...you must use the agent to pick up on network connections and processes running on the VMs. Agentless will not read those details.

upvoted 3 times

 **thala** 2 years, 1 month ago

Selected Answer: C

<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 1 times

Question #384

Topic 1

A company provides a software as a service (SaaS) application that runs in the AWS Cloud. The application runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in an Auto Scaling group and are distributed across three Availability Zones in a single AWS Region.

The company is deploying the application into additional Regions. The company must provide static IP addresses for the application to customers so that the customers can add the IP addresses to allow lists. The solution must automatically route customers to the Region that is geographically closest to them.

Which solution will meet these requirements?

- A. Create an Amazon CloudFront distribution. Create a CloudFront origin group. Add the NLB for each additional Region to the origin group. Provide customers with the IP address ranges of the distribution's edge locations.
- B. Create an AWS Global Accelerator standard accelerator. Create a standard accelerator endpoint for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.
- C. Create an Amazon CloudFront distribution. Create a custom origin for the NLB in each additional Region. Provide customers with the IP address ranges of the distribution's edge locations.
- D. Create an AWS Global Accelerator custom routing accelerator. Create a listener for the custom routing accelerator. Add the IP address and ports for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.

Correct Answer: B

Community vote distribution

B (93%)

7%

 **ayadmawla** Highly Voted 2 years ago

Selected Answer: B

Answer is B not D. CloudFront does not work with NLB nor does it accept a fixed IP address

A Standard accelerators automatically route traffic to a healthy endpoint that is nearest to your user. Since they're designed to load balance traffic, you can't deterministically route multiple users to a specific EC2 destination behind your accelerator. Custom routing accelerators allows you to do just that.

Another difference is that standard routing accelerators support Network Load Balancers, Application Load Balancers, EC2 instances, and Elastic IPs as endpoints. Custom routing accelerators support only VPC subnet endpoints, each containing one or more EC2 instances that are running your application.

<https://aws.amazon.com/global-accelerator/faqs/#:~:text=A%3A%20Standard%20accelerators%20automatically%20route,you%20to%20do%20just%20that.>

upvoted 14 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Option B

Creating a Standard Accelerator with multiple endpoints, one for each additional region, allows you to provide static IP addresses that can be used by customers to allow lists.

The Global Accelerator IP address is essentially a global IP address that points to an accelerator endpoint. This means that regardless of the customer's location, traffic will be routed to the nearest edge location (determined by AWS's latency algorithms), which is typically located in the closest region.

By providing customers with the Global Accelerator IP address, you can ensure that they can access your application from anywhere in the world.

upvoted 1 times

 **Pics00094** 1 year, 9 months ago

Selected Answer: B

B is correct

upvoted 1 times

 **saggy4** 1 year, 10 months ago

Selected Answer: B

D - With a custom routing accelerator, Global Accelerator does not route traffic based on the geoproximity or health of the endpoint.

A and C - Though it may work but the IP address list keeps on changing and we can use this only in internal AWS implementations where we have access to the prefix list of Cloudfront IPs

B is the correct answer

upvoted 2 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B is most appropriate here because requirement is to route the customer to closest region and not to specific EC2 instance. Option D provides custom routing that is not required in this case.

upvoted 2 times

 **J0n102** 2 years ago

Selected Answer: D

<https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-global-accelerator-custom-routing-accelerators/>

upvoted 2 times

 **shaaam80** 2 years ago

Selected Answer: B

Answer B.

For standard accelerators, the endpoints are Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses.

For custom routing accelerators, the endpoints are virtual private cloud (VPC) subnets with one or more EC2 instances.

upvoted 3 times

 **thala** 2 years, 1 month ago

Selected Answer: B

standard

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: B

Answer: B

upvoted 2 times

Question #385

Topic 1

A company is running multiple workloads in the AWS Cloud. The company has separate units for software development. The company uses AWS Organizations and federation with SAML to give permissions to developers to manage resources in their AWS accounts. The development units each deploy their production workloads into a common production account.

Recently, an incident occurred in the production account in which members of a development unit terminated an EC2 instance that belonged to a different development unit. A solutions architect must create a solution that prevents a similar incident from happening in the future. The solution also must allow developers the possibility to manage the instances used for their workloads.

Which strategy will meet these requirements?

- A. Create separate OUs in AWS Organizations for each development unit. Assign the created OUs to the company AWS accounts. Create separate SCP with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag that matches the development unit name. Assign the SCP to the corresponding OU.
- B. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Update the IAM policy for the developers' assumed IAM role with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit.
- C. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Create an SCP with an allow action and a StringEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit. Assign the SCP to the root OU.
- D. Create separate IAM policies for each development unit. For every IAM policy, add an allow action and a StringEquals condition for the DevelopmentUnit resource tag and the development unit name. During SAML federation, use AWS Security Token Service (AWS STS) to assign the IAM policy and match the development unit name to the assumed IAM role.

Correct Answer: B*Community vote distribution*

B (86%)

14%

 **vibzr2023** Highly Voted 1 year, 11 months ago

Answer: B

Option A: While OUs and SCPs can provide access control, they are more suitable for broader permission boundaries and might not offer the same granularity as STS session tags and IAM policies.

upvoted 6 times

 **AzureDP900** Most Recent 1 year, 1 month ago

B is right

The goal is to prevent developers from managing resources in another development unit's account, but still allow them to manage their own instances.

By passing an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation, you can filter the IAM policies assigned to the developers' assumed IAM roles based on their own development unit name.

Updating the IAM policy with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit ensures that developers cannot manage resources in another development unit's account.

This approach also allows developers to manage their own instances, as long as they are not trying to access resources from another development unit.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option A will not work for common Production Account.

upvoted 4 times

 **shaaam80** 2 years ago

Selected Answer: B

Answer B.

A won't work as developer units needs to deploy resources in the common Production account

upvoted 3 times

 **JOn102** 2 years ago

Selected Answer: B

Answer: B

upvoted 2 times

✉️  **siasiasia** 2 years ago

Selected Answer: B

A won't work for the common account which everybody needs access to. B is the way to go.

upvoted 2 times

✉️  **heatblur** 2 years ago

Selected Answer: B

B is the best answer. This approach involves tagging federated identity sessions with a DevelopmentUnit attribute and then using IAM policies to deny actions if the DevelopmentUnit tag of the resource does not match the aws:PrincipalTag/DevelopmentUnit. This method directly ties permissions to the federated identity, allowing for finer-grained access control that aligns with your requirements.

upvoted 4 times

✉️  **salazar35** 2 years ago

Selected Answer: B

Should be B

upvoted 2 times

✉️  **HunkyBunk** 2 years, 1 month ago

Selected Answer: B

Should be B - <https://www.examtopics.com/discussions/amazon/view/60000-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

✉️  **devalenzuela86** 2 years, 1 month ago

Selected Answer: A

A for sure

upvoted 3 times

✉️  **marszalekm** 1 year, 10 months ago

For sure not, this doesn't address the problem where developers need to deploy in common Production Account.

upvoted 4 times

Question #386

Topic 1

An enterprise company is building an infrastructure services platform for its users. The company has the following requirements:

- Provide least privilege access to users when launching AWS infrastructure so users cannot provision unapproved services.
- Use a central account to manage the creation of infrastructure services.
- Provide the ability to distribute infrastructure services to multiple accounts in AWS Organizations.
- Provide the ability to enforce tags on any infrastructure that is started by users.

Which combination of actions using AWS services will meet these requirements? (Choose three.)

- A. Develop infrastructure services using AWS CloudFormation templates. Add the templates to a central Amazon S3 bucket and add the IAM roles or users that require access to the S3 bucket policy.
- B. Develop infrastructure services using AWS CloudFormation templates. Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account. Share these portfolios with the Organizations structure created for the company.
- C. Allow user IAM roles to have AWSCloudFormationFullAccess and AmazonS3ReadOnlyAccess permissions. Add an Organizations SCP at the AWS account root user level to deny all services except AWS CloudFormation and Amazon S3.
- D. Allow user IAM roles to have ServiceCatalogEndUserAccess permissions only. Use an automation script to import the central portfolios to local AWS accounts, copy the TagOption, assign users access, and apply launch constraints.
- E. Use the AWS Service Catalog TagOption Library to maintain a list of tags required by the company. Apply the TagOption to AWS Service Catalog products or portfolios.
- F. Use the AWS CloudFormation Resource Tags property to enforce the application of tags to any CloudFormation templates that will be created for users.

Correct Answer: BDE*Community vote distribution*

BDE (94%)

6%

 **salazar35** Highly Voted 2 years, 1 month ago

Selected Answer: BDE

BDE - refer Service Catalog

upvoted 7 times

 **AzureDP900** Most Recent 1 year, 1 month ago

BDE are right options

upvoted 1 times

 **nimbus_00** 1 year, 1 month ago

Selected Answer: BDE<https://aws.amazon.com/blogs/mt/simplify-sharing-your-aws-service-catalog-portfolios-in-an-aws-organizations-setup/>

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: BDE

Love this kinda question.

Basically, there is no spaghetti between choices. If you know Service Catalogue is the choice, then you can immediately choose all 3 correct answers without hesitation

upvoted 2 times

 **a54b16f** 1 year, 9 months ago

Selected Answer: BDE

Approved == Service Catalog

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: BDE

Option B, D, E

upvoted 1 times

 **vibzr2023** 1 year, 11 months ago

Answer: B

B. Develop infrastructure using CloudFormation and AWS Service Catalog

D. Use Service Catalog EndUserAccess and automation

E. Use Service Catalog TagOption Library and apply to products/portfolios:

upvoted 3 times

 **vibzr2023** 1 year, 11 months ago

I mean Answer: BDE

upvoted 1 times

 **MegalodonBolado** 2 years ago

Selected Answer: BDE

+1 for BDE

upvoted 1 times

 **HunkyBunky** 2 years, 1 month ago

Selected Answer: BDE

I guess that the right answer should be BDE, because we uses Service catalog, so all other options should to refer on it.

upvoted 4 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: BCE

Answer BCE

upvoted 1 times

Question #387

A company deploys a new web application. As part of the setup, the company configures AWS WAF to log to Amazon S3 through Amazon Kinesis Data Firehose. The company develops an Amazon Athena query that runs once daily to return AWS WAF log data from the previous 24 hours. The volume of daily logs is constant. However, over time, the same query is taking more time to run.

A solutions architect needs to design a solution to prevent the query time from continuing to increase. The solution must minimize operational overhead.

Which solution will meet these requirements?

- A. Create an AWS Lambda function that consolidates each day's AWS WAF logs into one log file.
- B. Reduce the amount of data scanned by configuring AWS WAF to send logs to a different S3 bucket each day.
- C. Update the Kinesis Data Firehose configuration to partition the data in Amazon S3 by date and time. Create external tables for Amazon Redshift. Configure Amazon Redshift Spectrum to query the data source.
- D. Modify the Kinesis Data Firehose configuration and Athena table definition to partition the data by date and time. Change the Athena query to view the relevant partitions.

Correct Answer: D

Community vote distribution

D (100%)

-  **duriselvan** 1 year, 4 months ago
D ans :<https://repost.aws/knowledge-center/athena-queries-long-processing-time>
upvoted 4 times
-  **career360guru** 1 year, 5 months ago
Selected Answer: D
Option D
upvoted 1 times
-  **vibzr2023** 1 year, 5 months ago
Answer: D
Partitioning is a powerful technique for optimizing query performance and cost in Athena, especially for large, growing datasets. Firehose and Athena seamlessly support partitioning, making it easy to implement.
upvoted 2 times
-  **MegalodonBolado** 1 year, 6 months ago
Selected Answer: D
D. The user can split various logs into daily partitions. As daily volume is constant, the time to process will not increase over time.
upvoted 1 times
-  **GaryQian** 1 year, 6 months ago
Selected Answer: D
D is simple and easy to do
upvoted 1 times
-  **Russ99** 1 year, 6 months ago
Selected Answer: D
D, is correct. It looks like option a is viable as well.
upvoted 1 times
-  **George88** 1 year, 7 months ago
Answer: D
<https://aws.amazon.com/blogs/big-data/kinesis-data-firehose-now-supports-dynamic-partitioning-to-amazon-s3/>
upvoted 3 times
-  **devalenzuela86** 1 year, 7 months ago
Selected Answer: D
D is ok
upvoted 3 times

Question #388

Topic 1

A company is developing a web application that runs on Amazon EC2 instances in an Auto Scaling group behind a public-facing Application Load Balancer (ALB). Only users from a specific country are allowed to access the application. The company needs the ability to log the access requests that have been blocked. The solution should require the least possible maintenance.

Which solution meets these requirements?

- A. Create an IPSet containing a list of IP ranges that belong to the specified country. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from an IP range in the IPSet. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- B. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from the specified country. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- C. Configure AWS Shield to block any requests that do not originate from the specified country. Associate AWS Shield with the ALB.
- D. Create a security group rule that allows ports 80 and 443 from IP ranges that belong to the specified country. Associate the security group with the ALB.

Correct Answer: B

Community vote distribution

B (89%)

11%

 **vibzr2023** Highly Voted 1 year, 11 months ago

Answer: B

AWS WAF supports geo-matching rules, allowing you to easily block requests based on country of origin. This eliminates the need to manually manage IP ranges.

Option C - Shield primarily defends against DDoS attacks and does not offer granular geo-blocking capabilities.

upvoted 6 times

 **TomTom** Most Recent 1 year ago

Selected Answer: A

Why not A?

Option A allows for logging of blocked requests while minimizing maintenance needs, as AWS WAF handles updates to IP ranges effectively.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

 **J0n102** 2 years ago

Selected Answer: B

Answer: B

upvoted 1 times

 **GabrielDeBiasi** 2 years ago

Selected Answer: B

B for sure

upvoted 1 times

 **Maygam** 2 years, 1 month ago

Selected Answer: B

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-geo-match.html>

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: B

Answer: B

upvoted 2 times

Question #389

Topic 1

A company is migrating an application from on-premises infrastructure to the AWS Cloud. During migration design meetings, the company expressed concerns about the availability and recovery options for its legacy Windows file server. The file server contains sensitive business-critical data that cannot be recreated in the event of data corruption or data loss. According to compliance requirements, the data must not travel across the public internet. The company wants to move to AWS managed services where possible.

The company decides to store the data in an Amazon FSx for Windows File Server file system. A solutions architect must design a solution that copies the data to another AWS Region for disaster recovery (DR) purposes.

Which solution will meet these requirements?

- A. Create a destination Amazon S3 bucket in the DR Region. Establish connectivity between the FSx for Windows File Server file system in the primary Region and the S3 bucket in the DR Region by using Amazon FSx File Gateway. Configure the S3 bucket as a continuous backup source in FSx File Gateway.
- B. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using AWS Site-to-Site VPN. Configure AWS DataSync to communicate by using VPN endpoints.
- C. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using VPC peering. Configure AWS DataSync to communicate by using interface VPC endpoints with AWS PrivateLink.
- D. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using AWS Transit Gateway in each Region. Use AWS Transfer Family to copy files between the FSx for Windows File Server file system in the primary Region and the FSx for Windows File Server file system in the DR Region over the private AWS backbone network.

Correct Answer: C

Community vote distribution

C (72%)	A (24%)	4%
---------	---------	----

 **SeemaDataReader**  1 year, 11 months ago

Selected Answer: C

- A - for S3, data will traverse via internet
 - B- Site to Site VPN is not required for 2 VPC within AWS
 - C -VPC Peering is the best option for connecting 2 VPCs in different regions
 - D - Transit Gateway not required as the connection is only between 2 VPC, Peering is more cost effective.
- upvoted 6 times

 **LazyAutonomy**  1 year, 11 months ago

Selected Answer: A

Another terrible, terrible question. NONE of the answers meet all the requirements.

- The data cannot be recreated in the event of data corruption or data loss.
- The data must not travel across the public internet.

A - doesn't specify how it avoids traversing the internet (so you can safely assume it traverses the internet), but at least it's an actual "backup" that allows the business to recover corrupted or deleted files.
 B, C, D - file corruption or accidental deletion will propagate to the DR site, no previous versions.

In the exam, if I get this question and I'm feeling really confident with all my other answers, I'll pick A to intentionally get this question "wrong" and hopefully get it flagged as a crap question. But the answer they're looking for is C.

<https://search.brave.com/search?q=statistical+analysis+discrimination+index>

upvoted 5 times

 **nimbus_00** 1 year ago

You can schedule a replication task hourly/ daily so that changes aren't propagated immediately.

upvoted 1 times

 **AloraCloud** 1 year, 2 months ago

This might be required in this age of AI!

upvoted 1 times

 **asquared16** 1 year, 4 months ago

- If it wasn't for exam time, I'd rant in the comment section about it too.
upvoted 1 times
-  **AzureDP900** (Most Recent) 1 year, 1 month ago
C is right
upvoted 1 times
-  **AzureDP900** 1 year, 1 month ago
By using VPC peering and interface VPC endpoints with AWS PrivateLink, option C provides a direct, secure path for data transfer between the two FSx file systems without exposing data to the public internet.
upvoted 1 times
-  **Syre** 1 year, 3 months ago
Selected Answer: B
C is very wrong
upvoted 1 times
-  **Russ99** 1 year, 10 months ago
Selected Answer: C
Option A doesn't indicate what kind of connection will be created between the DR region. Option C is correct.
upvoted 1 times
-  **chelbsik** 1 year, 10 months ago
Selected Answer: C
Go for C
upvoted 1 times
-  **career360guru** 1 year, 11 months ago
Selected Answer: C
Option C
upvoted 1 times
-  **vibzr2023** 1 year, 11 months ago
Option C is correct - keyword - "VPC endpoints with AWS PrivateLink" offer a powerful way to keep data within the AWS network and avoid exposure to the public internet.
upvoted 3 times
-  **MegalodonBolado** 1 year, 12 months ago
Selected Answer: C
Connect FSx VPCs using VPC peering. Allow DataSync client to communicate with server using PrivateLink
<https://aws.amazon.com/blogs/storage/how-to-replicate-amazon-fsx-file-server-data-across-aws-regions/>
upvoted 4 times
-  **yuliaqwerty** 2 years ago
C see <https://aws.amazon.com/blogs/storage/how-to-replicate-amazon-fsx-file-server-data-across-aws-regions/>
upvoted 2 times
-  **shaaam80** 2 years ago
Answer C. FSx fs on Region B and configure VPC Peering. Access using VPC Interface endpoints so data stays private.
upvoted 1 times
-  **pic1** 2 years ago
Selected Answer: A
Option A feels more typical DR with S3 continuous backup and less complexity than option C
upvoted 1 times
-  **dutchy1988** 2 years ago
A is out since company requires data to travel not over the internet. no endpoints are defined so S3 is not targeted over AWS backbone network but over internet.
upvoted 1 times
-  **salazar35** 2 years, 1 month ago
Selected Answer: C
vote C
upvoted 2 times
-  **devalenzuela86** 2 years, 1 month ago
Selected Answer: C
C is ok
upvoted 3 times

Question #390

A company is currently in the design phase of an application that will need an RPO of less than 5 minutes and an RTO of less than 10 minutes. The solutions architecture team is forecasting that the database will store approximately 10 TB of data. As part of the design, they are looking for a database solution that will provide the company with the ability to fail over to a secondary Region.

Which solution will meet these business requirements at the LOWEST cost?

- A. Deploy an Amazon Aurora DB cluster and take snapshots of the cluster every 5 minutes. Once a snapshot is complete, copy the snapshot to a secondary Region to serve as a backup in the event of a failure.
- B. Deploy an Amazon RDS instance with a cross-Region read replica in a secondary Region. In the event of a failure, promote the read replica to become the primary.
- C. Deploy an Amazon Aurora DB cluster in the primary Region and another in a secondary Region. Use AWS DMS to keep the secondary Region in sync.
- D. Deploy an Amazon RDS instance with a read replica in the same Region. In the event of a failure, promote the read replica to become the primary.

Correct Answer: B*Community vote distribution*

B (81%)

C (19%)

 **tama1984** 4 months, 3 weeks ago

Selected Answer: C

Dms would be more expensive, but compared to B, it meets better the RPO. The RPO is of 5 mins, and a read replica lag could easily go over 5mins (especially in a cross-region scenario). When you promote a read replica there is the possibility to lose data because of the lag. I would go for C if the RPO would be higher.

upvoted 1 times

 **tama1984** 4 months, 3 weeks ago

Sorry, I wanted to say "I would go for B if the RPO would be higher."

upvoted 1 times

 **asquared16** 1 year, 4 months ago

Selected Answer: B

It's B. In A, the RTO won't be met using snapshots, in C, well, it works but it's expensive. D doesn't even fulfill the regional requirement.

upvoted 1 times

 **ftaws** 1 year, 11 months ago

Selected Answer: B

I choose B.

C : Aurora DB automatically support sync. We don't use DMS.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B is most cost effective

upvoted 2 times

 **vibzr2023** 1 year, 11 months ago

B for sure... Cross-Region read replicas continuously replicate data from the primary RDS instance to the secondary Region, providing a near-real-time RPO of less than 5 minutes. Failover to the replica can typically be achieved within minutes, meeting the RTO requirement. Option D doesn't provide cross-Region failover, which is a key requirement in this scenario.

upvoted 2 times

 **Russ99** 2 years ago

Selected Answer: B

Option C is not cost effective as per requirement

upvoted 2 times

 **PAUGURU** 2 years ago

Selected Answer: B

B for sure, C is way too expensive even though it's a correct solution

upvoted 2 times

✉  **shaaam80** 2 years ago

Selected Answer: B

Answer B.

upvoted 1 times

✉  **cypkir** 2 years, 1 month ago

Selected Answer: B

Answer: B

upvoted 4 times

✉  **devalenzuela86** 2 years, 1 month ago

Selected Answer: C

C for sure

upvoted 2 times

✉  **devalenzuela86** 2 years, 1 month ago

Sorry, correct D.

deploying an Amazon RDS instance with a read replica in the same Region and promoting the read replica to become the primary in the event of a failure, the company can meet the business requirements of an RPO of less than 5 minutes and an RTO of less than 10 minutes for the application that will store approximately 10 TB of data and provide the ability to fail over to a secondary Region at the lowest cost.

upvoted 1 times

✉  **heatblur** 2 years, 1 month ago

Deploying a read replica in the same region as their existing DB will not provide any failover to a secondary region. They must use a cross region replica to achieve this.

upvoted 4 times

Question #391

A financial company needs to create a separate AWS account for a new digital wallet application. The company uses AWS Organizations to manage its accounts. A solutions architect uses the IAM user Support1 from the management account to create a new member account with finance1@example.com as the email address.

What should the solutions architect do to create IAM users in the new member account?

- A. Sign in to the AWS Management Console with AWS account root user credentials by using the 64-character password from the initial AWS Organizations email sent to finance1@example.com. Set up the IAM users as required.
- B. From the management account, switch roles to assume the OrganizationAccountAccessRole role with the account ID of the new member account. Set up the IAM users as required.
- C. Go to the AWS Management Console sign-in page. Choose "Sign in using root account credentials." Sign in by using the email address finance1@example.com and the management account's root password. Set up the IAM users as required.
- D. Go to the AWS Management Console sign-in page. Sign in by using the account ID of the new member account and the Support1 IAM credentials. Set up the IAM users as required.

Correct Answer: B*Community vote distribution*

B (81%)

D (19%)

 **vibzr2023** Highly Voted 1 year, 11 months ago

Option B correct:

Key word - "OrganizationAccountAccessRole", By assuming the OrganizationAccountAccessRole, you gain temporary, controlled access to the member account without sharing root credentials or creating separate IAM users for cross-account access. This enhances security and reduces administrative overhead.

upvoted 8 times

 **AzureDP900** Most Recent 1 year, 1 month ago

B is right

Using IAM user credentials: The solution architect should use the Support1 IAM user credentials from the management account to create IAM users in the new member account, not the root account credentials.

Assuming roles: By switching roles using the OrganizationAccountAccessRole role with the account ID of the new member account, the solution architect can access the resources and perform actions on behalf of the new member account without using the management account's root credentials.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

 **duriselvan** 1 year, 12 months ago

b ISANS

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

upvoted 1 times

 **ayadmaawla** 2 years ago

Selected Answer: D

D is my answer. Those who chose B are correct about the process and the role that is created when you setup the account. But the user (Support1) that has management account access to setup a new account in the organisation automatically becomes part of the administrators in the new account that gets created and therefore will be able to access the new account with his/her credentials by specifying the new account.

The root user with the 64 character password is also a valid approach but it is not a recommended one by AWS.

upvoted 1 times

 **LazyAutonomy** 1 year, 11 months ago

This is an incorrect understanding.

"But the user (Support1) ... automatically becomes part of the administrators in the new account that gets created" - yes, by virtue of the cross-account OrganizationAccountAccessRole role ONLY. No IAM users are ever automatically created anywhere, ever, never ever, never ever ever. Never! :)

upvoted 3 times

✉️ **FuriouZ** 2 years ago

Selected Answer: B

B as most secure way
upvoted 2 times

✉️ **MegalodonBolado** 2 years ago

Selected Answer: B

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html
upvoted 3 times

✉️ **J0n102** 2 years ago

Selected Answer: B

Answer: B
upvoted 3 times

✉️ **dutchy1988** 2 years ago

quote out of article posted by thala:

"When you create a member account, AWS Organizations automatically creates an AWS Identity and Management (IAM) role called OrganizationAccountAccessRole in the account. This role has full administrative permissions in the member account."

B is only valid answer, assume the role and perform administrative actions
upvoted 3 times

✉️ **thala** 2 years, 1 month ago

Selected Answer: B

<https://repost.aws/knowledge-center/organizations-member-account-access>
upvoted 4 times

✉️ **devalenzuela86** 2 years, 1 month ago

Selected Answer: D

D is the correct answer
upvoted 1 times

✉️ **cypkir** 2 years, 1 month ago

Selected Answer: D

Answer: D
upvoted 1 times

Question #392

A car rental company has built a serverless REST API to provide data to its mobile app. The app consists of an Amazon API Gateway API with a Regional endpoint, AWS Lambda functions, and an Amazon Aurora MySQL Serverless DB cluster. The company recently opened the API to mobile apps of partners. A significant increase in the number of requests resulted, causing sporadic database memory errors.

Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time. Traffic is concentrated during business hours, with spikes around holidays and other events.

The company needs to improve its ability to support the additional usage while minimizing the increase in costs associated with the solution.

Which strategy meets these requirements?

- A. Convert the API Gateway Regional endpoint to an edge-optimized endpoint. Enable caching in the production stage.
- B. Implement an Amazon ElastiCache for Redis cache to store the results of the database calls. Modify the Lambda functions to use the cache.
- C. Modify the Aurora Serverless DB cluster configuration to increase the maximum amount of available memory.
- D. Enable throttling in the API Gateway production stage. Set the rate and burst values to limit the incoming calls.

Correct Answer: A*Community vote distribution*

A (55%)

B (44%)

 **career360guru** Highly Voted 1 year, 11 months ago

Selected Answer: A

Option A because B is more expensive than A
upvoted 11 times

 **vibzr2023** Highly Voted 1 year, 11 months ago

Option A is correct
While A and B do the job but the question says "minimizing the increase in costs associated with the solution".. I'll go with A coz Edge-optimized endpoints cache responses at edge locations closer to users, significantly reducing the number of requests reaching the database and Lambda functions.. While Option B -- While ElastiCache for Redis a good caching solution, it adds complexity and cost compared to edge caching.
upvoted 10 times

 **0dc6cac** Most Recent 6 months, 1 week ago

Selected Answer: A

A is right, it's much cheaper to cache the GET endpoints at the edge location. Creating a redis ElastiCache cluster might prove much more expensive, don't forget about the transfer costs of data from the edge location to the cluster. It will be FAR more expensive.

Lastly, caching in the edge WILL reduce database reads, as there wouldn't be as many requests to the database, because the cache is at the endpoint.
upvoted 2 times

 **Kaps443** 6 months, 2 weeks ago

Selected Answer: B

B. Use ElastiCache (Redis) as a caching layer
ElastiCache for Redis provides a high-performance, in-memory cache that can handle frequent identical queries without hitting the database.

Caching reduces database calls, which avoids memory errors and reduces Aurora Serverless compute scaling, thereby minimizing cost.

Lambda functions can easily be updated to check Redis before querying the database.

Ideal for read-heavy workloads with repeated identical queries, which is exactly the case here.
upvoted 1 times

 **874def1** 8 months, 2 weeks ago

Selected Answer: B

A - can work but will terminate the request at the Cache. Problem is due to DB read load and this is indirect way to reduce DB read load.
B- Best option because will be guaranteed to reduce DB read load
C is bad option because it will permanently increase the cost and cause downtime and still won't guarantee improved READ load.
D -Throttling will spoil the consumer experience and cause damage to the business

Problem states that the DB is experiencing memory issues due to read queries.
I would go for read replicas but that is not an option available. This means, we go with caching.
It will help to reduce interaction with the DB in this case rather than reducing interaction with the entire stack.
In other words, I would choose to have the cache as close as possible to the DB layer.

upvoted 1 times

✉️ **sergza888** 9 months ago

Selected Answer: D

Why it is not D. Question mentions Sporadic requests for short period of time. It is good to implement throttling to reduce error rates. Question does not ask about cache/performance. Besides it could be all new requests so cache would not necessarily help

upvoted 1 times

✉️ **aka1177** 2 weeks, 6 days ago

Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time

upvoted 1 times

✉️ **eesa** 9 months, 1 week ago

Selected Answer: B

Eliminates redundant database queries: Since multiple HTTP GET requests query the same data in a short period, caching the results in ElastiCache for Redis significantly reduces load on Aurora Serverless.

Improves performance: Redis provides low-latency access to frequently requested data, ensuring fast responses.

Reduces costs: By offloading queries from Aurora, this minimizes the need for additional database memory or scaling.

Handles traffic spikes effectively: Redis stores precomputed results, which helps in managing high traffic surges during peak hours.

upvoted 1 times

✉️ **Deztroyer88** 9 months, 2 weeks ago

Selected Answer: B

Option A is for mostly for latency and doesn't reduce the load on the DB.

upvoted 1 times

✉️ **deepakR20** 11 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 2 times

✉️ **ollyone** 12 months ago

Selected Answer: B

Option B

upvoted 1 times

✉️ **henrikhmkhitaryan59** 1 year ago

Selected Answer: A

Taking cost as the primary focus and assuming simple edge caching will suffice, Option A is the better choice.

upvoted 2 times

✉️ **Spike2020** 1 year ago

Selected Answer: A

API Gateway caching reduces database load by serving repeated requests

Caching is ideal for handling identical GET requests

Edge-optimized endpoints improve performance for distributed users

No code changes required

upvoted 2 times

✉️ **alexbraila** 1 year ago

Selected Answer: A

The exact same question is here:

<https://repost.aws/questions/QU4xZPFTZ3TASRtyDteJBM7Q/amazon-elasticache-vs-api-gateway-edge-optimized-endpoint>

I am voting for A, but I am still not convinced

upvoted 2 times

✉️ **alexbraila** 1 year ago

And, indeed, as mentioned by asquared16, Neal Davis has a similar question in one of his exams and he also picked A.

Overall explanation

An edge-optimized API endpoint is best for geographically distributed clients. API requests are routed to the nearest CloudFront Point of Presence (POP). For mobile clients this is a good use case for this type of endpoint. The Regional endpoint is best suited to traffic coming from within the Region only.

You can enable API caching in Amazon API Gateway to cache your endpoint's responses. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of requests to your API.

Why not B:

This will increase costs associated with the solution as the ElastiCache cluster could be expensive.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

option B (using ElastiCache for Redis) provides a more targeted solution that specifically addresses the issue of frequent requests and database memory errors. By caching frequently accessed data in ElastiCache, you can reduce the load on the Aurora Serverless DB cluster and improve performance.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

*Option B

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: B

Both options have their merits and can potentially address the issue to some extent. However, Option B (ElastiCache for Redis cache) is generally considered a more robust and targeted solution for caching database query results and addressing the root cause of redundant queries.

If the application data is highly dynamic or personalized, and cache invalidation is a significant concern, Option B may be the preferred choice, as it allows for more granular control over the caching logic within the application code.

Ultimately, the decision may depend on factors such as the nature of the data, the complexity of the caching requirements, the team's familiarity with the technologies involved, and the overall architectural preferences of the organization.

upvoted 1 times

 **sashenka** 1 year, 2 months ago

Selected Answer: A

Option A: Edge-Optimized Endpoint with API Gateway Caching

This is the most suitable solution because:

API Gateway caching can store frequently accessed query results at edge locations, reducing latency and database load¹⁴

Edge-optimized endpoints serve responses from locations closer to clients, improving performance⁴

It's more cost-effective compared to implementing ElastiCache or increasing database resources⁴

The pricing for HTTP API requests is very economical at \$1 per million requests for the first 300 million¹

upvoted 2 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: B

For those who are saying that option A is the correct one, why should API Gateway Regional Endpoint be converted to Edge-Optimized Endpoint, if caching can be enabled on either? Also, Between the two options, Option B tends to have a lower cost increase in the long term, especially because ElastiCache allows for more direct control over costs and can be adjusted to meet demand. Option A may result in significant data transfer costs, as switching to an Edge-Optimized endpoint involves CloudFront usage costs, which can increase rapidly as traffic grows. Therefore, if the goal is to minimize the increase in costs, Option B (using ElastiCache for Redis) is likely the best choice.,

upvoted 4 times

Question #393

Topic 1

A company is migrating an on-premises application and a MySQL database to AWS. The application processes highly sensitive data, and new data is constantly updated in the database. The data must not be transferred over the internet. The company also must encrypt the data in transit and at rest.

The database is 5 TB in size. The company already has created the database schema in an Amazon RDS for MySQL DB instance. The company has set up a 1 Gbps AWS Direct Connect connection to AWS. The company also has set up a public VIF and a private VIF. A solutions architect needs to design a solution that will migrate the data to AWS with the least possible downtime.

Which solution will meet these requirements?

- A. Perform a database backup. Copy the backup files to an AWS Snowball Edge Storage Optimized device. Import the backup to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.
- B. Use AWS Database Migration Service (AWS DMS) to migrate the data to AWS. Create a DMS replication instance in a private subnet. Create VPC endpoints for AWS DMS. Configure a DMS task to copy data from the on-premises database to the DB instance by using full load plus change data capture (CDC). Use the AWS Key Management Service (AWS KMS) default key for encryption at rest. Use TLS for encryption in transit.
- C. Perform a database backup. Use AWS DataSync to transfer the backup files to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.
- D. Use Amazon S3 File Gateway. Set up a private connection to Amazon S3 by using AWS PrivateLink. Perform a database backup. Copy the backup files to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.

Correct Answer: B*Community vote distribution*

B (100%)

  **shaaam80** Highly Voted 2 years ago**Selected Answer: B**

Answer B - Company has created a DB schema on AWS. So next logical step is to use DMS for DB migration over the Private VIF. VPC Endpoint is also used for DMS.

upvoted 5 times

  **AzureDP900** Most Recent 1 year, 1 month ago

B is right

upvoted 1 times

  **career360guru** 1 year, 11 months ago**Selected Answer: B**

Option B

upvoted 1 times

  **GaryQian** 2 years ago**Selected Answer: B**

Should be B

All other options are Loading data into S3 then copy again to DB . Way to slow

upvoted 2 times

  **FuriouZ** 2 years ago**Selected Answer: B**

B: Definitely DMS

upvoted 2 times

  **GabrielDeBiasi** 2 years ago**Selected Answer: B**

database migration AND least possible downtime? AWS DMS

upvoted 4 times

 **Jonalb** 2 years, 1 month ago

Selected Answer: B

B. Use o AWS Database Migration Service (AWS DMS) para migrar os dados para a AWS. Crie uma instância de replicação DMS em uma sub-rede privada. Crie endpoints VPC para AWS DMS. Configure uma tarefa DMS para copiar dados do banco de dados local para a instância de banco de dados usando carga total mais captura de dados de alteração (CDC). Use a chave padrão do AWS Key Management Service (AWS KMS) para criptografia em repouso. Use TLS para criptografia em trânsito.

upvoted 2 times

 **thala** 2 years, 1 month ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/89247-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

Answer B

upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: B

Answer: B

upvoted 1 times

Question #394

Accompany is deploying a new cluster for big data analytics on AWS. The cluster will run across many Linux Amazon EC2 instances that are spread across multiple Availability Zones.

All of the nodes in the cluster must have read and write access to common underlying file storage. The file storage must be highly available, must be resilient, must be compatible with the Portable Operating System Interface (POSIX), and must accommodate high levels of throughput.

Which storage solution will meet these requirements?

- A. Provision an AWS Storage Gateway file gateway NFS file share that is attached to an Amazon S3 bucket. Mount the NFS file share on each EC2 instance in the cluster.
- B. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses General Purpose performance mode. Mount the EFS file system on each EC2 instance in the cluster.
- C. Provision a new Amazon Elastic Block Store (Amazon EBS) volume that uses the io2 volume type. Attach the EBS volume to all of the EC2 instances in the cluster.
- D. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mode. Mount the EFS file system on each EC2 instance in the cluster.

Correct Answer: D*Community vote distribution*

D (73%)

B (27%)

 **JOn102**  2 years ago

Selected Answer: D

- General purpose performance mode (default)

Ideal for latency-sensitive use cases.

- Max I/O mode

Can scale to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations.

upvoted 17 times

 **titi_r** 1 year, 8 months ago

It's "B", not "D".

"For workloads that require high throughput and IOPS, use Regional file systems configured with the General Purpose performance mode and Elastic throughput.

Note: To achieve the maximum 250,000 read IOPS for frequently accessed data, the file system must use Elastic throughput.

Note: Elastic throughput is available only for file systems that use the General Purpose performance mode.

Max I/O mode is not supported for One Zone file systems or file systems that use Elastic throughput."

-

<https://docs.aws.amazon.com/efs/latest/ug/performance.html>

upvoted 1 times

 **mifune** 1 year, 7 months ago

Yes, that's the reason the description is saying that the EC2 are spread in multiple AZs. It's option "D" the correct one

upvoted 2 times

 **pangchn**  1 year, 9 months ago

Selected Answer: D

D

In contrast, Max I/O file systems are suitable for workloads such as data analytics, media processing, and machine learning. These workloads need to perform parallel operations from hundreds or even thousands of containers and require the highest possible aggregate throughput and IOPS

2 keywords matching the question, Throughput and Data analytic

<https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/storage-efs.html>

upvoted 9 times

 **aka1177**  2 weeks, 6 days ago

Selected Answer: D

For Big Data you must use Max I/O. So answer is D for sure.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

D is right

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: D

Option D is the correct answer because Amazon Elastic File System (Amazon EFS) with Max I/O performance mode meets all the requirements for the big data analytics cluster. EFS provides highly available, resilient, and POSIX-compatible file storage replicated across multiple Availability Zones. Max I/O mode offers high levels of throughput and IOPS required for high-performance workloads like big data analytics. By mounting the EFS file system on each EC2 instance in the cluster, all nodes can access the common file storage with read and write capabilities, enabling seamless collaboration and data sharing across the distributed cluster.

Option B (Amazon EFS General Purpose performance mode): The General Purpose performance mode is suitable for most file system workloads but may not provide the high levels of throughput required for big data analytics workloads.

upvoted 1 times

 **Dannm86** 1 year, 2 months ago

B is the correct answer, Max I/O mode is the legacy version available, for best performance AWS recommends using default mode which is general purpose.

<https://docs.aws.amazon.com/efs/latest/ug/performance.html#performancemodes>

upvoted 1 times

 **seetpt** 1 year, 7 months ago

Selected Answer: D

D for me

upvoted 1 times

 **titi_r** 1 year, 8 months ago

Selected Answer: B

B - correct.

upvoted 1 times

 **CMMC** 1 year, 9 months ago

Selected Answer: D

for analytics workload

upvoted 2 times

 **yog927** 1 year, 9 months ago

Selected Answer: D

D looks correct

upvoted 3 times

 **career360guru** 1 year, 9 months ago

Selected Answer: D

Option D because of High Throughput requirement

upvoted 3 times

 **liquen14** 1 year, 9 months ago

Selected Answer: B

from <https://docs.aws.amazon.com/efs/latest/ug/performance.html#performancemodes>:

"Due to the higher per-operation latencies with Max I/O, we recommend using General Purpose performance mode for all file systems."

upvoted 2 times

 **cf9e355** 1 year, 10 months ago

Selected Answer: D

Performance

....." In contrast, Max I/O file systems are suitable for workloads such as data analytics, media processing, and machine learning. ".....
ref:

<https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/storage-efs.html>

upvoted 3 times

 **marszalekm** 1 year, 10 months ago

Selected Answer: B

IOPS is something different than throughput

upvoted 1 times

 **Exams22** 1 year, 11 months ago

Selected Answer: B

IOPS is not throughput... General Purpose performance mode has a higher throughput

upvoted 2 times

 **tmlong18** 1 year, 11 months ago

Selected Answer: D

"Max I/O performance mode has higher per-operation latencies than General Purpose performance mode. For faster performance, we recommend always using General Purpose performance mode"

No performance requirement but high I/O in the question.

upvoted 2 times

 career360guru 1 year, 11 months ago

Selected Answer: D

Option D as Maximum Throughput is primary requirement here.

upvoted 3 times

Question #395

A company hosts a software as a service (SaaS) solution on AWS. The solution has an Amazon API Gateway API that serves an HTTPS endpoint. The API uses AWS Lambda functions for compute. The Lambda functions store data in an Amazon Aurora Serverless v1 database.

The company used the AWS Serverless Application Model (AWS SAM) to deploy the solution. The solution extends across multiple Availability Zones and has no disaster recovery (DR) plan.

A solutions architect must design a DR strategy that can recover the solution in another AWS Region. The solution has an RTO of 5 minutes and an RPO of 1 minute.

What should the solutions architect do to meet these requirements?

- A. Create a read replica of the Aurora Serverless v1 database in the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region. Promote the read replica to primary in case of disaster.
- B. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region.
- C. Create an Aurora Serverless v1 DB cluster that has multiple writer instances in the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.
- D. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.

Correct Answer: D

Community vote distribution

D (82%)	Other
---------	-------

 **GabrielDeBiasi**  2 years ago

Selected Answer: D

One thing we can learn here is if you see "aurora serverless VERSION 1" -> migrate away from this
upvoted 12 times

 **heatblur**  2 years, 1 month ago

Selected Answer: D

D is the answer.

Convert the Aurora Serverless v1 database to a standard Aurora MySQL global database extending across the source and target regions, launch the solution in the target region, and configure the two regional solutions to work in an active-passive configuration. This approach provides the necessary speed for recovery and data replication to meet the strict RTO and RPO.

Aurora Serverless v1 doesn't support read replicas, cross region replicas, or global databases.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless.html#aurora-serverless.limitations>

upvoted 8 times

 **hiberus**  8 months, 3 weeks ago

Selected Answer: B

Why not B? What is the problem of launching de runbook with SAM?

upvoted 1 times

 **Spike2020** 1 year ago

Selected Answer: B

More cost-effective (no constantly running passive environment)

Uses SAM runbook for automated, consistent deployment

upvoted 1 times

 **TomTom** 1 year ago

Selected Answer: B

Why not B?

Option B can fulfill the requirement for RTO of 5 mins and RPO of 1 min.

Option D Active-Passive require manual intervention and introduce additional complexity.

upvoted 1 times

 **Syre** 1 year, 3 months ago

Selected Answer: B

B is indeed a better choice here because it focuses on using a global database with automated deployment, which is critical for achieving both the RTO and RPO requirements efficiently.

upvoted 2 times

 **career360guru** 1 year, 11 months ago

Selected Answer: D

Option D

upvoted 1 times

 **salazar35** 2 years ago

Selected Answer: D

D will provide "RTO of 5 minutes and an RPO of 1 minute"

upvoted 4 times

 **Jonalb** 2 years, 1 month ago

Selected Answer: D

D. Altere o banco de dados Aurora Serverless v1 para um banco de dados global Aurora MySQL padrão que se estende pela região de origem e pela região de destino. Inicie a solução na região de destino. Configure as duas soluções regionais para funcionarem em uma configuração ativa-passiva.

upvoted 2 times

 **thala** 2 years, 1 month ago

Selected Answer: D

Option D (Change to Aurora MySQL Global Database and Launch Solution in Target Region with Active-Passive Configuration) is the most suitable solution. It addresses both the database replication and application layer readiness in the target region, meeting the specified RTO and RPO requirements.

upvoted 4 times

 **devalenzuela86** 2 years, 1 month ago

D is incorrect because changing the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region and launching the solution in the target Region does not meet the RTO and RPO requirements.

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: A

A for sure

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

To design a disaster recovery (DR) strategy that can recover the solution in another AWS Region with an RTO of 5 minutes and an RPO of 1 minute, the best solution would be to create a read replica of the Aurora Serverless v1 database in the target Region. Then, use AWS SAM to create a runbook to deploy the solution to the target Region. Finally, promote the read replica to primary in case of disaster.

upvoted 1 times

 **shaaam80** 2 years ago

Aurora Serverless v1 db does not support replicas.

upvoted 2 times

 **cypkir** 2 years, 1 month ago

Selected Answer: D

Answer: D

upvoted 1 times

Question #396

Topic 1

A company owns a chain of travel agencies and is running an application in the AWS Cloud. Company employees use the application to search for information about travel destinations. Destination content is updated four times each year.

Two fixed Amazon EC2 instances serve the application. The company uses an Amazon Route 53 public hosted zone with a multivalue record of travel.example.com that returns the Elastic IP addresses for the EC2 instances. The application uses Amazon DynamoDB as its primary data store. The company uses a self-hosted Redis instance as a caching solution.

During content updates, the load on the EC2 instances and the caching solution increases drastically. This increased load has led to downtime on several occasions. A solutions architect must update the application so that the application is highly available and can handle the load that is generated by the content updates.

Which solution will meet these requirements?

- A. Set up DynamoDB Accelerator (DAX) as in-memory cache. Update the application to use DAX. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias. Configure scheduled scaling for the EC2 instances before the content updates.
- B. Set up Amazon ElastiCache for Redis. Update the application to use ElastiCache. Create an Auto Scaling group for the EC2 instances. Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.
- C. Set up Amazon ElastiCache for Memcached. Update the application to use ElastiCache. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias. Configure scheduled scaling for the application before the content updates.
- D. Set up DynamoDB Accelerator (DAX) as in-memory cache. Update the application to use DAX. Create an Auto Scaling group for the EC2 instances. Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.

Correct Answer: A

Community vote distribution

A (98%)

 **heatblur**  2 years ago

Selected Answer: A

The length of these questions should be a crime....

upvoted 36 times

 **kgpoj** 1 year, 4 months ago

Couldn't agree more.

They can just ask us, hey for DynamoDB's cache, should you use DAX or ElastiCache or Memcached? Is CloudFront Distribution designed for fixing sudden traffic spike?

Then we can just say: 1. DAX; 2. no. :D

upvoted 2 times

 **juanife** 10 months, 2 weeks ago

the thing is (as other people already said as well) AWS is evaluating not only our technical knowledge about its Cloud services but also how we manage to solve technical scenarios while using English language

upvoted 1 times

 **vibzr2023**  1 year, 11 months ago

Option A correct... other options

B. ElastiCache for Redis: While a good caching solution, DAX is specifically optimized for DynamoDB, making it a better choice in this context.

C. ElastiCache for Memcached: Memcached is not as feature-rich as Redis and lacks DAX's DynamoDB integration.

D. CloudFront: While useful for content delivery, it's not the primary solution for handling database load and scaling EC2 instances.

upvoted 9 times

 **AzureDP900**  1 year, 1 month ago

A and D are similar however manually scale up instances can be eliminated easily. A is right

upvoted 1 times

 **asquared16** 1 year, 4 months ago

That felt like reading a eulogy with a gun to my face.

upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

Selected Answer: A

A, for sure.

No need for CF in the case of content updates

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: A

A: Correct. Utilizes DAX for DynamoDB caching, Auto Scaling for EC2, and ALB for traffic distribution; aligns with best practices.

B Incorrect. CloudFront is not optimal for dynamic content load handling; manual scaling is less efficient than scheduled scaling.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: A

Option A

upvoted 1 times

 **shaaam80** 2 years ago

Selected Answer: A

Answer - A. use DAX, in memory cache of DynamoDB.

B is wrong - manually scale up & Autoscaling group as origin for the CF distro

upvoted 3 times

 **salazar35** 2 years, 1 month ago

Selected Answer: A

A - Update issue no need CloudFront here

upvoted 3 times

 **Jonalb** 2 years, 1 month ago

Selected Answer: A

A. Configure o DynamoDB Accelerator (DAX) como cache na memória. Atualize o aplicativo para usar o DAX. Crie um grupo do Auto Scaling para as instâncias do EC2. Crie um平衡ador de carga de aplicativo (ALB). Defina o grupo do Auto Scaling como destino para o ALB. Atualize o registro do Route 53 para usar uma política de roteamento simples que tenha como alvo o alias DNS do ALB. Configure o escalonamento programado para as instâncias do EC2 antes das atualizações de conteúdo.

upvoted 3 times

 **thala** 2 years, 1 month ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/70883-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 3 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Yes, A is correct

upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: A

Answer: A

upvoted 1 times

Question #397

A company needs to store and process image data that will be uploaded from mobile devices using a custom mobile app. Usage peaks between 8 AM and 5 PM on weekdays, with thousands of uploads per minute. The app is rarely used at any other time. A user is notified when image processing is complete.

Which combination of actions should a solutions architect take to ensure image processing can scale to handle the load? (Choose three.)

- A. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon MQ queue.
- B. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon Simple Queue Service (Amazon SQS) standard queue.
- C. Invoke an AWS Lambda function to perform image processing when a message is available in the queue.
- D. Invoke an S3 Batch Operations job to perform image processing when a message is available in the queue.
- E. Send a push notification to the mobile app by using Amazon Simple Notification Service (Amazon SNS) when processing is complete.
- F. Send a push notification to the mobile app by using Amazon Simple Email Service (Amazon SES) when processing is complete.

Correct Answer: BCE*Community vote distribution*

BCE (90%) 10%

 **shaam80**  2 years ago

Selected Answer: BCE

BCE - SQS + Lambda + SNS

upvoted 5 times

 **vibzr2023**  1 year, 11 months ago

BCE... other options incorrect

- A. Amazon MQ: While viable for durable messaging, it's less scalable and cost-effective compared to SQS for this use case.
- D. S3 Batch Operations: Designed for batch processing of large datasets, not real-time processing of individual image uploads.
- F. Amazon SES: Primarily for email delivery, not push notifications to mobile apps.

upvoted 5 times

 **bjexamprep**  1 year, 9 months ago

Selected Answer: BCF

100% vote on SNS over SES, when I see this question.

"A user is notified when image processing is complete", that means the user needs to subscribe the SNS.

Then, there are two ways to achieve this: Create different SNS for each user, or create different subscription for each user on the same SNS and apply filter policy. Apparently, the latter one is better, but it still need a heavy administration overhead which can't be completed manually. Then, another automation piece will be required to maintain the subscription list. Which is not mentioned in any of the answers. Does that sound a good design?

I go with SES, cause it will be much easier to design the solution. I understand SES is not usually for push notification, but I hate complex solutions.

upvoted 2 times

 **asquared16** 1 year, 4 months ago

Don't complicate it for yourself. SES isn't for push notifications.

upvoted 2 times

 **career360guru** 1 year, 11 months ago

Selected Answer: BCE

Option B, C, E

upvoted 1 times

 **yuliaqwerty** 2 years ago

agree BCE

upvoted 2 times

 **GabrielDeBiasi** 2 years ago

Selected Answer: BCE

BCE answer

upvoted 3 times

 **salazar35** 2 years, 1 month ago

Selected Answer: BCE

BCE answer

upvoted 3 times

  **thala** 2 years, 1 month ago**Selected Answer: BCE**

ditto S3

upvoted 3 times

  **devalenzuela86** 2 years, 1 month ago**Selected Answer: BCE**

BCE Answers

upvoted 2 times

  **cypkir** 2 years, 1 month ago**Selected Answer: BCE**

Answer: B C E

upvoted 1 times

Question #398

Topic 1

A company is building an application on AWS. The application sends logs to an Amazon OpenSearch Service cluster for analysis. All data must be stored within a VPC.

Some of the company's developers work from home. Other developers work from three different company office locations. The developers need to access OpenSearch Service to analyze and visualize logs directly from their local development machines.

Which solution will meet these requirements?

- A. Configure and set up an AWS Client VPN endpoint. Associate the Client VPN endpoint with a subnet in the VPC. Configure a Client VPN self-service portal. Instruct the developers to connect by using the client for Client VPN.
- B. Create a transit gateway, and connect it to the VPC. Create an AWS Site-to-Site VPN. Create an attachment to the transit gateway. Instruct the developers to connect by using an OpenVPN client.
- C. Create a transit gateway, and connect it to the VPC. Order an AWS Direct Connect connection. Set up a public VIF on the Direct Connect connection. Associate the public VIF with the transit gateway. Instruct the developers to connect to the Direct Connect connection.
- D. Create and configure a bastion host in a public subnet of the VPC. Configure the bastion host security group to allow SSH access from the company CIDR ranges. Instruct the developers to connect by using SSH.

Correct Answer: A*Community vote distribution*

A (100%)

vibzr2023 Highly Voted 1 year, 11 months ago

A correct: Best choice to use Client VPN

- B. Site-to-Site VPN: Designed for connecting entire networks, not individual devices, and requires VPN hardware/software at each office location.
- C. Direct Connect: Primarily for high-bandwidth, low-latency connections between on-premises networks and AWS, not individual developer access.
- D. Bastion Host: While providing access, it introduces a potential security risk by exposing a public-facing host and requires developers to learn SSH.

upvoted 5 times

AI8282 Most Recent 5 months, 2 weeks ago**Selected Answer: A**

A. They need to access it directly it states. Typically I'd go with D which has centralized logging and other benefits but bast hosts technically are not directly.

upvoted 1 times

AzureDP900 1 year, 1 month ago

A is right, client VPN is best option.

upvoted 1 times

career360guru 1 year, 11 months ago**Selected Answer: A**

Option A

upvoted 3 times

FuriouZ 2 years ago**Selected Answer: A**

A because work from home

upvoted 3 times

dutchy1988 2 years ago

Site-to-Site and Direct Connect eliminates the developers from home to access VPC -> B and C out
D states company CIDR range, so also developers at home are excluded -> D out
A is only valid option. Each developer needs to access environment using point-to-site connection.

upvoted 3 times

shaaam80 2 years ago

Answer A - Client VPN endpoint

upvoted 1 times

Maygam 2 years, 1 month ago

Selected Answer: A

1. <https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/cvpn-working-endpoints.html>
2. <https://docs.aws.amazon.com/vpn/latest/clientvpn-user/self-service-portal.html>

upvoted 3 times

 **thala** 2 years, 1 month ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/69499-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: A

Answer: A

upvoted 3 times

Question #399

A company wants to migrate its website from an on-premises data center onto AWS. At the same time, it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency. The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege.

A solutions architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster.

What steps are required after the deployment to meet the requirements? (Choose two.)

- A. Create tasks using the bridge network mode.
- B. Create tasks using the awsvpc network mode.
- C. Apply security groups to Amazon EC2 instances, and use IAM roles for EC2 instances to access other resources.
- D. Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources.
- E. Apply security groups to the tasks, and use IAM roles for tasks to access other resources.

Correct Answer: BE*Community vote distribution*

BE (100%)

 **SIJUTHOMASP** 1 year ago

Selected Answer: BE

Apply security groups to tasks is right with IAM role. Option D says IAM identity which is working. So, BE.

upvoted 1 times

 **ahmadraufsyahputra** 1 year, 3 months ago

BE , you can apply security group to the task using vpcmode, because in vpcmode the task will use ENI within the VPC and the ENI can use security groups

upvoted 4 times

 **VerRi** 1 year, 3 months ago

Selected Answer: BE

BE for sure

upvoted 1 times

 **career360guru** 1 year, 5 months ago

Selected Answer: BE

Option B and E

upvoted 1 times

 **GabrielDeBiasi** 1 year, 7 months ago

Selected Answer: BE

BE, easy

upvoted 2 times

 **Jonalb** 1 year, 7 months ago

Selected Answer: BE

B. Crie tarefas usando o modo de rede awsvpc.

E. Aplique grupos de segurança às tarefas e use funções do IAM para tarefas para acessar outros recursos.

upvoted 2 times

 **Jonalb** 1 year, 7 months ago

B. Crie tarefas usando o modo de rede awsvpc.

E. Aplique grupos de segurança às tarefas e use funções do IAM para tarefas para acessar outros recursos.

upvoted 2 times

 **thala** 1 year, 7 months ago

Selected Answer: BE<https://www.examtopics.com/discussions/amazon/view/5362-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

 **devalenzuela86** 1 year, 7 months ago

Selected Answer: BE

BE for sure

upvoted 1 times

  **cypkir** 1 year, 7 months ago**Selected Answer: BE**

Answer: B E

upvoted 1 times

Question #400

Topic 1

A company is running a serverless application that consists of several AWS Lambda functions and Amazon DynamoDB tables. The company has created new functionality that requires the Lambda functions to access an Amazon Neptune DB cluster. The Neptune DB cluster is located in three subnets in a VPC.

Which of the possible solutions will allow the Lambda functions to access the Neptune DB cluster and DynamoDB tables? (Choose two.)

- A. Create three public subnets in the Neptune VPC, and route traffic through an internet gateway. Host the Lambda functions in the three new public subnets.
- B. Create three private subnets in the Neptune VPC, and route internet traffic through a NAT gateway. Host the Lambda functions in the three new private subnets.
- C. Host the Lambda functions outside the VPC and update the Neptune security group to allow access from the IP ranges of the Lambda functions.
- D. Host the Lambda functions outside the VPC. Create a VPC endpoint for the Neptune database, and have the Lambda functions access Neptune over the VPC endpoint.
- E. Create three private subnets in the Neptune VPC. Host the Lambda functions in the three new isolated subnets. Create a VPC endpoint for DynamoDB, and route DynamoDB traffic to the VPC endpoint.

Correct Answer: BE

Community vote distribution

BE (94%)	3%
----------	----

 **heatblur** Highly Voted 2 years, 1 month ago

Selected Answer: BE

B and E is the answer. Was really torn about option D....

D involves hosting Lambda functions outside the VPC and creating a VPC endpoint for the Neptune database. The key issue here is that while AWS supports VPC endpoints for several services, as of my last update in April 2023, Amazon Neptune does not support VPC endpoints. Without VPC endpoint support for Neptune, Lambda functions outside the VPC cannot access the Neptune DB cluster in this way.

So it must be B and E !

upvoted 11 times

 **Dgix** Highly Voted 1 year, 9 months ago

Selected Answer: BE

The only thing to remember with this question is that the two alternatives are SEPARATE. They are complete on their own and are not in conjunction.

upvoted 7 times

 **0dc6cac** 6 months ago

OH MY GOD, I've been looking at this question for like an hour trying to figure out why we need both of the points.....and if that's the case, there's nothing stopping A+D from working in conjunction.

It makes sense after reading your comment, THANK YOU! I really need to read questions like this to see if it's a combination of 2 points, or separately.

upvoted 1 times

 **AloraCloud** Most Recent 1 year, 2 months ago

For B:

Why do we need to route internet traffic through a NAT gateway??

upvoted 2 times

 **alexbraila** 1 year ago

To access DynamoDB over public internet

upvoted 2 times

 **djangoUnchained** 1 year, 9 months ago

Selected Answer: AE

For B how will the Lambda access DynamoDB from a Private subnet and without an IGW? Should be A.

upvoted 1 times

 **pangchn** 1 year, 9 months ago

Selected Answer: BE

till March 2024

"its endpoints are only accessible within that VPC"

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

so any answer outside the VPC is wrong

apparently you won't choose A to have it public

upvoted 3 times

 **career360guru** 1 year, 9 months ago

Selected Answer: BE

B and E

upvoted 1 times

 **ayadmawla** 2 years ago

Amazon Neptune only allows connections from clients located in the same VPC as the Neptune cluster. So we have to use a load balancer or proxy inside the vpc to give us access. The following Github article show architectural designs that outline the approach.

<https://aws-samples.github.io/aws-dbs-refarch-graph/src/connecting-using-a-load-balancer/#:~:text=your%20Neptune%20cluster.-,Amazon%20Neptune%20only%20allows%20connections%20from%20clients%20located%20in%20the,via%20an%20Application%20Load%20Balancer>

upvoted 4 times

 **heatblur** 2 years, 1 month ago

Selected Answer: BE

B. Create three private subnets in the Neptune VPC, route internet traffic through a NAT gateway, and host the Lambda functions in the new private subnets.

E. Create three private subnets in the Neptune VPC, host the Lambda functions in these subnets, and create a VPC endpoint for DynamoDB.

upvoted 2 times

 **Jonalb** 2 years, 1 month ago

Selected Answer: BE

opções B e E são as mais viáveis

upvoted 1 times

 **Jonalb** 2 years, 1 month ago

Portanto, as opções B e E são as mais viáveis para permitir que as funções Lambda accessem tanto o cluster de banco de dados Amazon Neptune quanto as tabelas do Amazon DynamoDB.

upvoted 2 times

 **thala** 2 years, 1 month ago

Selected Answer: BE

<https://www.examtopics.com/discussions/amazon/view/81635-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 3 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: DE

Answer DE

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

It's true BE

upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: BE

Answer: B E

upvoted 1 times

Question #401

A company wants to design a disaster recovery (DR) solution for an application that runs in the company's data center. The application writes to an SMB file share and creates a copy on a second file share. Both file shares are in the data center. The application uses two types of files: metadata files and image files.

The company wants to store the copy on AWS. The company needs the ability to use SMB to access the data from either the data center or AWS if a disaster occurs. The copy of the data is rarely accessed but must be available within 5 minutes.

- A. Deploy AWS Outposts with Amazon S3 storage. Configure a Windows Amazon EC2 instance on Outposts as a file server.
- B. Deploy an Amazon FSx File Gateway. Configure an Amazon FSx for Windows File Server Multi-AZ file system that uses SSD storage.
- C. Deploy an Amazon S3 File Gateway. Configure the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and to use S3 Glacier Deep Archive for the image files.
- D. Deploy an Amazon S3 File Gateway. Configure the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and image files.

Correct Answer: D*Community vote distribution*

D (74%)

B (23%)

ayadmaula Highly Voted 2 years ago

Selected Answer: D

Answer is D = S3 File Gateway.
For those that have chosen B, they are right of course as FSx File Gateway will work as well. But if you read the requirements (The company wants to store the copy on AWS. The company needs the ability to use SMB to access the data from either the data center or AWS if a disaster occurs. The copy of the data is rarely accessed but must be available within 5 minutes.) it is only about storing the data with rare access. So why would you choose option B that has a Multi-AZ + SSD over a cheaper option for DR?

upvoted 13 times

ayadmaula 2 years ago

and A is just silly
upvoted 1 times

ayadmaula 2 years ago

and of course C would be wrong because for glacier, it would take more than 5 minutes to get the files out
upvoted 2 times

chelbsik Highly Voted 1 year, 10 months ago

Selected Answer: D

Vote for D:

1. Amazon S3 File Gateway is suitable for SMB file share
<https://docs.aws.amazon.com/filegateway/latest/files3/CreatingAnSMBFileShare.html>
 2. S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. <https://aws.amazon.com/s3/storage-classes/>
- upvoted 7 times

lunt Most Recent 2 weeks ago

Selected Answer: D

Not sure why so much discussion on this.

A = No.

- B. Only makes sense cost wise if HDD was used.
 - C. S3 GDA rules this out. No GIR in use here.
 - D. Only option that makes sense. Key part to understand is that the answer does not specify where the S3 FG will be deployed, the misdirection here is thinking its goes in the DC - FG goes on-site. Easier way to read it: Deploy an Amazon S3 FG 'onsite'. Now I have 2x copies in DC + if DC goes down > direct to AWS via FG.
- upvoted 1 times

redipa 1 month, 3 weeks ago

Selected Answer: B

This is a poorly worded question. I would normally choose D except for this part of the question "The company needs the ability to use SMB to access the data from either the data center or AWS if a disaster occurs." If you use S3 File Gateway it lives on prem and allows the SMB communication. But if a disaster occurs, they won't be able to access the S3 data in AWS using SMB anymore because the File Gateway will be gone. With FSx they would still be able to access the files in AWS using SMB during a disaster.

upvoted 1 times

 **jimee11** 7 months, 1 week ago

Selected Answer: C

"The copy of the data is rarely accessed but must be available within 5 minutes." Data is equivalent to metadata, NOT the images. The images can go cold storage.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option D is correct because it:

Deploys an Amazon S3 File Gateway, which enables SMB access to stored objects in Amazon S3.

Configures the S3 File Gateway to use:

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for both metadata and image files, providing fast access and reducing storage costs.

upvoted 1 times

 **seetpt** 1 year, 7 months ago

Selected Answer: D

D for me

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: B

Option B is right.

upvoted 2 times

 **djangoUnchained** 1 year, 9 months ago

I wouldnt waste tons of money to host data that a rarely accessed on FSx. S3 IA will do just fine.

upvoted 4 times

 **master9** 1 year, 11 months ago

Selected Answer: D

Amazon S3 File Gateway provides a seamless way to connect to the cloud to store application data files and backup images as durable objects in Amazon S3 cloud storage. Amazon S3 File Gateway offers SMB or NFS-based access to data in Amazon S3 with local caching. It can be used for on-premises data-intensive Amazon EC2-based applications that need file protocol access to S3 object storage.

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

upvoted 3 times

 **lanjr01** 1 year, 11 months ago

<https://www.amazonaws.cn/en/storagegateway/faqs/>

With S3 File Gateway, your configured S3 buckets will be available as Network File System (NFS) mount points or Server Message Block (SMB) file shares. Your applications read and write files and directories over NFS or SMB, interfacing to the gateway as a file server. In turn, the gateway translates these file operations into object requests on your S3 buckets.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B. - Requirement states that company needs SMB protocol access to it in case of Disaster in AWS, this is only possible with Fsx Filegateway.

upvoted 3 times

 **CProgrammer** 1 year, 12 months ago

While S3 File Gateway options (C and D) are cost-effective for long-term storage, they introduce retrieval delays that don't meet the 5-minute availability requirement.

upvoted 1 times

 **Help_please** 2 years ago

Selected Answer: B

Answer is B. Although S3 filegateway supports both NFS and SMB, D cannot be the right answer since question does not mention it to be cost efficient.

upvoted 2 times

 **shaaam80** 2 years ago

Selected Answer: D

Answer D - User S3 file GW with S3 Infreq Access for metadata and image files

upvoted 3 times

 **heatblur** 2 years, 1 month ago

Selected Answer: D

Amazon S3 File Gateway supports SMB and can be used to store and retrieve files in Amazon S3 using file-based interfaces. Using S3 Standard-Infrequent Access for both metadata and image files ensures that the data is available within the required 5 minutes while optimizing costs for infrequently accessed data.

upvoted 3 times

✉  **Jonalb** 2 years, 1 month ago

Selected Answer: D

D. Implantar um gateway de arquivos Amazon S3. Configure o S3 File Gateway para usar o Amazon S3 Standard-Infrequent Access (S3 Standard-IA) para os arquivos de metadados e arquivos de imagem.

upvoted 4 times

✉  **devalenzuela86** 2 years, 1 month ago

D is incorrect because deploying an Amazon S3 File Gateway and configuring the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and image files does not provide the ability to use SMB to access the data from either the data center or AWS if a disaster occurs.

upvoted 4 times

✉  **oomwowwww** 2 years, 1 month ago

GPT ? lol

upvoted 1 times

✉  **vibzr2023** 1 year, 11 months ago

D is correct --- option B is incorrect, FSx File Gateway with Multi-AZ SSD: Offers high performance but is more expensive for infrequently accessed data.

upvoted 1 times

✉  **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 3 times

Question #402

A company is creating a solution that can move 400 employees into a remote working environment in the event of an unexpected disaster. The user desktops have a mix of Windows and Linux operating systems. Multiple types of software, such as web browsers and mail clients, are installed on each desktop.

A solutions architect needs to implement a solution that can be integrated with the company's on-premises Active Directory to allow employees to use their existing identity credentials. The solution must provide multifactor authentication (MFA) and must replicate the user experience from the existing desktops.

Which solution will meet these requirements?

- A. Use Amazon WorkSpaces for the cloud desktop service. Set up a VPN connection to the on-premises network. Create an AD Connector, and connect to the on-premises Active Directory. Activate MFA for Amazon WorkSpaces by using the AWS Management Console.
- B. Use Amazon AppStream 2.0 as an application streaming service. Configure Desktop View for the employees. Set up a VPN connection to the on-premises network. Set up Active Directory Federation Services (AD FS) on premises. Connect the VPC network to AD FS through the VPN connection.
- C. Use Amazon WorkSpaces for the cloud desktop service. Set up a VPN connection to the on-premises network. Create an AD Connector, and connect to the on-premises Active Directory. Configure a RADIUS server for MFA.
- D. Use Amazon AppStream 2.0 as an application streaming service. Set up Active Directory Federation Services on premises. Configure MFA to grant users access on AppStream 2.0.

Correct Answer: C

Community vote distribution

C (88%)

9%

 PAUGURU Highly Voted 1 year, 6 months ago

Selected Answer: C

C is the only way to implement MFA. "To enable MFA for AWS services such as Amazon WorkSpaces and QuickSight, a key requirement is an MFA solution that is a Remote Authentication Dial-In User Service (RADIUS) server or a plugin to a RADIUS server already implemented in your on-premises infrastructure." <https://aws.amazon.com/it/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/>

upvoted 19 times

 07c2d2a Highly Voted 1 year, 4 months ago

C. is the answer, but really none of the answers are right. The real flaw here is that they're using an AD connector as a backup. They should be using a managed AD or have an EC2 AD server. If there's an actual disaster, relying on a VPN and a server that might be unreachable well architected.

upvoted 9 times

 JPSWS 1 year, 1 month ago

So true! I was about to write the exact same thing... Disaster can often equals no more Datacenter so no AD to "connect" to for the AD connector.

upvoted 3 times

 ma23 Most Recent 1 year, 5 months ago

Selected Answer: C

Answer C.

<https://aws.amazon.com/workspaces/>

"maximize user experience" is the keyword to decide Option C.

upvoted 1 times

 career360guru 1 year, 5 months ago

Selected Answer: C

Option C

upvoted 1 times

 m1xa 1 year, 6 months ago

Selected Answer: D

A and C are out because these options require implementing a RADIUS server on-premise.

So, B or D.

I would prefer B because it is a more secure solution, but since there is no mention of traffic security, I choose D.

Using SAML2 you can set MFA for users.

<https://docs.aws.amazon.com/appstream2/latest/developerguide/external-identity-providers-further-info.html>

upvoted 1 times

 **siasasia** 1 year, 7 months ago

Selected Answer: C

you enable MFA through RADIUS not AWS Console. so A is out.
there is no AppStream Linux so B and D are out.

upvoted 2 times

 **thotwielder** 1 year, 5 months ago

Amazon AppStream 2.0 Introduces Linux Application Streaming

<https://aws.amazon.com/about-aws/whats-new/2021/11/amazon-appstream-2-0-linux-application-streaming/>

upvoted 1 times

 **geekgirl007** 1 year, 7 months ago

Selected Answer: C

To enable MFA for AWS services such as Amazon WorkSpaces and QuickSight, a key requirement is an MFA solution that is RADIUS
upvoted 2 times

 **Totoroha** 1 year, 7 months ago

why answer is D: <https://aws.amazon.com/appstream2/?p=pm&c=euc&pd=appstream2&z=4>

upvoted 1 times

 **salazar35** 1 year, 7 months ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/>

upvoted 3 times

 **Jonalb** 1 year, 7 months ago

Selected Answer: C

C. Use Amazon WorkSpaces para o serviço de desktop em nuvem. Configure uma conexão VPN com a rede local. Crie um conector AD e conecte-se ao Active Directory local. Configure um servidor RADIUS para MFA.

upvoted 2 times

 **devalenzuela86** 1 year, 7 months ago

incorrect because it requires you to configure a RADIUS server for MFA, which is not required for this solution

upvoted 1 times

 **devalenzuela86** 1 year, 7 months ago

Selected Answer: A

A for sure

upvoted 3 times

Question #403

Topic 1

A company has deployed an Amazon Connect contact center. Contact center agents are reporting large numbers of computer-generated calls. The company is concerned about the cost and productivity effects of these calls. The company wants a solution that will allow agents to flag the call as spam and automatically block the numbers from going to an agent in the future.

What is the MOST operationally efficient solution to meet these requirements?

- A. Customize the Contact Control Panel (CCP) by adding a flag call button that will invoke an AWS Lambda function that calls the UpdateContactAttributes API. Use an Amazon DynamoDB table to store the spam numbers. Modify the contact flows to look for the updated attribute and to use a Lambda function to read and write to the DynamoDB table.
- B. Use a Contact Lens for Amazon Connect rule that will look for spam calls. Use an Amazon DynamoDB table to store the spam numbers. Modify the contact flows to look for the rule and to invoke an AWS Lambda function to read and write to the DynamoDB table.
- C. Use an Amazon DynamoDB table to store the spam numbers. Create a quick connect that the agents can transfer the spam call to from the Contact Control Panel (CCP). Modify the quick connect contact flow to invoke an AWS Lambda function to write to the DynamoDB table.
- D. Modify the initial contact flow to ask for caller input. If the agent does not receive input, the agent should mark the caller as spam. Use an Amazon DynamoDB table to store the spam numbers. Use an AWS Lambda function to read and write to the DynamoDB table.

Correct Answer: A

Community vote distribution

A (89%)	11%
---------	-----

 **ma23** Highly Voted 1 year, 5 months ago

Selected Answer: A

Sorry. It should be Answer A as per AWS URL.
<https://repost.aws/knowledge-center/connect-deny-list-numbers>
 upvoted 6 times

 **dman** Most Recent 1 year, 2 months ago

D, operationally efficient also.
<https://aws.amazon.com/blogs/contact-center/deter-spam-callers-using-amazon-connect/>
 upvoted 2 times

 **ftaws** 1 year, 4 months ago

why not C ?
 upvoted 2 times

 **ma23** 1 year, 5 months ago

Selected Answer: C
 Surely Answer C.
<https://repost.aws/knowledge-center/connect-deny-list-numbers>
 upvoted 1 times

 **shaam80** 1 year, 7 months ago

Selected Answer: A
 Answer A. Create a Lambda function to store spam /denied numbers in the DynamDB table. Create a second Lambda function to check the table against any incoming number and take appropriate action.
<https://repost.aws/knowledge-center/connect-deny-list-numbers>
 upvoted 3 times

 **heatblur** 1 year, 7 months ago

Selected Answer: A
 A is the most operationally efficient solution. It directly empowers agents to flag spam calls with minimal disruption, automates the blocking process via contact flows, and effectively utilizes AWS Lambda and DynamoDB for real-time processing and storage. This approach is both agent-friendly and technically robust, aligning well with the requirements.
 upvoted 3 times

 **Jonalb** 1 year, 7 months ago

Selected Answer: C
 C. Use uma tabela do Amazon DynamoDB para armazenar os números de spam. Crie uma conexão rápida para a qual os agentes possam transferir a chamada de spam a partir do Painel de controle de contato (CCP). Modifique o fluxo de contato de conexão rápida para invocar uma função do AWS Lambda para gravar na tabela do DynamoDB.
 upvoted 1 times

 thala 1 year, 7 months ago

Selected Answer: A

The most operationally efficient solution to allow agents to flag calls as spam and automatically block these numbers from reaching agents in the future in an Amazon Connect contact center involves a combination of Amazon Connect's features, AWS Lambda, and Amazon DynamoDB. Let's evaluate the options:

A. Customize CCP and Use Lambda with DynamoDB:

Customizing the Contact Control Panel (CCP) by adding a 'flag call' button allows agents to easily mark calls as spam.

The button can invoke an AWS Lambda function, which calls the UpdateContactAttributes API to flag the call.

Using an Amazon DynamoDB table to store spam numbers is an effective way to maintain a blocklist.

Modifying contact flows to check for the spam attribute and interact with the DynamoDB table via Lambda ensures that future calls from these numbers are blocked.

This solution provides a seamless experience for agents and integrates efficiently with Amazon Connect and AWS services.

upvoted 4 times

 devalenzuela86 1 year, 7 months ago

Selected Answer: A

Answer A

upvoted 1 times

Question #404

A company has mounted sensors to collect information about environmental parameters such as humidity and light throughout all the company's factories. The company needs to stream and analyze the data in the AWS Cloud in real time. If any of the parameters fall out of acceptable ranges, the factory operations team must receive a notification immediately.

Which solution will meet these requirements?

- A. Stream the data to an Amazon Kinesis Data Firehose delivery stream. Use AWS Step Functions to consume and analyze the data in the Kinesis Data Firehose delivery stream. Use Amazon Simple Notification Service (Amazon SNS) to notify the operations team.
- B. Stream the data to an Amazon Managed Streaming for Apache Kafka (Amazon MSK) cluster. Set up a trigger in Amazon MSK to invoke an AWS Fargate task to analyze the data. Use Amazon Simple Email Service (Amazon SES) to notify the operations team.
- C. Stream the data to an Amazon Kinesis data stream. Create an AWS Lambda function to consume the Kinesis data stream and to analyze the data. Use Amazon Simple Notification Service (Amazon SNS) to notify the operations team.
- D. Stream the data to an Amazon Kinesis Data Analytics application. Use an automatically scaled and containerized service in Amazon Elastic Container Service (Amazon ECS) to consume and analyze the data. Use Amazon Simple Email Service (Amazon SES) to notify the operations team.

Correct Answer: C

Community vote distribution

C (95%)	5%
---------	----

 **874def1** 8 months, 2 weeks ago

Selected Answer: C

stream and analyze the data in the AWS Cloud in real time = Kinesis Data stream.

Note that Kinesis Data firehose is NEAR realtime.

Kinesis Data stream IS REALTIME

Notification = SNS

Notification is NEVER NEVER SES

upvoted 3 times

 **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C.

upvoted 1 times

 **bjexamprep** 1 year, 5 months ago

Selected Answer: B

Near real time analysis needs a long running function, while Lambda can only run about 15mins. So, none of the Lamda function answers should be in the picture.

IOT streaming can be done by Kinesis solution or MSK.

B: Since this is a continuously running analysis, trigger is not required.

D: The answer doesn't mention what solution is used to stream data to Kinesis Data Analytics. And Kinesis Data Analytics itself is a real time analytics tool, which means the ECS is not required.

None of B and D is flawless. I vote B because B has less flaws.

upvoted 1 times

 **pangchn** 1 year, 3 months ago

B is wrong when you see it use SES for notification

upvoted 5 times

 **career360guru** 1 year, 5 months ago

Selected Answer: C

Option C. D is possible but requirement does not state the notification over e-mail.

upvoted 2 times

 **shaaam80** 1 year, 7 months ago

Selected Answer: C

Answer C. Use Kinesis Data streams to ingest data streams in real-time and use a AWS Lambda function to analyze data. Use SNS to send notifications to the factory Operations team.

upvoted 4 times

 **salazar35** 1 year, 7 months ago

Selected Answer: C

C is answer
upvoted 2 times

 **Jonalb** 1 year, 7 months ago

Selected Answer: C

C. Transmite os dados para um fluxo de dados do Amazon Kinesis. Crie uma função AWS Lambda para consumir o fluxo de dados do Kinesis e analisar os dados. Use o Amazon Simple Notification Service (Amazon SNS) para notificar a equipe de operações.

upvoted 1 times

 **thala** 1 year, 7 months ago

Selected Answer: C

Streaming data to an Amazon Kinesis data stream and using an AWS Lambda function for consuming and analyzing the data in real-time is a robust solution.

AWS Lambda can process the data stream efficiently and trigger immediate actions.

Using Amazon SNS for notifications ensures quick and effective communication with the operations team.

This solution is likely to provide the real-time analysis and immediate notification required.

upvoted 3 times

 **devalenzuela86** 1 year, 7 months ago

Selected Answer: C

Answer c

upvoted 1 times

 **cypkir** 1 year, 7 months ago

Selected Answer: C

Answer: C

upvoted 1 times

Question #405

A company is preparing to deploy an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for a workload. The company expects the cluster to support an unpredictable number of stateless pods. Many of the pods will be created during a short time period as the workload automatically scales the number of replicas that the workload uses.

Which solution will MAXIMIZE node resilience?

- A. Use a separate launch template to deploy the EKS control plane into a second cluster that is separate from the workload node groups.
- B. Update the workload node groups. Use a smaller number of node groups and larger instances in the node groups.
- C. Configure the Kubernetes Cluster Autoscaler to ensure that the compute capacity of the workload node groups stays underprovisioned.
- D. Configure the workload to use topology spread constraints that are based on Availability Zone.

Correct Answer: D

Community vote distribution

D (92%)	8%
---------	----

✉  thala  1 year, 7 months ago

Selected Answer: D

Use Topology Spread Constraints Based on Availability Zone
upvoted 11 times

✉  devalenzuela86 1 year, 7 months ago

To maximize node resilience for an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that is expected to support an unpredictable number of stateless pods, the best solution would be to configure the Kubernetes Cluster Autoscaler to ensure that the compute capacity of the workload node groups stays underprovisioned.

upvoted 5 times

✉  HunkyBlinky  1 year, 7 months ago

Selected Answer: D

I guess D, because question requires to MAXIMIZE NODE resilience. Node not workload, so we need to spread nodes across AZs.
upvoted 10 times

✉  Malluchan  3 months, 2 weeks ago

Selected Answer: D

Use topology spread constraints across AZs

This directly improves resilience. By spreading pods evenly across Availability Zones, you reduce the blast radius if one node or even an entire AZ fails. Kubernetes will distribute pods in a way that maintains high availability, and EKS node groups in multiple AZs will ensure that scaling events don't overload a single zone.

upvoted 1 times

✉  career360guru 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

✉  career360guru 1 year, 5 months ago

Selected Answer: D

Option D

upvoted 2 times

✉  MegalodonBolado 1 year, 6 months ago

"To achieve high availability, customers deploy Amazon EKS worker nodes (Amazon EC2 instances) across multiple distinct AZs. To complement this approach, we recommend customers to implement Kubernetes primitives, such as pod topology spread constraints to achieve pod-level high availability as well as efficient resource utilization."

<https://aws.amazon.com/blogs/containers/getting-visibility-into-your-amazon-eks-cross-az-pod-to-pod-network-bytes/>

upvoted 5 times

✉  shaaam80 1 year, 7 months ago

Selected Answer: D

Answer D.

From GPT - This approach ensures that the stateless pods are distributed across different Availability Zones, maximizing node resilience. If a failure occurs in one Availability Zone, the impact on the workload is minimized because other pods are spread across different zones. Makes sense for Node Resilience!

upvoted 2 times

 **heatblur** 1 year, 7 months ago

Selected Answer: D

D is the answer. Configuring the workload to use topology spread constraints based on Availability Zone — is the best solution to maximize node resilience. This approach enhances the stability and availability of the EKS cluster by ensuring that the workload is evenly spread across different Availability Zones, thereby mitigating the risks associated with zone-specific failures or performance issues.

Remember, it's asking about Node Resilience, not Pod Resilience

upvoted 4 times

 **Jonalb** 1 year, 7 months ago

Selected Answer: D

D. Configure a carga de trabalho para usar restrições de propagação de topologia baseadas na zona de disponibilidade.

upvoted 2 times

 **devalenzuela86** 1 year, 7 months ago

To maximize node resilience for an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that is expected to support an unpredictable number of stateless pods, the best solution would be to configure the Kubernetes Cluster Autoscaler to ensure that the compute capacity of the workload node groups stays underprovisioned.

upvoted 1 times

 **devalenzuela86** 1 year, 7 months ago

Selected Answer: C

C for sure

upvoted 3 times

Question #406

Topic 1

A company needs to implement a disaster recovery (DR) plan for a web application. The application runs in a single AWS Region.

The application uses microservices that run in containers. The containers are hosted on AWS Fargate in Amazon Elastic Container Service (Amazon ECS). The application has an Amazon RDS for MySQL DB instance as its data layer and uses Amazon Route 53 for DNS resolution. An Amazon CloudWatch alarm invokes an Amazon EventBridge rule if the application experiences a failure.

A solutions architect must design a DR solution to provide application recovery to a separate Region. The solution must minimize the time that is necessary to recover from a failure.

Which solution will meet these requirements?

- A. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Create an AWS Lambda function to perform the following actions: take a snapshot of the RDS DB instance, copy the snapshot to the separate Region, create a new RDS DB instance from the snapshot, and update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.
- B. Create an AWS Lambda function that creates a second ECS cluster and ECS service in the separate Region. Configure the Lambda function to perform the following actions: take a snapshot of the RDS DB instance, copy the snapshot to the separate Region, create a new RDS DB instance from the snapshot, and update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.
- C. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Create a cross-Region read replica of the RDS DB instance in the separate Region. Create an AWS Lambda function to promote the read replica to the primary database. Configure the Lambda function to update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.
- D. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Take a snapshot of the RDS DB instance. Convert the snapshot to an Amazon DynamoDB global table. Create an AWS Lambda function to update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.

Correct Answer: C

Community vote distribution

C (100%)

 **shaaam80** Highly Voted 2 years ago

Selected Answer: C

Answer C. Configure RDS read-replica instead of Snapshots. Invoke Lambda function to promote read-replica to primary and update Route53 to point to secondary region incase of DR

upvoted 5 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Option C provides a suitable DR solution by:

Setting up a second ECS cluster and ECS service in the separate Region, which allows for containerless deployment of the application.

Creating a cross-Region read replica of the RDS DB instance in the separate Region, ensuring that the data is available in the new Region even if the primary database fails.

Creating an AWS Lambda function to promote the read replica to the primary database, which ensures that both Regions have an up-to-date copy of the data.

Configuring the Lambda function to update Route 53 to route traffic to the second ECS cluster, ensuring seamless failover.

This solution provides several benefits, including:

Rapid application recovery (less than 30 minutes)
High availability and low downtime
Easy disaster recovery with minimal manual intervention

upvoted 2 times

 **gfhbox0083** 1 year, 5 months ago

C, for sure.

It's not straight forward to Convert the RDS MySQL snapshot to an Amazon DynamoDB global table.

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: C

Option C

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: C

Option C

upvoted 1 times

 **_Juwon** 2 years ago

C. read replica

upvoted 2 times

 **GabrielDeBiasi** 2 years ago

Selected Answer: C

Answer c

upvoted 2 times

 **salazar35** 2 years, 1 month ago

Selected Answer: C

The solution must minimize the time that is necessary to recover from a failure

upvoted 2 times

 **thala** 2 years, 1 month ago

Selected Answer: C

Second ECS Cluster and RDS Read Replica with Lambda

upvoted 1 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: C

Answer c

upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: C

Answer: C

upvoted 1 times

Question #407

Topic 1

A company has AWS accounts that are in an organization in AWS Organizations. The company wants to track Amazon EC2 usage as a metric. The company's architecture team must receive a daily alert if the EC2 usage is more than 10% higher than the average EC2 usage from the last 30 days.

Which solution will meet these requirements?

- A. Configure AWS Budgets in the organization's management account. Specify a usage type of EC2 running hours. Specify a daily period. Set the budget amount to be 10% more than the reported average usage for the last 30 days from AWS Cost Explorer. Configure an alert to notify the architecture team if the usage threshold is met
- B. Configure AWS Cost Anomaly Detection in the organization's management account. Configure a monitor type of AWS Service. Apply a filter of Amazon EC2. Configure an alert subscription to notify the architecture team if the usage is 10% more than the average usage for the last 30 days.
- C. Enable AWS Trusted Advisor in the organization's management account. Configure a cost optimization advisory alert to notify the architecture team if the EC2 usage is 10% more than the reported average usage for the last 30 days.
- D. Configure Amazon Detective in the organization's management account. Configure an EC2 usage anomaly alert to notify the architecture team if Detective identifies a usage anomaly of more than 10%.

Correct Answer: A*Community vote distribution*

A (63%)

B (37%)

 **shaaam80**  2 years ago

Selected Answer: A

Answer A. C cannot be correct because Cost Anomaly detection is for a surprise cost exceeds. A is a perfect use case for this scenario.
upvoted 14 times

 **37b2ab7**  2 years ago

Selected Answer: A

"A" describe perfectly the process to create this kind of control. Besides Cost Anomaly is very focused on "Cost", while the question ask to control the "usage" (ex:hours), not exactly \$ cost. I suggest doing a demo. "A" for sure
upvoted 9 times

 **aka1177**  4 weeks ago

Selected Answer: B

C'mon guys B is more logic and right answer. AWS Budgets cannot automatically calculate a rolling 30-day average. Manual setup or a forecast would be required. That is why B is correct - Cost anomaly detection.
upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 3 months, 3 weeks ago

Selected Answer: B

AWS Cost Anomaly Detection automatically analyzes past usage with ML and detects when EC2 usage goes more than ~10% above the 30-day average, then sends alerts. Budgets (A) is static and does not adapt daily, while Trusted Advisor (C) and Detective (D) don't track EC2 usage anomalies.
upvoted 1 times

 **studybuddy12** 6 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/cost-management/latest/userguide/getting-started-ad.html#:~:text=Monitor%20types-,Creating%20your%20cost%20monitors%20and%20alert%20subscriptions,help%20decrease%20false%20positive%20alerts.>
upvoted 1 times

 **CAIAsia** 8 months, 2 weeks ago

Selected Answer: B

A cannot be correct because AWS Budgets requires manual input of the threshold (e.g., 10% above the 30-day average). If the average changes daily, the budget amount would need constant manual updates, making it impractical.
upvoted 4 times

 **eesa** 9 months ago

Selected Answer: B

Option B: Configure AWS Cost Anomaly Detection in the organization's management account. Configure a monitor type of AWS Service. Apply a filter of Amazon EC2. Configure an alert subscription to notify the architecture team if the usage is 10% more than the average

usage for the last 30 days.

✗ Explanation:

The company needs a solution that:

Tracks EC2 usage over time.

Calculates the average usage for the past 30 days.

Alerts the architecture team if usage exceeds 10% of the average.

AWS Cost Anomaly Detection is designed for this exact purpose. It:

Monitors usage and cost metrics at the AWS service level (e.g., EC2).

Uses machine learning to detect anomalies based on historical usage.

Sends alerts when usage exceeds a defined threshold (in this case, 10% more than the last 30-day average).

upvoted 4 times

✉ **Deztroyer88** 9 months, 3 weeks ago

Selected Answer: B

AWS Cost Anomaly Detection is designed to automatically track usage trends and detect anomalies in EC2 usage patterns.

You can set up a monitoring rule to compare daily EC2 usage against a 30-day average.

If usage exceeds 10% over the historical average, it will trigger an alert.

This solution is automated, scalable, and requires minimal operational overhead.

upvoted 1 times

✉ **AloraCloud** 1 year, 2 months ago

AWS Budgets can be used to set custom budget based on your expected usage and notify you when a threshold is exceeded. AWS Cost Anomaly Detection uses advanced machine learning (ML) technologies to identify anomalous spend and root causes.

upvoted 2 times

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

Selected Answer: A

For those who think the correct answer is B:

<https://docs.aws.amazon.com/cost-management/latest/userguide/getting-started-ad.html>

"For Threshold, enter a number to configure the anomalies that you want to generate alerts for. There are two types of thresholds: absolute and percentage. Absolute thresholds trigger alerts when an anomaly's total COST impact exceeds your chosen threshold. Percentage thresholds trigger alerts when an anomaly's total impact percentage exceeds your chosen threshold. Total impact percentage is the percentage difference between the total expected SPEND and total actual SPEND.""

AWS COST Anomaly Detection primarily focuses on COST anomalies rather than specific usage metrics.

upvoted 3 times

✉ **Chakanetsa** 1 year, 4 months ago

Selected Answer: B

Explanation:

AWS Cost Anomaly Detection: This service can monitor your AWS usage and costs, identifying anomalies and deviations from normal usage patterns. By setting up a monitor for Amazon EC2 usage, you can detect if the usage is significantly higher than usual, such as exceeding 10% of the average usage over the past 30 days.

Monitor Type: Choosing "AWS Service" as the monitor type allows you to focus specifically on EC2 usage.

Alert Subscription: You can configure alerts to notify the architecture team when the detected usage anomaly exceeds the threshold, such as a 10% increase over the historical average.

upvoted 2 times

✉ **kgpoj** 1 year, 4 months ago

Selected Answer: A

It has to be A.

I have tried to do it in AWS Budget Console. Here's a step by step breakdown of what I have done:

Step 1: Click on the "Create budget" button and choose the "Usage budget" type

Step 2: Set the Usage type groups as 'EC2 Running hours', Set budget amount's baseline timerange as 'Last 30 days' with a 'daily' period

Step 3: Configure alerts with 110% of budgeted amount

upvoted 3 times

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

I can not reproduce your steps. For usage type group, there are 3 types: fixed/planned/auto-adjusted. both of them are absolute number and don't support percentage setting.

upvoted 1 times

✉ **kgpoj** 1 year, 4 months ago

When setting the time range, even if the label says 'Last 30 days', but if you hover on it, it expands and says 'last-30 day average'

So really now AWS Budget can help us collect daily average using a 30-day sliding window. You can use this as baseline, and use 110% of baseline value to trigger the alert

upvoted 2 times

 **gfhbox0083** 1 year, 5 months ago

A, for sure.

Service Monitor tracks spend across all deployed services, but not for a specific service (like ec2)

upvoted 1 times

 **9f02c8d** 1 year, 6 months ago

It should be D as AWS Cost Anomaly Detection is a service that monitors your cost and usage data to detect anomalies based on machine learning models. It can identify unusual spending patterns and notify you when anomalies are detected based on historical usage patterns

upvoted 1 times

 **9f02c8d** 1 year, 6 months ago

I mean B

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: A

Option A - Maybe I am the problem here, I don't why people are selecting option "B", when the first line in AWS Cost Management documentation Under AWS Budget states - "You can use AWS Budgets to track and take action on your AWS costs and usage. You can use AWS Budgets to monitor your aggregate utilization and coverage metrics for your Reserved Instances (RIs) or Savings Plans."

<https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html>

AWS Blog - <https://aws.amazon.com/blogs/mt/manage-cost-overruns-part-1/>

upvoted 5 times

 **Dgix** 1 year, 9 months ago

Selected Answer: B

It's B. Cost Anomaly detection can do this kind of thing. AWS Budgets is for overall costs and is a less sharp tool here.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: A

Option A - Cost Anomaly detection does not allow to filter based on EC2 type only.

upvoted 5 times

Question #408

Topic 1

An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's CIO has asked a solutions architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during marketing campaigns to process the orders with minimal delays.

Which of the following is the MOST reliable approach to meet the requirements?

- A. Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them.
- B. Receive the orders in an Amazon SQS queue and invoke an AWS Lambda function to process them.
- C. Receive the orders using the AWS Step Functions program and launch an Amazon ECS container to process them.
- D. Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them.

Correct Answer: B*Community vote distribution*

B (84%) C (16%)

✉  **tfl**  2 years ago

Selected Answer: B

Loosely coupled = SQS - Lambda is also the simplest to use
upvoted 7 times

✉  **AWSum1** 1 year, 2 months ago

Yip that key words "loosely coupled" has been repeated several times during the trainings
upvoted 1 times

✉  **career360guru**  1 year, 11 months ago

Selected Answer: B

option B
upvoted 5 times

✉  **AzureDP900**  1 year, 1 month ago

Using an Amazon SQS queue (option B) and an AWS Lambda function is the most reliable approach for several reasons:
Scalability: AWS Lambda can automatically scale based on incoming requests, ensuring that orders are processed quickly even during peak traffic.
High availability: By using a message queue like SQS, orders are stored temporarily until they can be processed, ensuring that no orders are lost due to system failures.
Loosely coupled architecture: The use of an SQS queue and Lambda function decouples the order processing from the storage (Amazon DynamoDB) in a separate logical layer, making it easier to scale and maintain individual components independently.
Handling sporadic traffic patterns: AWS Lambda provides a serverless computing experience that automatically scales based on demand, making it well-suited for handling variable workload spikes.
upvoted 2 times

✉  **career360guru** 1 year, 9 months ago

Selected Answer: B

Option B
upvoted 3 times

✉  **ele** 1 year, 10 months ago

Selected Answer: C

Answer is C
Order processing is a multi-step cycle not a two step one. Stepfunction and ECS is the most reliable way to go.
upvoted 2 times

✉  **yog927** 1 year, 9 months ago

what about loosely coupled? SQS required for it.
upvoted 1 times

✉  **ma23** 1 year, 11 months ago

Selected Answer: B

Option B
upvoted 3 times

✉  **vibzr2023** 1 year, 12 months ago

Selected Answer: B -- SQS for sure coz you can't take a chance of loosing data.

upvoted 2 times

 **MegalodonBolado** 2 years ago

". The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table." We can't assume, without further information, that it's a multistep action. For now, it just processes one order and send info to Dynamo.

Looks reasonable to use SQS+Lambda for a loosely coupled solution

B

upvoted 3 times

 **ayadmawla** 2 years ago

Selected Answer: C

Here is an example of a Step Function for a simple order flow. You can see how many lambda functions will be necessary that can't be replaced by a single SQS and Lambda

<https://dev.to/aws-builders/aws-step-functions-simple-order-flow-6gn>

upvoted 2 times

 **ayadmawla** 2 years ago

Selected Answer: C

Answer is C

Order processing is a multi-step cycle not a two step one.

upvoted 2 times

 **shaaam80** 2 years ago

Selected Answer: B

Answer B

upvoted 2 times

 **salazar35** 2 years ago

Selected Answer: B

B is correct

upvoted 4 times

 **GabrielDeBiasi** 2 years ago

Selected Answer: B

B for sure

upvoted 4 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 3 times

Question #409

Topic 1

A company is deploying AWS Lambda functions that access an Amazon RDS for PostgreSQL database. The company needs to launch the Lambda functions in a QA environment and in a production environment.

The company must not expose credentials within application code and must rotate passwords automatically.

Which solution will meet these requirements?

- A. Store the database credentials for both environments in AWS Systems Manager Parameter Store. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Within the application code of the Lambda functions, pull the credentials from the Parameter Store parameter by using the AWS SDK for Python (Boto3). Add a role to the Lambda functions to provide access to the Parameter Store parameter.
- B. Store the database credentials for both environments in AWS Secrets Manager with distinct key entry for the QA environment and the production environment. Turn on rotation. Provide a reference to the Secrets Manager key as an environment variable for the Lambda functions.
- C. Store the database credentials for both environments in AWS Key Management Service (AWS KMS). Turn on rotation. Provide a reference to the credentials that are stored in AWS KMS as an environment variable for the Lambda functions.
- D. Create separate S3 buckets for the QA environment and the production environment. Turn on server-side encryption with AWS KMS keys (SSE-KMS) for the S3 buckets. Use an object naming pattern that gives each Lambda function's application code the ability to pull the correct credentials for the function's corresponding environment. Grant each Lambda function's execution role access to Amazon S3.

Correct Answer: B

Community vote distribution

B (100%)

 **shaaam80** Highly Voted  2 years ago

Selected Answer: B

Answer B. Always remember - Automatic Password Rotation - AWS Secrets Manager!

upvoted 13 times

 **AzureDP900** Most Recent  1 year, 1 month ago

B is perfect

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: B

Option B

upvoted 1 times

 **SwapnilAWS** 1 year, 11 months ago

Option : B is the correct answer

While AWS Systems Manager Parameter Store is a valid service for storing configuration data, including secrets, using AWS KMS for encryption and Boto3 for retrieval, it lacks the built-in support for automatic rotation of secrets.

AWS KMS is primarily designed for managing cryptographic keys and does not provide built-in support for storing and rotating secrets like database credentials.

While AWS KMS key rotation is available, it is intended for cryptographic key rotation rather than the rotation of sensitive data like passwords.

upvoted 1 times

 **bjexamprep** 1 year, 11 months ago

Selected Answer: B

The correct solution should be:

Store the database credentials for both environments in AWS Secrets Manager with distinct key entry for the QA environment and the production environment. Enable a Lambda function to rotate the secrets regularly. Create a KMS key for each secret and use them to encrypt the credentials. Assign permissions to allow the business Lambda function to retrieve the credential from Secret manager and decrypt the credential with the KMS key.

B is not ideal but is the only acceptable answer:

"Turn on rotation." In Secret Manager, you must enable a Lambda function to rotate the credential

"Provide a reference to the Secrets Manager key as an environment variable for the Lambda functions. " permission must be set to allow the Lambda function to use the Key to decrypt the credential.

upvoted 1 times

 **career360guru** 1 year, 11 months ago

Selected Answer: B

Option B

upvoted 1 times

 **GabrielDeBiasi** 2 years ago

Selected Answer: B

"rotate passwords automatically" -> AWS Secrets Manager

upvoted 3 times

 **thala** 2 years, 1 month ago

Selected Answer: B

AWS Secrets Manager with Rotation Enabled:

upvoted 2 times

 **devalenzuela86** 2 years, 1 month ago

Selected Answer: B

B for sure

upvoted 1 times

 **321swa** 2 years, 1 month ago

Correct Answer is B

upvoted 1 times

 **cypkir** 2 years, 1 month ago

Selected Answer: B

Answer: B

upvoted 1 times

Question #410

Topic 1

A company is using AWS Control Tower to manage AWS accounts in an organization in AWS Organizations. The company has an OU that contains accounts. The company must prevent any new or existing Amazon EC2 instances in the OU's accounts from gaining a public IP address.

Which solution will meet these requirements?

- A. Configure all instances in each account in the OU to use AWS Systems Manager. Use a Systems Manager Automation runbook to prevent public IP addresses from being attached to the instances.
- B. Implement the AWS Control Tower proactive control to check whether instances in the OU's accounts have a public IP address. Set the AssociatePublicIpAddress property to False. Attach the proactive control to the OU.
- C. Create an SCP that prevents the launch of instances that have a public IP address. Additionally, configure the SCP to prevent the attachment of a public IP address to existing instances. Attach the SCP to the OU.
- D. Create an AWS Config custom rule that detects instances that have a public IP address. Configure a remediation action that uses an AWS Lambda function to detach the public IP addresses from the instances.

Correct Answer: C

Community vote distribution

C (68%)

B (32%)

 **TonytheTiger** Highly Voted 1 year, 9 months ago

Selected Answer: C

Option C - From AWS doc page "Don't use AWS Organizations to update service control policies (SCPs) attached to an OU that is registered with AWS Control Tower. Doing so could result in the controls entering an unknown state, which will require you to repair your landing zone or re-register your OU in AWS Control Tower. Instead, you can create new SCPs and attach those to the OUs rather than editing the SCPs that AWS Control Tower has created."

<https://docs.aws.amazon.com/controlltower/latest/userguide/orgs-guidance.html>
upvoted 12 times

 **chelbsik** Highly Voted 1 year, 10 months ago

Selected Answer: B

Voting for B: SCP will cause a state drift, since company already use Control Tower
upvoted 6 times

 **8693a49** 1 year, 4 months ago

Adding a new SCP will not cause drift. Modifying an existing SCP that was created by CT would, which is not the case here.
upvoted 3 times

 **ProcureSense** Most Recent 1 month, 2 weeks ago

Selected Answer: B

Why Option B Is the Best Fit

Proactive controls in AWS Control Tower use CloudFormation hooks to validate resource configurations before deployment. By setting the AssociatePublicIpAddress property to False, you ensure that:

- New EC2 instances cannot be launched with public IPs.
- The control is enforced across all accounts in the OU, maintaining centralized governance.
- Deployment fails if the configuration violates the control, preventing misconfigurations before they occur.

This approach is preventive and scalable, aligning perfectly with the requirement to block public IPs for both new and existing EC2 instances.

upvoted 1 times

 **studybuddy12** 6 months, 3 weeks ago

Selected Answer: C

"Behavior of proactive controls

Proactive controls check resources whenever those resources are created or updated by means of AWS CloudFormation stack operations. Specifically, these proactive controls are implemented as preCreate and preUpdate hook handlers. As a consequence, these controls may not affect requests that are made directly to services through the AWS console, through AWS APIs, or through other means such as AWS SDKs, or other Infrastructure-as-Code (IaC) tools. For more information about when preCreate and preUpdate hooks operate, see AWS CloudFormation hooks."

upvoted 1 times

 **874def1** 8 months, 2 weeks ago

Selected Answer: C

Control Tower's Proactive Control Uses Cloud Formation.

This means AWS CLI, AWS API, AWS console will be able to bypass Proactive controls.

Option C of using new SCP will enforce Public IP restriction effectively.

upvoted 1 times

 **BelloMio** 8 months, 2 weeks ago

Selected Answer: C

Answer is 100% C.

It asks to prevent NEW or EXISTING. It doesn't talk about remediation.

A proactive control is only applied if you deploy with CloudFormation.

If you deploy with the console or through API, the control does not apply.

Answer is C

upvoted 1 times

 **sergza888** 8 months, 3 weeks ago

Selected Answer: C

Unfortunately it is C even though I liked B better "Proactive controls check resources whenever those resources are created or updated by means of AWS CloudFormation stack operations. Specifically, these proactive controls are implemented as preCreate and preUpdate hook handlers. As a consequence, these controls may not affect requests that are made directly to services through the AWS console, through AWS APIs, or through other means such as AWS SDKs, or other Infrastructure-as-Code (IaC) tools."

upvoted 1 times

 **Ob43291** 1 year, 1 month ago

Selected Answer: C

Option C (SCP): Service Control Policies (SCPs) provide a proactive mechanism to prevent non-compliant actions from occurring in the first place. The SCP will block the launch of instances with public IP addresses or the attachment of public IP addresses to existing instances, ensuring that the requirement is met from the outset.

Option B (Control Tower proactive control): Proactive controls in AWS Control Tower are designed to detect and remediate non-compliant resources after they have been created. While they can remediate instances with public IP addresses, they do not prevent the initial assignment of public IP addresses.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Option C is actually a good solution for this scenario.

C is right.

By creating an SCP (Security Policy) that:

Prevents the launch of instances with public IP addresses.

Prevents the attachment of a public IP address to existing instances, you can effectively prevent new or existing Amazon EC2 instances in the OU's accounts from gaining a public IP address.

This solution is suitable because it:

Is proactive and automated, reducing the risk of human error Can detect existing instances with public IP addresses and prevent future assignments Is directly attached to the OU, ensuring that all accounts within it are subject to this policy.

upvoted 2 times

 **sashenka** 1 year, 1 month ago

Selected Answer: C

The company must prevent any new or existing Amazon EC2 instances in the OU's accounts from gaining a public IP address." The key phrase is "from gaining" a public IP address - this means:

It's about preventing future actions of getting public IPs

It's NOT about removing already attached public IPs

It applies to both new and existing instances

In this case, an SCP (Option C) is indeed the correct solution

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: C

"The company MUST PREVENT..."

Proactive controls do not directly prevent the action of attaching a public IP. They are applicable to resources that are specifically PROVISIONED THROUGH AWS SERVICE CATALOG. They do not have the ability to broadly prevent all EC2 instances in an organization from obtaining a public IP, especially those created outside of Service Catalog.

Also, as user VerRi says here in the comments, how will AWS Control Tower proactive control "check whether instances IN the OU's accounts have a public IP address."?

Option C is the best solution because it uses an SCP, which is a preventive control that directly stops the creation or modification of EC2 instances with public IP addresses in all accounts under the specified OU. This ensures compliance with the requirement of preventing public IP addresses on EC2 instances.

upvoted 3 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: C

B. AWS Control Tower's Active Controls primarily focus on security related best practices such as IAM policies, security group rules, etc., rather than directly controlling the public IP addresses of EC2 instances. Although custom proactive control can be created, setting the associatePublicIpAddress property to False is usually done through API calls or CLI/SDK when starting an EC2 instance, rather than

through proactive control in AWS Control Tower.

C. AWS Service Control Policies (SCPs) are a mechanism provided by AWS Organizations for implementing access control to AWS services at the OU level. SCP can restrict the ability to request public IP addresses when launching EC2 instances within OU accounts, as well as limit the permission to modify existing instances to attach public IP addresses. This fully meets the company's needs as it ensures the implementation of a unified strategy at the OU level without the need to manage each account or instance separately.

upvoted 2 times

michele_scar 1 year, 6 months ago

Selected Answer: B

SCP prevent but not remediate existing. So correct is B with CT

upvoted 1 times

teo2157 1 year, 7 months ago

Selected Answer: B

Going for B as Control Tower permissions have to be managed using Controls but not SCPs which causes drifts.

upvoted 2 times

VerRi 1 year, 9 months ago

Selected Answer: C

B is a bit weird because proactive control is used to check NEW resources.

It is weird to say "Check whether instances IN the OU's accounts have a public IP address.".

upvoted 4 times

Dgix 1 year, 9 months ago

Selected Answer: C

C.

B is not correct since Control Tower doesn't have this capability.

upvoted 2 times

career360guru 1 year, 9 months ago

Selected Answer: B

Option B is the right option.

upvoted 2 times

Question #411

Topic 1

A company is deploying a third-party web application on AWS. The application is packaged as a Docker image. The company has deployed the Docker image as an AWS Fargate service in Amazon Elastic Container Service (Amazon ECS). An Application Load Balancer (ALB) directs traffic to the application.

The company needs to give only a specific list of users the ability to access the application from the internet. The company cannot change the application and cannot integrate the application with an identity provider. All users must be authenticated through multi-factor authentication (MFA).

Which solution will meet these requirements?

- A. Create a user pool in Amazon Cognito. Configure the pool for the application. Populate the pool with the required users. Configure the pool to require MFA. Configure a listener rule on the ALB to require authentication through the Amazon Cognito hosted UI.
- B. Configure the users in AWS Identity and Access Management (IAM). Attach a resource policy to the Fargate service to require users to use MFA. Configure a listener rule on the ALB to require authentication through IAM.
- C. Configure the users in AWS Identity and Access Management (IAM). Enable AWS IAM Identity Center (AWS Single Sign-On). Configure resource protection for the ALB. Create a resource protection rule to require users to use MFA.
- D. Create a user pool in AWS Amplify. Configure the pool for the application. Populate the pool with the required users. Configure the pool to require MFA. Configure a listener rule on the ALB to require authentication through the Amplify hosted UI.

Correct Answer: A

Community vote distribution

A (100%)

 **JMAN1** Highly Voted 1 year, 5 months ago

Selected Answer: A

A?

As GPT says,

In this scenario, setting up a user pool in Amazon Cognito allows you to define the specific list of users who can access the application. You can configure the user pool to require multi-factor authentication (MFA), ensuring an additional layer of security for user authentication.

Configuring the ALB listener rule to require authentication through the Amazon Cognito hosted UI means that users attempting to access the application through the ALB will be redirected to the Cognito hosted UI for authentication, where they'll need to provide their credentials and MFA code.

This setup ensures that only authenticated users from the specific user pool with MFA will have access to the application, meeting the requirements without modifying the application itself.

upvoted 9 times

 **thotwielder** Highly Voted 1 year, 5 months ago

web application = Cognito

upvoted 6 times

 **career360guru** Most Recent 1 year, 3 months ago

Selected Answer: A

As application can not be changed to integrate with Identity provider and users needs to be authenticated from internet using Cognito is the only possible solution among the options.

upvoted 4 times

 **duriselvan** 1 year, 4 months ago

A ans <https://repost.aws/knowledge-center/cognito-user-pool-alb-authentication>

upvoted 3 times

 **igor12ghsj577** 1 year, 5 months ago

A sounds OK

upvoted 1 times

 **tmlong18** 1 year, 5 months ago

Selected Answer: A

Answer is A

ALB authentication only integration with:
Cognito

AWS_IAM
Lambda authorizer
upvoted 1 times

 **tmlong18** 1 year, 5 months ago

No, I am wrong.
But answer is still A.

API GW authentication only integration with:
Cognito
AWS_IAM
Lambda authorizer

ALB authentication only integration with:
Cognito
OIDC
upvoted 4 times

 **career360guru** 1 year, 5 months ago

Selected Answer: A

Answer is A
upvoted 1 times

 **Laercio96** 1 year, 5 months ago

Answer is A
upvoted 1 times

 **clevvve** 1 year, 6 months ago

B&C is for accessing aws resources
upvoted 1 times

 **clevvve** 1 year, 6 months ago

Selected Answer: A
Answer is A
upvoted 1 times

Question #412

A solutions architect is preparing to deploy a new security tool into several previously unused AWS Regions. The solutions architect will deploy the tool by using an AWS CloudFormation stack set. The stack set's template contains an IAM role that has a custom name. Upon creation of the stack set, no stack instances are created successfully.

What should the solutions architect do to deploy the stacks successfully?

- A. Enable the new Regions in all relevant accounts. Specify the CAPABILITY_NAMED_IAM capability during the creation of the stack set.
- B. Use the Service Quotas console to request a quota increase for the number of CloudFormation stacks in each new Region in all relevant accounts. Specify the CAPABILITY_IAM capability during the creation of the stack set.
- C. Specify the CAPABILITY_NAMED_IAM capability and the SELF_MANAGED permissions model during the creation of the stack set.
- D. Specify an administration role ARN and the CAPABILITY_IAM capability during the creation of the stack set.

Correct Answer: A

Community vote distribution

A (93%)

7%

 **kejam**  1 year, 10 months ago

Selected Answer: A

Some stack templates might include resources that can affect permissions in your AWS account; for example, by creating new AWS Identity and Access Management (IAM) users. For those stacks, you must explicitly acknowledge this by specifying one of these capabilities.

https://docs.aws.amazon.com/AWSCloudFormation/latest/APIReference/API_CreateStack.html

upvoted 6 times

 **sat2008**  1 year, 10 months ago

Selected Answer: A

Question says "several previously unused AWS Regions" so you have to enable them under the Account first ?
And the CAPABILITY_NAMED_IAM for the custom name

upvoted 5 times

 **AzureDP900**  1 year, 1 month ago

The correct answer is A.

When deploying a CloudFormation stack set to multiple Regions, you need to ensure that the IAM role has sufficient permissions to create stacks in those Regions. The issue here is likely due to a limitation on the number of CloudFormation stacks that can be created in a Region.

To resolve this issue, you should:

Enable the new Regions in all relevant accounts.

Specify the CAPABILITY_NAMED_IAM capability during the creation of the stack set. This allows AWS to create stacks without having to manage IAM roles for each stack instance.

upvoted 2 times

 **career360guru** 1 year, 9 months ago

Selected Answer: A

A seems to be the right choice

upvoted 1 times

 **ele** 1 year, 10 months ago

Selected Answer: C

C is the answer.

The following resources require you to specify CAPABILITY_IAM or CAPABILITY_NAMED_IAM: AWS::IAM::Group, AWS::IAM::InstanceProfile, AWS::IAM::Policy, and AWS::IAM::Role. If the application contains IAM resources with custom names, you must specify CAPABILITY_NAMED_IAM.

With self-managed permissions, you create the AWS Identity and Access Management (IAM) roles required by StackSets to deploy across accounts and AWS Regions.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-prereqs-self-managed.html>

<https://docs.aws.amazon.com/serverlessrepo/latest/devguide/acknowledging-application-capabilities.html>

upvoted 1 times

 **ele** 1 year, 10 months ago

nop, it's A.

By "Enable the new Regions in all relevant accounts." they mean:

Create the necessary IAM service roles in your administrator and target accounts to define the permissions you want.
The A IS CORRECT.

upvoted 2 times

 **HunkBunk** 1 year, 10 months ago

Selected Answer: A
Proper answer is - A

We want to create Cloudformation stack that contains IAM role with custom name - so we need to set CAPABILITY_NAMED_IAM
upvoted 1 times

 **alexis123456** 1 year, 10 months ago

Correct A
upvoted 3 times

Question #413

A company has an application that uses an Amazon Aurora PostgreSQL DB cluster for the application's database. The DB cluster contains one small primary instance and three larger replica instances. The application runs on an AWS Lambda function. The application makes many short-lived connections to the database's replica instances to perform read-only operations.

During periods of high traffic, the application becomes unreliable and the database reports that too many connections are being established. The frequency of high-traffic periods is unpredictable.

Which solution will improve the reliability of the application?

- A. Use Amazon RDS Proxy to create a proxy for the DB cluster. Configure a read-only endpoint for the proxy. Update the Lambda function to connect to the proxy endpoint.
- B. Increase the max_connections setting on the DB cluster's parameter group. Reboot all the instances in the DB cluster. Update the Lambda function to connect to the DB cluster endpoint.
- C. Configure instance scaling for the DB cluster to occur when the DatabaseConnections metric is close to the max connections setting. Update the Lambda function to connect to the Aurora reader endpoint.
- D. Use Amazon RDS Proxy to create a proxy for the DB cluster. Configure a read-only endpoint for the Aurora Data API on the proxy. Update the Lambda function to connect to the proxy endpoint.

Correct Answer: A*Community vote distribution*

A (100%)

 **kejam** Highly Voted 1 year, 10 months ago

Selected Answer: A

lambda -> rds-proxy -> aurora replica(s) read-only endpoint

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>
<https://aws.amazon.com/about-aws/whats-new/2021/03/amazon-rds-proxy-adds-read-only-endpoints-for-amazon-aurora-replicas/>

RDS Data API is used with Aurora Serverless

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/data-api.html#data-api.limitations>

upvoted 16 times

 **0b43291** Most Recent 1 year, 1 month ago

Selected Answer: A

The other options have limitations or do not address the root cause of the issue:

Option B (Increasing max_connections): While increasing the maximum number of connections allowed on the DB cluster may provide a temporary solution, it does not address the underlying issue of inefficient connection management, and it may lead to increased resource consumption and potential performance degradation.

Option C (Instance scaling): While instance scaling can help increase the overall capacity of the DB cluster, it does not directly address the issue of too many connections being established. Additionally, it may not be effective if the high-traffic periods are unpredictable and short-lived.

Option D (RDS Proxy with Aurora Data API): The Aurora Data API is designed for serverless applications to interact with Aurora Serverless databases using a web services model, not for traditional database connections. It does not address the issue of connection management for the existing application architecture.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Option A allows the application to connect to the replica instances without directly accessing them. This approach helps to:

- 1) Reduce the number of connections to the primary instance
- 2) Increase performance by offloading read operations to the replica instances
- 3) Improve reliability by reducing the load on the primary instance during periods of high traffic

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: A

Option A

upvoted 1 times

 **duriselvan** 1 year, 10 months ago

A is ans lambda -> rds-proxy -> aurora replica(s) read-only endpoint

upvoted 2 times

 **master9** 1 year, 10 months ago

Selected Answer: A

rds-proxy

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

correct Answer is A

upvoted 4 times

Question #414

Topic 1

A retail company is mounting IoT sensors in all of its stores worldwide. During the manufacturing of each sensor, the company's private certificate authority (CA) issues an X.509 certificate that contains a unique serial number. The company then deploys each certificate to its respective sensor.

A solutions architect needs to give the sensors the ability to send data to AWS after they are installed. Sensors must not be able to send data to AWS until they are installed.

Which solution will meet these requirements?

- A. Create an AWS Lambda function that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Add the Lambda function as a pre-provisioning hook. During manufacturing, call the RegisterThing API operation and specify the template and parameters.
- B. Create an AWS Step Functions state machine that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Specify the Step Functions state machine to validate parameters. Call the StartThingRegistrationTask API operation during installation.
- C. Create an AWS Lambda function that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Add the Lambda function as a pre-provisioning hook. Register the CA with AWS IoT Core, specify the provisioning template, and set the allow-auto-registration parameter.
- D. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Include parameter validation in the template. Provision a claim certificate and a private key for each device that uses the CA. Grant AWS IoT Core service permissions to update AWS IoT things during provisioning.

Correct Answer: C

Community vote distribution

C (77%) D (15%) 8%

 **kejam** Highly Voted 1 year, 10 months ago

Selected Answer: C

In addition to validating the bootstrap certificate presented by devices, Fleet Provisioning also provides Lambda-based provisioning hooks that enable appropriate validation for pertinent device attributes. Examples of device attributes could include a serial number ...

<https://aws.amazon.com/blogs/iot/how-to-automate-onboarding-of-iot-devices-to-aws-iot-core-at-scale-with-fleet-provisioning/>
upvoted 8 times

 **TomTom** Most Recent 1 year, 1 month ago

Selected Answer: A

Option A, meet the requirements. Why Not C, because C mentioned as Auto Provisioning, while the requirements is to have control.
upvoted 1 times

 **titi_r** 1 year, 8 months ago

Selected Answer: C

Correct ans - C.
upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: C

Option C
upvoted 1 times

 **duriselvan** 1 year, 10 months ago

<https://docs.aws.amazon.com/iot/latest/developerguide/iot-provision.html>
upvoted 1 times

 **duriselvan** 1 year, 10 months ago

AWS provides several different ways to provision a device and install unique client certificates on it. This section describes each way and how to select the best one for your IoT solution. These options are described in detail in the whitepaper titled Device Manufacturing and Provisioning with X.509 Certificates in AWS IoT Core.

upvoted 1 times

 **duriselvan** 1 year, 10 months ago

cANSGiven the requirements, Option C is the most suitable solution:

It combines serial number validation using a Lambda function.

The pre-provisioning hook ensures validation before registration.

The allow-auto-registration parameter provides fine-grained control over auto-registration.

upvoted 3 times

 **ele** 1 year, 10 months ago

Selected Answer: D

Devices can be manufactured with a provisioning claim certificate and private key (which are special purpose credentials) embedded in them. If these certificates are registered with AWS IoT, the service can exchange them for unique device certificates that the device can use for regular operations

<https://docs.aws.amazon.com/iot/latest/developerguide/provision-wo-cert.html#claim-based>

upvoted 2 times

 **duriselvan** 1 year, 10 months ago

C is ans

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is D

upvoted 2 times

Question #415

Topic 1

A startup company recently migrated a large ecommerce website to AWS. The website has experienced a 70% increase in sales. Software engineers are using a private GitHub repository to manage code. The DevOps team is using Jenkins for builds and unit testing. The engineers need to receive notifications for bad builds and zero downtime during deployments. The engineers also need to ensure any changes to production are seamless for users and can be rolled back in the event of a major issue.

The software engineers have decided to use AWS CodePipeline to manage their build and deployment process.

Which solution will meet these requirements?

- A. Use GitHub websockets to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.
- B. Use GitHub webhooks to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.
- C. Use GitHub websockets to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.
- D. Use GitHub webhooks to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.

Correct Answer: B*Community vote distribution*

B (100%)

  **kejam** Highly Voted 1 year, 10 months ago**Selected Answer: B**

They use Jenkins. X-Ray is for debugging not unit testing. Seamless deploys and rollbacks mean blue/green deployments. That leaves Answer B:

<https://aws.amazon.com/blogs/devops/setting-up-a-ci-cd-pipeline-by-integrating-jenkins-with-aws-codebuild-and-aws-codedeploy/>
upvoted 5 times

  **AzureDP900** Most Recent 1 year, 1 month ago

The correct answer is B.

This solution meets the requirements:

Receive notifications for bad builds: Using GitHub webhooks to trigger the CodePipeline pipeline ensures that build failures are detected and notified via Amazon SNS topic.

Zero downtime during deployments: Using a blue/green deployment with AWS CodeDeploy allows for zero downtime deployments, as changes are made to the new environment while the old one remains available.

Seamless rollbacks in case of major issues: The blue/green deployment architecture enables seamless rollbacks by simply switching traffic back to the previous version.

upvoted 2 times

  **career360guru** 1 year, 9 months ago**Selected Answer: B**

Option B

upvoted 1 times

  **ele** 1 year, 10 months ago**Selected Answer: B**

B, no-brainer

upvoted 1 times

  **aabdilmouna** 1 year, 10 months ago**Selected Answer: B**

Answer is B

upvoted 1 times

  **master9** 1 year, 10 months ago**Selected Answer: B**

AWS CodeBuild can be used to conduct unit testing. CodeBuild is a managed service that compiles your source code, runs tests, and produces deployable application artifacts. You can create reports in CodeBuild that contain details about tests that are run during builds. These tests can include unit tests, configuration tests, and functional tests

upvoted 2 times

 **onlyvimal2103** 1 year, 10 months ago

Correct Answer B

<https://aws.amazon.com/about-aws/whats-new/2018/05/aws-codepipeline-supports-push-events-from-github-via-webhooks/>

<https://docs.aws.amazon.com/codebuild/latest/userguide/jenkins-plugin.html>

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is C

upvoted 1 times

Question #416

A software as a service (SaaS) company has developed a multi-tenant environment. The company uses Amazon DynamoDB tables that the tenants share for the storage layer. The company uses AWS Lambda functions for the application services.

The company wants to offer a tiered subscription model that is based on resource consumption by each tenant. Each tenant is identified by a unique tenant ID that is sent as part of each request to the Lambda functions. The company has created an AWS Cost and Usage Report (AWS CUR) in an AWS account. The company wants to allocate the DynamoDB costs to each tenant to match that tenant's resource consumption.

Which solution will provide a granular view of the DynamoDB cost for each tenant with the LEAST operational effort?

- A. Associate a new tag that is named tenant ID with each table in DynamoDB. Activate the tag as a cost allocation tag in the AWS Billing and Cost Management console. Deploy new Lambda function code to log the tenant ID in Amazon CloudWatch Logs. Use the AWS CUR to separate DynamoDB consumption cost for each tenant ID.
- B. Configure the Lambda functions to log the tenant ID and the number of RCU and WCU consumed from DynamoDB for each transaction to Amazon CloudWatch Logs. Deploy another Lambda function to calculate the tenant costs by using the logged capacity units and the overall DynamoDB cost from the AWS Cost Explorer API. Create an Amazon EventBridge rule to invoke the calculation Lambda function on a schedule.
- C. Create a new partition key that associates DynamoDB items with individual tenants. Deploy a Lambda function to populate the new column as part of each transaction. Deploy another Lambda function to calculate the tenant costs by using Amazon Athena to calculate the number of tenant items from DynamoDB and the overall DynamoDB cost from the AWS CUR. Create an Amazon EventBridge rule to invoke the calculation Lambda function on a schedule.
- D. Deploy a Lambda function to log the tenant ID, the size of each response, and the duration of the transaction call as custom metrics to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the custom metrics for each tenant. Use AWS Pricing Calculator to obtain the overall DynamoDB costs and to calculate the tenant costs.

Correct Answer: B

Community vote distribution

B (79%)

A (21%)

 **kejam**  1 year, 10 months ago

Selected Answer: B

Answer B: LEAST operational effort and fine grained approach.
<https://aws.amazon.com/blogs/apn/optimizing-cost-per-tenant-visibility-in-saas-solutions/>

RCU and WCU metrics are already logged in CloudWatch.
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/metrics-dimensions.html>
 upvoted 6 times

 **zbarbaross**  2 weeks, 2 days ago

Selected Answer: A

A is the answer :
 for D- GuardDuty alerts after threats—it does not prevent deletion or modification.
 No mention of object lock, versioning, or backup/replication.
 An attacker with sufficient credentials could still erase evidence and data.
 upvoted 1 times

 **TomTom** 1 year ago

Selected Answer: A

Option A is the preferred solution for providing a granular view of DynamoDB costs for each tenant with the least operational effort.

Advantages of Option A:

- * Utilizes AWS's built-in tagging capabilities for cost allocation, which is straightforward to implement and maintain.
- * Provides detailed cost reports in AWS Cost Explorer without requiring additional custom code or complex calculations.

Disadvantages of Option B:

While it offers precise tracking of resource consumption, it significantly increases operational complexity and maintenance requirements.

Thus, for a balance of granularity and minimal operational effort, Option A is the optimal choice.

upvoted 2 times

 **altonh** 10 months, 1 week ago

Tenants do not have their own tables. They share tables.

upvoted 2 times

 **Chicote** 1 year, 2 months ago

Selected Answer: B

es B, seguro

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: B

Option B

upvoted 1 times

 **zzyy** 1 year, 10 months ago

Selected Answer: B

Answer B

upvoted 1 times

 **aabdilmouna** 1 year, 10 months ago

Selected Answer: B

Answer is B

upvoted 1 times

 **07c2d2a** 1 year, 10 months ago

AWS Cost Explorer API vs cost calculator is really all you need to consider here.

upvoted 4 times

 **07c2d2a** 1 year, 10 months ago

API can automate it, cost calculator is a manual process and never ideal for something like this.

upvoted 2 times

 **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: B

Answer is B

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is A

upvoted 1 times

Question #417

A company has an application that stores data in a single Amazon S3 bucket. The company must keep all data for 1 year. The company's security team is concerned that an attacker could gain access to the AWS account through leaked long-term credentials.

Which solution will ensure that existing and future objects in the S3 bucket are protected?

- A. Create a new AWS account that is accessible only to the security team through an assumed role. Create an S3 bucket in the new account. Enable S3 Versioning and S3 Object Lock. Configure a default retention period of 1 year. Set up replication from the existing S3 bucket to the new S3 bucket. Create an S3 Batch Replication job to copy all existing data.
- B. Use the s3-bucket-versioning-enabled AWS Config managed rule. Configure an automatic remediation action that uses an AWS Lambda function to enable S3 Versioning and MFA Delete on noncompliant resources. Add an S3 Lifecycle rule to delete objects after 1 year.
- C. Explicitly deny bucket creation from all users and roles except for an AWS Service Catalog launch constraint role. Define a Service Catalog product for the creation of the S3 bucket to force S3 Versioning and MFA Delete to be enabled. Authorize users to launch the product when they need to create an S3 bucket.
- D. Enable Amazon GuardDuty with the S3 protection feature for the account and the AWS Region. Add an S3 Lifecycle rule to delete objects after 1 year.

Correct Answer: A*Community vote distribution*

A (71%)	D (25%)	4%
---------	---------	----

 **nharaz**  1 year, 10 months ago

Selected Answer: A

S3 Object Lock - prevents objects from being deleted or overwritten for a fixed amount of time or indefinitely, adding a layer of protection against malicious or accidental deletion.

Replication - to a new account limits the risk of a single point of compromise; even if attackers gain access to the original account, they cannot alter or delete the locked objects in the replicated bucket.

Versioning - keeps multiple versions of an object in an S3 bucket, providing additional security and recovery options.

upvoted 9 times

 **career360guru**  1 year, 9 months ago

Selected Answer: D

Option D is the only option that addresses security risk. Option A is not addressing this - Replicating existing bucket to another bucket does not eliminate the risk due to original bucket credential leak.

upvoted 5 times

 **zbarbaross**  2 weeks, 2 days ago

Selected Answer: A

A is the answer :

for D- GuardDuty alerts after threats—it does not prevent deletion or modification.

No mention of object lock, versioning, or backup/replication.

An attacker with sufficient credentials could still erase evidence and data.

upvoted 1 times

 **BelloMio** 8 months, 2 weeks ago

Selected Answer: B

I will go with B. As option A does not protect the original bucket

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: A

Option A, the company can effectively isolate sensitive data in a separate, secure account with strict access controls, while ensuring that both existing and future data are protected against unauthorized access, deletion, or modification, even if the original account's credentials are compromised.

The other options do not provide the same level of protection or have limitations:

Option B relies on AWS Config and automatic remediation, which may not be effective if the attacker gains access to the account and disables or modifies these configurations.

Option C focuses on controlling bucket creation but does not address the protection of existing data or objects in the current bucket.

Option D relies on Amazon GuardDuty, which is a threat detection service and does not provide the same level of data protection as S3 Versioning and Object Lock.

upvoted 3 times

 **AzureDP900** 1 year, 1 month ago

The correct answer to this question is Option C. Explicitly denying bucket creation from all users and roles except for an AWS Service Catalog launch constraint role, defining a Service Catalog product for the creation of the S3 bucket, and forcing S3 Versioning and MFA Delete ensures that existing and future objects in the S3 bucket are protected. This option provides explicit access controls for S3 bucket creation and forces S3 versioning and MFA Delete on noncompliant resources, making it the most suitable solution to address the security concerns of the company. Option A is not the best choice because creating a new AWS account can introduce complexity and create a single point of failure. While Options B and D offer some benefits, they do not provide explicit access controls for S3 bucket creation, which is essential for protecting sensitive data.

upvoted 1 times

 **AloraCloud** 1 year, 1 month ago

Eliminate C & D

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: A

A

assume role to provide short-term credential

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: A

Option A: Amazon S3 now allows you to enable S3 Object Lock for existing buckets with just a few clicks and to enable S3 Replication for buckets using S3 Object Lock

<https://aws.amazon.com/about-aws/whats-new/2023/11/amazon-s3-enabling-object-lock-buckets/#:~:text=To%20lock%20existing%20objects%2C%20you,of%20objects%20at%20a%20time.>

upvoted 2 times

 **Dgix** 1 year, 9 months ago

Selected Answer: A

The question is, as so often, misleading. None of the alternatives deal with _access_, only with modification.

upvoted 2 times

 **bjexamprep** 1 year, 10 months ago

The question is looking for solution for "concerned that an attacker could gain access to the AWS account through leaked long-term credentials".

None of the answer is addressing the concern of "Access" Through "leaked long-term credentials".

The is question doesn't mention anything about data loss concerns, while, all the answers are providing protection for deleting the data.

upvoted 2 times

 **9f02c8d** 1 year, 7 months ago

creating new account accessed by security team members is action taken to avoid the risk through leaked long-term credentials of existing account so Option A

upvoted 1 times

 **Daniel76** 1 year, 3 months ago

Attacker can just take the data and leave it intact. The damage is done.

upvoted 1 times

 **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: D

Answer is D. It's the only one that specifically addresses the issue. The question never said only the security team needs access.

upvoted 2 times

 **07c2d2a** 1 year, 10 months ago

The answer is a. It's the only one that prevents the data from being deleted by attackers that get access using long term credential. GuardDuty is a monitoring system. By itself, it doesn't actually stop anything from happening. It also likely wouldn't catch use of existing long-term credentials as malicious.

upvoted 1 times

 **nharaz** 1 year, 10 months ago

Enabling GuardDuty with S3 protection and adding a lifecycle rule to delete objects after 1 year focuses on monitoring for threats and managing object lifecycle but:

Does not prevent the deletion or alteration of objects by an attacker who has gained access.

S3 protection in GuardDuty helps identify suspicious access patterns but after-the-fact rather than preventing unauthorized changes.

upvoted 1 times

 **kejam** 1 year, 10 months ago

Selected Answer: A

<https://repost.aws/knowledge-center/s3-cross-account-replication-object-lock>

upvoted 2 times

 **duriselvan** 1 year, 10 months ago

A ans :

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html>

upvoted 3 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is A

upvoted 1 times

Question #418

Topic 1

A company needs to improve the security of its web-based application on AWS. The application uses Amazon CloudFront with two custom origins. The first custom origin routes requests to an Amazon API Gateway HTTP API. The second custom origin routes traffic to an Application Load Balancer (ALB). The application integrates with an OpenID Connect (OIDC) identity provider (IdP) for user management.

A security audit shows that a JSON Web Token (JWT) authorizer provides access to the API. The security audit also shows that the ALB accepts requests from unauthenticated users.

A solutions architect must design a solution to ensure that all backend services respond to only authenticated users.

Which solution will meet this requirement?

- A. Configure the ALB to enforce authentication and authorization by integrating the ALB with the IdP. Allow only authenticated users to access the backend services.
- B. Modify the CloudFront configuration to use signed URLs. Implement a permissive signing policy that allows any request to access the backend services.
- C. Create an AWS WAF web ACL that filters out unauthenticated requests at the ALB level. Allow only authenticated traffic to reach the backend services.
- D. Enable AWS CloudTrail to log all requests that come to the ALB. Create an AWS Lambda function to analyze the logs and block any requests that come from unauthenticated users.

Correct Answer: A

Community vote distribution

A (100%)

 **kejam** Highly Voted 1 year, 10 months ago

Selected Answer: A

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>
upvoted 10 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Option A is right, this solution meets the requirement of ensuring that all backend services respond to only authenticated users:
1) Authentication at the load balancer level: By configuring the ALB to integrate with the OIDC IdP, you can enforce authentication and authorization for incoming requests.
2) Preventing unauthenticated requests: The ALB will reject any requests from unauthenticated users, ensuring that only authenticated users can access the backend services.
upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: A

Option A
upvoted 1 times

 **a54b16f** 1 year, 10 months ago

Selected Answer: A

A is right
upvoted 2 times

 **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: A

Answer is A
upvoted 2 times

 **alexis123456** 1 year, 10 months ago

correct Answer is A
upvoted 3 times

Question #419

Topic 1

A company creates an AWS Control Tower landing zone to manage and govern a multi-account AWS environment. The company's security team will deploy preventive controls and detective controls to monitor AWS services across all the accounts. The security team needs a centralized view of the security state of all the accounts.

Which solution will meet these requirements?

- A. From the AWS Control Tower management account, use AWS CloudFormation StackSets to deploy an AWS Config conformance pack to all accounts in the organization.
- B. Enable Amazon Detective for the organization in AWS Organizations. Designate one AWS account as the delegated administrator for Detective.
- C. From the AWS Control Tower management account, deploy an AWS CloudFormation stack set that uses the automatic deployment option to enable Amazon Detective for the organization.
- D. Enable AWS Security Hub for the organization in AWS Organizations. Designate one AWS account as the delegated administrator for Security Hub.

Correct Answer: D

Community vote distribution

D (100%)

 **AzureDP900** 1 year, 1 month ago

option D meets the requirements of providing a centralized view of the security state of all accounts:
Centralized view: AWS Security Hub provides a unified view of security findings across multiple AWS services and accounts, making it easy to monitor the security posture of your organization.

Delegated administration: By designating one account as the delegated administrator for Security Hub, you can centralize the management of Security Hub across all accounts in the organization.

Integration with AWS Organizations: Enabling Security Hub at the organization level allows you to see the security findings from all member accounts in a single view.

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: D

Option D: Enable AWS Security Hub and use Central Configuration for multiple AWS account and delegated Sec Hub Admin. "Central configuration is a Security Hub feature that helps you set up and manage Security Hub across multiple AWS accounts and AWS Regions & From the delegated Security Hub administrator account, you can specify how the Security Hub service, security standards, and security controls are configured in your organization accounts and organizational units (OUs) across Regions"

- (1) <https://docs.aws.amazon.com/securityhub/latest/userguide/central-configuration-intro.html>
- (2) <https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-setup-prereqs.html>

upvoted 2 times

 **career360guru** 1 year, 9 months ago

Selected Answer: D

Option D

upvoted 1 times

 **a54b16f** 1 year, 10 months ago

Selected Answer: D

centralized view == security hub

upvoted 3 times

 **adelyn|||||||** 1 year, 10 months ago

D

<https://aws.amazon.com/blogs/mt/centralized-dashboard-for-aws-config-and-aws-security-hub/>

upvoted 2 times

 **onlyimal2103** 1 year, 10 months ago

Correct Answer A

<https://aws.amazon.com/blogs/mt/extend-aws-control-tower-governance-using-aws-config-conformance-packs/>

upvoted 1 times

 **kejam** 1 year, 10 months ago

Selected Answer: D

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

upvoted 3 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is D

upvoted 3 times

Question #420

Topic 1

A company that develops consumer electronics with offices in Europe and Asia has 60 TB of software images stored on premises in Europe. The company wants to transfer the images to an Amazon S3 bucket in the ap-northeast-1 Region. New software images are created daily and must be encrypted in transit. The company needs a solution that does not require custom development to automatically transfer all existing and new software images to Amazon S3.

What is the next step in the transfer process?

- A. Deploy an AWS DataSync agent and configure a task to transfer the images to the S3 bucket.
- B. Configure Amazon Kinesis Data Firehose to transfer the images using S3 Transfer Acceleration.
- C. Use an AWS Snowball device to transfer the images with the S3 bucket as the target.
- D. Transfer the images over a Site-to-Site VPN connection using the S3 API with multipart upload.

Correct Answer: A

Community vote distribution

A (100%)

 **kejam** Highly Voted 1 year, 10 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/storage/synchronizing-your-data-to-amazon-s3-using-aws-datasync/>
upvoted 9 times

 **nharaz** Highly Voted 1 year, 10 months ago

Selected Answer: A

AWS DataSync - is a managed data transfer service that simplifies, automates, and accelerates moving data between on-premises storage systems and AWS storage services, as well as between AWS storage services. It supports encryption in transit and can be configured to transfer data to Amazon S3 automatically, handling both existing and new files efficiently. DataSync can be set up without requiring any custom development, making it a strong fit for the company's requirements. However Snowball it is not suited for the ongoing daily transfer of new software images due to the physical shipment of the device involved.

upvoted 5 times

 **AI8282** Most Recent 5 months ago

Selected Answer: A

A. S3 supports HTTPS endpoints negating the need for D. C wont handle the new files and B requires customization which they don't want.
upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option A is right

Easy to use: DataSync makes it easy to transfer large datasets from on-premises locations to Amazon S3 without requiring custom development.

High-speed data transfer: DataSync can achieve speeds of up to 10 Gbps, which is much faster than other methods like S3 API with multipart upload (which was my initial answer).

Efficient data transfer: DataSync is designed for large-scale data transfers and can handle many concurrent transfers, making it an ideal solution for this scenario.

Low maintenance: Once configured, DataSync requires minimal maintenance, which aligns well with the company's need to not require custom development.

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: A

Option A: Additional info on AWS DataSync and S3 transfer

<https://aws.amazon.com/blogs/storage/migrating-hundreds-of-tb-of-data-to-amazon-s3-with-aws-datasync/>
upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: A

Option A. Option D is feasible but this needs custom development that company does not want to do.

upvoted 1 times

 **a54b16f** 1 year, 10 months ago

Selected Answer: A

Easy to pick A as the answer, since all others are invalid. Though, the images are in on premise, the solution should at least mention VPN or direct connect.

upvoted 2 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is A

upvoted 1 times

Question #421

Topic 1

A company has a web application that uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. A recent marketing campaign has increased demand. Monitoring software reports that many requests have significantly longer response times than before the marketing campaign.

A solutions architect enabled Amazon CloudWatch Logs for API Gateway and noticed that errors are occurring on 20% of the requests. In CloudWatch, the Lambda function Throttles metric represents 1% of the requests and the Errors metric represents 10% of the requests. Application logs indicate that, when errors occur, there is a call to DynamoDB.

What change should the solutions architect make to improve the current response times as the web application becomes more popular?

- A. Increase the concurrency limit of the Lambda function.
- B. Implement DynamoDB auto scaling on the table.
- C. Increase the API Gateway throttle limit.
- D. Re-create the DynamoDB table with a better-partitioned primary index.

Correct Answer: B

Community vote distribution

B (100%)

 **AI8282** 5 months ago

Selected Answer: B

Remember DynamoDB has provisioned capacity and autoscaling is still useful for that, even if on demand automatically scales up and down for you.

upvoted 1 times

 **juanife** 10 months, 2 weeks ago

Selected Answer: B

without any doubt it's b, since the error is related to calls against dynamodb when traffic spike occurs

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option B is right. Auto scaling for DynamoDB can help ensure that your table is always provisioned with enough capacity to handle incoming requests, which in turn can help prevent throttle limit exceeds. By automatically adjusting the provisioned capacity of your table based on actual usage patterns, you can maintain optimal performance and responsiveness, even during periods of high traffic or demand.

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: B

Option B

upvoted 1 times

 **HunkBunk** 1 year, 10 months ago

Selected Answer: B

Answer is B

upvoted 2 times

 **kejam** 1 year, 10 months ago

Selected Answer: B

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

upvoted 4 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is B

upvoted 4 times

Question #422

Topic 1

A company has an application that has a web frontend. The application runs in the company's on-premises data center and requires access to file storage for critical data. The application runs on three Linux VMs for redundancy. The architecture includes a load balancer with HTTP request-based routing.

The company needs to migrate the application to AWS as quickly as possible. The architecture on AWS must be highly available.

Which solution will meet these requirements with the FEWEST changes to the architecture?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type in three Availability Zones. Use Amazon S3 to provide file storage for all three containers. Use a Network Load Balancer to direct traffic to the containers.
- B. Migrate the application to Amazon EC2 instances in three Availability Zones. Use Amazon Elastic File System (Amazon EFS) for file storage. Mount the file storage on all three EC2 instances. Use an Application Load Balancer to direct traffic to the EC2 instances.
- C. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) containers that use the Fargate launch type in three Availability Zones. Use Amazon FSx for Lustre to provide file storage for all three containers. Use a Network Load Balancer to direct traffic to the containers.
- D. Migrate the application to Amazon EC2 instances in three AWS Regions. Use Amazon Elastic Block Store (Amazon EBS) for file storage. Enable Cross-Region Replication (CRR) for all three EC2 instances. Use an Application Load Balancer to direct traffic to the EC2 instances.

Correct Answer: B

Community vote distribution

B (100%)

 **AzureDP900** 1 year, 1 month ago

Option B meets the requirements with the fewest changes to the architecture:

Migrate the application to Amazon EC2 instances in three Availability Zones: This is a straightforward migration of the existing Linux VMs to AWS EC2 instances, which provides high availability and redundancy.

Use Amazon Elastic File System (Amazon EFS) for file storage: Amazon EFS is a scalable file system that can be mounted on multiple EC2 instances, providing access to shared files without modifying the application's architecture.

Mount the file storage on all three EC2 instances: This ensures that all three EC2 instances have access to the critical data stored in Amazon EFS.

Use an Application Load Balancer to direct traffic to the EC2 instances: The existing load balancer with HTTP request-based routing can be replaced with an AWS Application Load Balancer, which provides better performance and scalability.

upvoted 2 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: B

Option B - "Amazon EFS provides scalable file storage for use with Amazon EC2. You can use an EFS file system as a common data source for workloads and applications running on multiple instances."

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEFS.html>

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: B

Option B

upvoted 1 times

 **nharaz** 1 year, 10 months ago

Selected Answer: B

B - is the best solution to meet the requirements with the fewest changes to the architecture. It maintains the application's architecture by using EC2 instances for compute, EFS for shared file storage across instances (mirroring on-premises file storage capabilities), and an ALB for HTTP request-based routing, ensuring a smooth transition to AWS with high availability.

upvoted 4 times

 **HunkBunk** 1 year, 10 months ago

Selected Answer: B

Answer - B

upvoted 2 times

 **kejam** 1 year, 10 months ago

Selected Answer: B

Answer B: FEWEST changes to the architecture

upvoted 3 times

 alexis123456 1 year, 10 months ago

Correct Answer is B

upvoted 4 times

Question #423

Topic 1

A company is planning to migrate an on-premises data center to AWS. The company currently hosts the data center on Linux-based VMware VMs. A solutions architect must collect information about network dependencies between the VMs. The information must be in the form of a diagram that details host IP addresses, hostnames, and network connection information.

Which solution will meet these requirements?

- A. Use AWS Application Discovery Service. Select an AWS Migration Hub home AWS Region. Install the AWS Application Discovery Agent on the on-premises servers for data collection. Grant permissions to Application Discovery Service to use the Migration Hub network diagrams.
- B. Use the AWS Application Discovery Service Agentless Collector for server data collection. Export the network diagrams from the AWS Migration Hub in .png format.
- C. Install the AWS Application Migration Service agent on the on-premises servers for data collection. Use AWS Migration Hub data in Workload Discovery on AWS to generate network diagrams.
- D. Install the AWS Application Migration Service agent on the on-premises servers for data collection. Export data from AWS Migration Hub in .csv format into an Amazon CloudWatch dashboard to generate network diagrams.

Correct Answer: A*Community vote distribution*

A (78%)

B (22%)

 **kejam** Highly Voted 1 year, 10 months ago

Selected Answer: A

<https://docs.aws.amazon.com/migrationhub/latest/ug/network-diagram-prerequisites.html>

upvoted 7 times

 **titi_r** 1 year, 8 months ago

"AWS Application Discovery Service Discovery Agent must be running on all of the on-premises servers that you want mapped in the diagram."

upvoted 2 times

 **MFEC** Most Recent 3 months, 3 weeks ago

Selected Answer: A

A is correct.

Agentless can not collect network connection data (network dependency)

upvoted 1 times

 **Soliner_Bilgi_Teknolojileri** 3 months, 3 weeks ago

Selected Answer: A

Answer A because only AWS Application Discovery Service with agents can capture detailed network dependencies (IP, hostnames, connections). This data flows into AWS Migration Hub, which can generate the required network diagrams. The other options either lack network-level visibility (agentless) or are for migration (MGN), not discovery.

upvoted 1 times

 **CAIYasia** 8 months, 2 weeks ago

Selected Answer: B

The Agentless Collector Works for Network Dependency Mapping
VMware Integration:

The Agentless Collector connects directly to your VMware vCenter Server.

It analyzes metadata and configurations of your VMware VMs, including:

IP addresses

Hostnames

Network interfaces

Running processes

Network Dependency Detection:

By monitoring network traffic patterns between VMs (e.g., TCP/UDP connections, ports, and communication frequency), the Agentless Collector identifies directional dependencies (e.g., which VMs communicate with each other).

Example: If VM-A connects to VM-B on port 443, the Collector logs this relationship.

Data Output:

The collected data is sent to AWS Migration Hub, where it is automatically visualized as network topology diagrams (exportable as .png).

Diagrams include:

IP addresses and hostnames of VMs.

Lines showing network connections between VMs.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option A. This solution meets all the requirements:

Use AWS Application Discovery Service: This service is designed to help you discover and map your on-premises infrastructure, including network dependencies between systems.

Select an AWS Migration Hub home AWS Region: This step ensures that the discovery process can collect data from the on-premises environment and import it into the Migration Hub for visualization.

Install the AWS Application Discovery Agent on the on-premises servers for data collection: The agent collects detailed information about network dependencies, including host IP addresses, hostnames, and network connection information.

Grant permissions to Application Discovery Service to use the Migration Hub network diagrams: This allows the service to create a visual representation of the network dependencies, which can be used to inform migration planning.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: A

A is correct.

Agentless can not collect network connection data(network dependency)

<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>

upvoted 2 times

 **gfhbox0083** 1 year, 5 months ago

A, for sure.

It's called AWS Application Discovery Agent, and not AWS Application Migration Service agent

upvoted 1 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: A

AWS ADS can't publish data to AWS Migration Hub without permission granted. B is wrong because question doesn't mention that all the vms are managed by vcenter plus missing grant permissom to ADS

upvoted 1 times

 **mns0173** 1 year, 6 months ago

You don't need agents in VMware environment

upvoted 2 times

 **BrijMohan08** 1 year, 8 months ago

Selected Answer: B

VMware VMs = Agentless

upvoted 4 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: A

Option A: AWS Application Discovery Service and agent types.

<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>

upvoted 2 times

 **career360guru** 1 year, 9 months ago

Selected Answer: A

Option A

upvoted 1 times

 **alexandercamachop** 1 year, 10 months ago

Selected Answer: A

A is the correct answer. We need agent install in order to generate network diagrams.

upvoted 3 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is A

upvoted 3 times

Question #424

Topic 1

A company runs a software-as-a-service (SaaS) application on AWS. The application consists of AWS Lambda functions and an Amazon RDS for MySQL Multi-AZ database. During market events, the application has a much higher workload than normal. Users notice slow response times during the peak periods because of many database connections. The company needs to improve the scalable performance and availability of the database.

Which solution meets these requirements?

- A. Create an Amazon CloudWatch alarm action that triggers a Lambda function to add an Amazon RDS for MySQL read replica when resource utilization hits a threshold.
- B. Migrate the database to Amazon Aurora, and add a read replica. Add a database connection pool outside of the Lambda handler function.
- C. Migrate the database to Amazon Aurora, and add a read replica. Use Amazon Route 53 weighted records.
- D. Migrate the database to Amazon Aurora, and add an Aurora Replica. Configure Amazon RDS Proxy to manage database connection pools.

Correct Answer: D

Community vote distribution

D (100%)

 **kejam** Highly Voted 1 year, 10 months ago

Selected Answer: D

Answer D:

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 6 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Option D meets all the requirements:

Migrate the database to Amazon Aurora: This provides a more scalable and available database solution.

Add an Aurora Replica: This allows for read-heavy workloads to be offloaded from the primary instance, reducing the load on the primary instance and improving overall performance.

Configure Amazon RDS Proxy to manage database connection pools: Amazon RDS Proxy is a dedicated proxy service that can manage connections to your database, allowing you to maintain multiple active connections without overwhelming the database. This helps improve scalability and availability.

upvoted 1 times

 **VerRi** 1 year, 9 months ago

Selected Answer: D

Moving database connection settings outside of the Lambda handler function may allow Lambda to reuse the connection, but RDS Proxy is better.

upvoted 3 times

 **career360guru** 1 year, 9 months ago

Selected Answer: D

Option D

upvoted 1 times

 **HunkyBunky** 1 year, 10 months ago

Selected Answer: D

D is a correct answer

upvoted 2 times

 **alexis123456** 1 year, 10 months ago

correct Answer is D

upvoted 4 times

Question #425

Topic 1

A company is planning to migrate an application from on premises to the AWS Cloud. The company will begin the migration by moving the application's underlying data storage to AWS. The application data is stored on a shared file system on premises, and the application servers connect to the shared file system through SMB.

A solutions architect must implement a solution that uses an Amazon S3 bucket for shared storage. Until the application is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB. The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data.

Which solution will meet these requirements?

- A. Create a new Amazon FSx for Windows File Server file system. Configure AWS DataSync with one location for the on-premises file share and one location for the new Amazon FSx file system. Create a new DataSync task to copy the data from the on-premises file share location to the Amazon FSx file system.
- B. Create an S3 bucket for the application. Copy the data from the on-premises storage to the S3 bucket.
- C. Deploy an AWS Server Migration Service (AWS SMS) VM to the on-premises environment. Use AWS SMS to migrate the file storage server from on premises to an Amazon EC2 instance.
- D. Create an S3 bucket for the application. Deploy a new AWS Storage Gateway file gateway on an on-premises VM. Create a new file share that stores data in the S3 bucket and is associated with the file gateway. Copy the data from the on-premises storage to the new file gateway endpoint.

Correct Answer: D*Community vote distribution*

D (95%) 5%

 **AzureDP900** 1 year, 1 month ago

Option D meets all the requirements:

- Create an S3 bucket for the application: This provides a shared storage location for the application's data.
- Deploy a new AWS Storage Gateway file gateway on an on-premises VM: The file gateway is used to enable SMB access to the S3 bucket, allowing the on-premises application to continue accessing the data through SMB.
- Create a new file share that stores data in the S3 bucket and is associated with the file gateway: This creates a bridge between the on-premises file system and the S3 bucket, allowing data to be copied from one location to another.
- Copy the data from the on-premises storage to the new file gateway endpoint: This ensures that all application data is migrated to the new shared storage location.

upvoted 2 times

 **juanife** 10 months, 2 weeks ago

this is a very completed and comprehensive answer. Thanks AzureDP900 for making our lives easier while trying to understand AWS' questions

upvoted 2 times

 **[Removed]** 1 year, 6 months ago

Option A

For me it's quite clear: "The solutions architect must migrate the application data to AWS to its new location WHILE STILL ALLOWING the on-premises application to access the data."

upvoted 3 times

 **wbedair** 1 year, 6 months ago

Not right. As per question requirements "A solutions architect must implement a solution that uses an Amazon S3 bucket for shared storage"

upvoted 4 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: D

Option D : AWS Architecture Blog

<https://aws.amazon.com/blogs/architecture/connect-amazon-s3-file-gateway-using-aws-privatelink-for-amazon-s3/>

upvoted 3 times

 **career360guru** 1 year, 9 months ago

Selected Answer: D

Option D.

upvoted 2 times

 **GeorgeRemus** 1 year, 10 months ago

Selected Answer: D

Correct Answer is D

upvoted 3 times

 **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: D

the application must continue to have access to the data through SMB = Storage Gateway

upvoted 4 times

 **HunkBunk** 1 year, 10 months ago

Selected Answer: D

I guess that proper answer is - D

We need to implement solution that uses Amazon S3 bucket for shared storage, but during migration phase - data should be available through SMB. Only D option fits in this requirements

upvoted 3 times

 **kejam** 1 year, 10 months ago

Selected Answer: D

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

upvoted 4 times

 **master9** 1 year, 10 months ago

Selected Answer: B

S3 bucket

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is D

upvoted 3 times

Question #426

A global company has a mobile app that displays ticket barcodes. Customers use the tickets on the mobile app to attend live events. Event scanners read the ticket barcodes and call a backend API to validate the barcode data against data in a database. After the barcode is scanned, the backend logic writes to the database's single table to mark the barcode as used.

The company needs to deploy the app on AWS with a DNS name of api.example.com. The company will host the database in three AWS Regions around the world.

Which solution will meet these requirements with the LOWEST latency?

- A. Host the database on Amazon Aurora global database clusters. Host the backend on three Amazon Elastic Container Service (Amazon ECS) clusters that are in the same Regions as the database. Create an accelerator in AWS Global Accelerator to route requests to the nearest ECS cluster. Create an Amazon Route 53 record that maps api.example.com to the accelerator endpoint
- B. Host the database on Amazon Aurora global database clusters. Host the backend on three Amazon Elastic Kubernetes Service (Amazon EKS) clusters that are in the same Regions as the database. Create an Amazon CloudFront distribution with the three clusters as origins. Route requests to the nearest EKS cluster. Create an Amazon Route 53 record that maps api.example.com to the CloudFront distribution.
- C. Host the database on Amazon DynamoDB global tables. Create an Amazon CloudFront distribution. Associate the CloudFront distribution with a CloudFront function that contains the backend logic to validate the barcodes. Create an Amazon Route 53 record that maps api.example.com to the CloudFront distribution.
- D. Host the database on Amazon DynamoDB global tables. Create an Amazon CloudFront distribution. Associate the CloudFront distribution with a Lambda@Edge function that contains the backend logic to validate the barcodes. Create an Amazon Route 53 record that maps api.example.com to the CloudFront distribution.

Correct Answer: D

Community vote distribution

D (92%)	8%
---------	----

 **alexis123456** Highly Voted  1 year, 10 months ago

Correct Answer is A
upvoted 6 times

 **HunkBunk** Highly Voted  1 year, 10 months ago

Selected Answer: D
D is the proper answer

CloudFront Functions - can be used only for manipulation with requests data
CloudFront Lambda@Edge functions - can be used for anything, because this is a regular lambda function
upvoted 6 times

 **strike3test** Most Recent  5 months, 3 weeks ago

Selected Answer: D
Aurora global databases have a primary region for writes and secondary read-only regions, which can add latency for write operations (marking barcodes as used).
upvoted 1 times

 **sergza888** 8 months, 2 weeks ago

Selected Answer: A
I do not think it is Lambda@Edge use case which are mostly addressing routing or content management type of things or A/B testing. It is write intensive so i would choose Aurora and Global Accelerator and this is not about content cache (Cloud front)
upvoted 1 times

 **LeoSantos12121212121212121** 8 months, 3 weeks ago

Selected Answer: A
Aurora Global Database provides low-latency read access from multiple Regions and allows writes in a primary Region. Since the system only marks the ticket as used once, it's safe to centralize writes.
ECS clusters deployed regionally offer scalable, containerized API backends.

AWS Global Accelerator routes users to the closest backend ECS cluster using the AWS edge network, minimizing latency and maximizing performance.

Route 53 maps the DNS (api.example.com) to the Global Accelerator endpoint.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option D is correct

DynamoDB global tables: By hosting your database in multiple Regions, you can reduce latency for users located in different parts of the world.

CloudFront: You can use CloudFront as a CDN to cache static assets and route dynamic requests to the nearest origin. In this case, it will direct users to the Lambda@Edge function closest to them.

Lambda@Edge functions: These allow you to execute code at the edge of the network, which reduces latency and improves performance. Using Lambda@Edge functions in conjunction with DynamoDB global tables provides a great combination for reducing latency and improving performance.

upvoted 1 times

 **9f02c8d** 1 year, 6 months ago

Option: D

upvoted 1 times

 **red_panda** 1 year, 7 months ago

Selected Answer: D

D without any doubt.

For this simple data, a DynamoDB Table is enough; so global table is perfect.

For check logic, cloudfront function is not enough because it is only for manipulate HTTP header or something very very light (code, metadata etc.). So for calling some backend layer (querying DynamoDB in this case) we need a Lambda@Edge function, which is much complete.

upvoted 5 times

 **career360guru** 1 year, 9 months ago

Selected Answer: D

Option D

upvoted 1 times

 **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: D

D. Lambda@Edge

upvoted 4 times

 **kejam** 1 year, 10 months ago

Selected Answer: D

<https://aws.amazon.com/blogs/networking-and-content-delivery/leveraging-external-data-in-lambdaedge/>

<https://aws.amazon.com/blogs/networking-and-content-delivery/lambdaedge-design-best-practices/>

upvoted 5 times

Question #427

Topic 1

A medical company is running a REST API on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group behind an Application Load Balancer (ALB). The ALB runs in three public subnets, and the EC2 instances run in three private subnets. The company has deployed an Amazon CloudFront distribution that has the ALB as the only origin.

Which solution should a solutions architect recommend to enhance the origin security?

- A. Store a random string in AWS Secrets Manager. Create an AWS Lambda function for automatic secret rotation. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Create an AWS WAF web ACL rule with a string match rule for the custom header. Associate the web ACL with the ALB.
- B. Create an AWS WAF web ACL rule with an IP match condition of the CloudFront service IP address ranges. Associate the web ACL with the ALB. Move the ALB into the three private subnets.
- C. Store a random string in AWS Systems Manager Parameter Store. Configure Parameter Store automatic rotation for the string. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Inspect the value of the custom HTTP header, and block access in the ALB.
- D. Configure AWS Shield Advanced. Create a security group policy to allow connections from CloudFront service IP address ranges. Add the policy to AWS Shield Advanced, and attach the policy to the ALB.

Correct Answer: A

Community vote distribution

A (91%) 9%

 **kejam** Highly Voted 1 year, 10 months ago

Selected Answer: A

In this blog post, you'll see how to use CloudFront custom headers, AWS WAF, and AWS Secrets Manager to restrict viewer requests from accessing your CloudFront origin resources directly.

<https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/>
upvoted 6 times

 **SIJUTHOMASP** Most Recent 1 year ago

Selected Answer: B

While secret manager can auto rotate the secrets why to use Lamda to rotate? The choice B is neater than A?
upvoted 1 times

 **GabrielShiao** 11 months ago

B is not correct. Moving ALB to private subnets makes the Cloudfront traffic unreachable.
upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Option A is right
Store a random string in Secrets Manager: This provides a secure way to store sensitive data, such as a token or secret key.
Create an AWS Lambda function for automatic secret rotation: This ensures that the secret is regularly rotated and updated to prevent unauthorized access.
Configure CloudFront to inject the random string as a custom HTTP header for the origin request: This adds an additional layer of protection by requiring the ALB to verify the custom header before allowing access.
Create an AWS WAF web ACL rule with a string match rule for the custom header: This checks that the custom header matches the expected value, preventing unauthorized access if it doesn't.
Associate the web ACL with the ALB: This ensures that the security rules are enforced at the edge of the network, protecting against malicious traffic.

The other options don't provide sufficient protection:

upvoted 1 times

 **Win007** 1 year, 7 months ago

D is the correct Answer
upvoted 1 times

 **trungtd** 1 year, 6 months ago

you cannot directly add a security group to AWS Shield Advanced. BTW, what is security group policy?
upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: A

Option A

upvoted 1 times

  **TheCloudGuruu** 1 year, 10 months ago**Selected Answer: A**

Answer is A

upvoted 1 times

  **HunkkBunk** 1 year, 10 months ago**Selected Answer: A**

A - is a proper answer

<https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/>

upvoted 2 times

  **alexis123456** 1 year, 10 months ago

Correct Answer is A

upvoted 4 times

Question #428

Topic 1

To abide by industry regulations, a solutions architect must design a solution that will store a company's critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located. The solutions architect is required to provide access to the data stored in AWS to the company's global WAN network. The security team mandates that no traffic accessing this data should traverse the public internet.

How should the solutions architect design a highly available solution that meets the requirements and is cost-effective?

- A. Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use. Use the company WAN to send traffic over to the headquarters and then to the respective DX connection to access the data.
- B. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use inter-region VPC peering to access the data in other AWS Regions.
- C. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use an AWS transit VPC solution to access data in other AWS Regions.
- D. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use Direct Connect Gateway to access data in other AWS Regions.

Correct Answer: D*Community vote distribution*

D (85%)

Other

 **trungtd** Highly Voted 1 year, 6 months ago

Selected Answer: D

DX + DXGW

upvoted 5 times

 **TomTom** Most Recent 1 year, 1 month ago

Selected Answer: B

The most cost-effective option for accessing data across multiple AWS Regions while using AWS Direct Connect is B.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

This solution meets the requirements and is cost-effective.

Option D

AWS Direct Connect: This service allows you to establish a dedicated network connection between your premises and an AWS Region, which bypasses the public internet.

Two connections: Establishing two connections provides redundancy, ensuring that if one connection fails, the other can take over. This meets the requirement for high availability.

Direct Connect Gateway: By using a Direct Connect Gateway, you can extend the connectivity to multiple AWS Regions, allowing your global WAN network to access data in those regions without traversing the public internet.

upvoted 3 times

 **sarlos** 1 year, 7 months ago

between C and D: TGW is a regional service. So D is the answer

upvoted 3 times

 **career360guru** 1 year, 9 months ago

Selected Answer: D

Option D

upvoted 1 times

 **adelynlll** 1 year, 10 months ago

D:

Need direct connect gateway to share with other regions

upvoted 4 times

 **nharaz** 1 year, 10 months ago

Selected Answer: D

D - offers a blend of high availability (through redundancy with two DX connections), cost-effectiveness (by reducing the number of DX connections required), and simplicity (by avoiding the complexity of managing a transit VPC or multiple peering connections).

upvoted 3 times

✉️ **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: C

C. transit VPC

upvoted 1 times

✉️ **pangchn** 1 year, 8 months ago

D

Transit gateway is regional service.

We need DX gateway here

upvoted 4 times

✉️ **kejam** 1 year, 10 months ago

Selected Answer: D

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/direct-connect.html>

upvoted 2 times

✉️ **07c2d2a** 1 year, 10 months ago

It seems to suggest you pay extra to do it that way. This is asking for the most cost-effective option.

upvoted 1 times

✉️ **07c2d2a** 1 year, 10 months ago

"With the previous two options, you pay for Direct Connect pricing. For this option, you also pay for the Transit Gateway attachment and data processing charges."

upvoted 2 times

✉️ **alexis123456** 1 year, 10 months ago

Correct Answer is D

upvoted 2 times

Question #429

Topic 1

A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts on premises. The application data is stored in a proprietary format that must be read through the application. The company manually provisioned the servers and the application.

As part of its disaster recovery plan, the company wants the ability to host its application on AWS temporarily if the company's on-premises environment becomes unavailable. The company wants the application to return to on-premises hosting after a disaster recovery event is complete. The RPO is 5 minutes.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Configure AWS DataSync. Replicate the data to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and attach the EBS volumes.
- B. Configure AWS Elastic Disaster Recovery. Replicate the data to replication Amazon EC2 instances that are attached to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use Elastic Disaster Recovery to launch EC2 instances that use the replicated volumes.
- C. Provision an AWS Storage Gateway file gateway. Replicate the data to an Amazon S3 bucket. When the on-premises environment is unavailable, use AWS Backup to restore the data to Amazon Elastic Block Store (Amazon EBS) volumes and launch Amazon EC2 instances from these EBS volumes.
- D. Provision an Amazon FSx for Windows File Server file system on AWS. Replicate the data to the file system. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and use AWS::CloudFormation::Init commands to mount the Amazon FSx file shares.

Correct Answer: B

Community vote distribution

B (94%)	6%
---------	----

 **TomTom** 1 year, 1 month ago

Selected Answer: B

The best solution for the company's disaster recovery needs with minimal operational overhead is B. Configure AWS Elastic Disaster Recovery.

This option enables continuous data replication to Amazon EC2 instances attached to Amazon EBS volumes, ensuring the RPO of 5 minutes is met. When the on-premises environment fails, Elastic Disaster Recovery can automatically launch the EC2 instances using the replicated volumes, streamlining the recovery process and reducing manual intervention compared to other options.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Option B is right

Elastic Disaster Recovery: This service allows you to create a replication instance in AWS, which can be used as a target for your application data. When your on-premises environment is unavailable, Elastic Disaster Recovery can automatically launch EC2 instances using the replicated volumes.

Zero-configuration restore: With Elastic Disaster Recovery, there's no need to configure any additional services or scripts to restore the application. The service takes care of launching the correct EC2 instances with the necessary EBS volumes attached.

RPO of 5 minutes: By replicating your data regularly (e.g., every 5 minutes), you can ensure that your RPO is met, and in case of a disaster, the replicated data will be available on AWS.

upvoted 2 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: B

Option B: AWS Elastic Disaster Recovery performance Failover and Failback

<https://docs.aws.amazon.com/drs/latest/userguide/failback-overview.html>

upvoted 3 times

 **Dgix** 1 year, 9 months ago

Selected Answer: B

B is the correct answer. AWS Elastic Disaster Recovery aligns with low operational overhead and 5-minute RPO. It takes care of ongoing replication

A: Incorrect, DataSync lacks comprehensive DR capabilities and requires manual provisioning.

C: Incorrect, introduces complexity and doesn't support a 5-minute RPO for DR.

D: Incorrect, FSx lacks automated DR solutions for VMware vSphere VMs, increasing overhead.

upvoted 3 times

 **career360guru** 1 year, 9 months ago

Selected Answer: B

Option B

upvoted 1 times

 **Russ99** 1 year, 10 months ago

Selected Answer: D

I selected option D, option B is requires enabling and configuring AWS disaster recovery service, monitoring replication status. In the even of a disaster. The replication of EC2 instances needs to be managed and maintained even where not in used.

upvoted 1 times

 **marszalekm** 1 year, 10 months ago

The RPO is 5 minutes.

upvoted 1 times

 **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: B

Answer is B

upvoted 2 times

 **HunkyBunkY** 1 year, 10 months ago

Selected Answer: B

Correct answer is B - because only this option will provide LEAST amount of operational overhead.

A - is out, because DataSync can't replicate data to EBS volumes

C - is out, because AWS Backup can't restore not managed data from S3 to EBS

D - is out, because it is not provide a way HOW we will replicate data from on-premise to FSx. Also, it is require additional amount of operational overhead

upvoted 4 times

 **kejam** 1 year, 10 months ago

Selected Answer: B

<https://aws.amazon.com/disaster-recovery/>

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is D

upvoted 2 times

Question #430

A company runs a highly available data collection application on Amazon EC2 in the eu-north-1 Region. The application collects data from end-user devices and writes records to an Amazon Kinesis data stream and a set of AWS Lambda functions that process the records. The company persists the output of the record processing to an Amazon S3 bucket in eu-north-1. The company uses the data in the S3 bucket as a data source for Amazon Athena.

The company wants to increase its global presence. A solutions architect must launch the data collection capabilities in the sa-east-1 and ap-northeast-1 Regions. The solutions architect deploys the application, the Kinesis data stream, and the Lambda functions in the two new Regions. The solutions architect keeps the S3 bucket in eu-north-1 to meet a requirement to centralize the data analysis.

During testing of the new setup, the solutions architect notices a significant lag on the arrival of data from the new Regions to the S3 bucket.

Which solution will improve this lag time the MOST?

- A. In each of the two new Regions, set up the Lambda functions to run in a VPC. Set up an S3 gateway endpoint in that VPC.
- B. Turn on S3 Transfer Acceleration on the S3 bucket in eu-north-1. Change the application to use the new S3 accelerated endpoint when the application uploads data to the S3 bucket.
- C. Create an S3 bucket in each of the two new Regions. Set the application in each new Region to upload to its respective S3 bucket. Set up S3 Cross-Region Replication to replicate data to the S3 bucket in eu-north-1.
- D. Increase the memory requirements of the Lambda functions to ensure that they have multiple cores available. Use the multipart upload feature when the application uploads data to Amazon S3 from Lambda.

Correct Answer: C*Community vote distribution*

C (69%)

B (31%)

 **wyedh1** Highly Voted 1 year, 10 months ago

Selected Answer: C

s3 transfer acceleration is not supported in eu-north-1 region yet
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html>
 upvoted 20 times

 **VerRi** Highly Voted 1 year, 9 months ago

Selected Answer: C

"improve this lag time the MOST" means improve the time for "uploading files" not "uploading the files to the destination." Uploading the files to the bucket in the same region is faster than transferring them to other regions.
 upvoted 8 times

 **teashoppe** Most Recent 1 week, 1 day ago

Selected Answer: C

B incorrect (S3 Transfer Acceleration): Helps most when uploads come from the public internet and can benefit from entering AWS at an edge location. Your uploads are coming from AWS Regions (Lambda/EC2) over AWS backbone already; TA usually won't be the biggest improvement here.
 upvoted 1 times

 **aka1177** 4 weeks ago

Selected Answer: C

The requirement for centralizing data in the region exists solely because analysis is done with Athena. Therefore, replicating data from other regions is definitely a viable solution. The correct answer is C.
 upvoted 1 times

 **0dc6cac** 6 months, 1 week ago

Selected Answer: B

None of the answers are correct. B isn't supported in that region, and C breaks the requirement to keep the data in the specific region (EU has very strong regulations regarding data, moving to another region is out of the question).

I'd say that the region is a typo, and go with B for this question
 upvoted 1 times

 **BelloMio** 8 months, 2 weeks ago

Selected Answer: C

Answer is C

I mean if this question is on the exam that's just ridiculous.

You would have to know by heart that eu-north-1 is not yet supported for transfer acceleration.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html>

upvoted 1 times

 **itsjunukim** 9 months, 2 weeks ago

Selected Answer: B

"keeps the S3 bucket in eu-north-1 to meet a requirement to centralize the data analysis" B

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: C

By implementing Option C, the company can leverage the proximity of local S3 buckets in each Region, while still maintaining a centralized data store in eu-north-1 through Cross-Region Replication. This approach minimizes the lag time for data arrival and ensures that the data analysis in Amazon Athena is performed on the complete and up-to-date dataset.

The other options have limitations or may not address the lag time issue effectively:

Option A (VPC and S3 gateway endpoint) does not directly address the latency issue caused by the long distances between Regions.

Option B (S3 Transfer Acceleration) can improve transfer speeds but may not be as effective as having local S3 buckets in each Region.

Option D (increasing Lambda memory and using multipart uploads) may improve Lambda performance but does not address the underlying network latency issue.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Considering the current limitations of S3 Transfer Acceleration in the eu-north-1 Region, I would say that Option C is actually the best choice.

upvoted 1 times

 **AloraCloud** 1 year, 1 month ago

Except if RTC is enabled you cannot guarantee that the data replicated to the central S3 bucket in eu-north-1 will be up to date.

I'll be dammed if AWS is really expecting folks to remember the regions which do not have the Amazon S3 Transfer Acceleration feature.

upvoted 2 times

 **AloraCloud** 1 year, 2 months ago

I think the answer is C because Amazon Kinesis Data Streams cannot directly leverage S3 Transfer Acceleration. S3 Transfer Acceleration is typically used for accelerating transfers from clients to S3 and doesn't support Kinesis Data Streams directly.

upvoted 2 times

 **Syre** 1 year, 3 months ago

Selected Answer: B

While C would work, it adds complexity by requiring separate S3 buckets in each Region and replicating data, which could increase cost and delay due to replication schedules.

upvoted 2 times

 **trungtd** 1 year, 6 months ago

Selected Answer: C

No matter how fast you run, you cannot run from Tokyo to Stockholm as fast as someone 10km from Stockholm.

upvoted 2 times

 **e4bc18e** 1 year, 7 months ago

Answer is C but feel this is one they definitely want people to get wrong. No one is going to memorize which regions every feature is supported in, it is something anyone would look up.

upvoted 2 times

 **seetp** 1 year, 7 months ago

Selected Answer: C

I would choose B but it cannot be B because S3 Transfer Acceleration is not supported in eu-north-1. This leaves C as the only viable option.

upvoted 3 times

 **qaz12wsx** 1 year, 8 months ago

Selected Answer: C

agree with bjexamprep

upvoted 3 times

 **bjexamprep** 1 year, 8 months ago

Selected Answer: C

S3 Transfer Acceleration achieves acceleration by AWS routing traffic to AWS CloudFront edge location and transfer AWS network backbone. The key speed improvement is AWS network backbone.

While, in this case, the application in the two new regions is the client to write the output to S3 in EU, which means the client is already on AWS, the data transportation is already on AWS network backbone. So S3 Transfer Acceleration is not helping at all. B is out.

C is the best answer.

upvoted 6 times

Question #431

Topic 1

A company provides a centralized Amazon EC2 application hosted in a single shared VPC. The centralized application must be accessible from client applications running in the VPCs of other business units. The centralized application front end is configured with a Network Load Balancer (NLB) for scalability.

Up to 10 business unit VPCs will need to be connected to the shared VPC. Some of the business unit VPC CIDR blocks overlap with the shared VPC, and some overlap with each other. Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only.

Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?

- A. Create an AWS Transit Gateway. Attach the shared VPC and the authorized business unit VPCs to the transit gateway. Create a single transit gateway route table and associate it with all of the attached VPCs. Allow automatic propagation of routes from the attachments into the route table. Configure VPC routing tables to send traffic to the transit gateway.
- B. Create a VPC endpoint service using the centralized application NLB and enable the option to require endpoint acceptance. Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint service. Accept authorized endpoint requests from the endpoint service console.
- C. Create a VPC peering connection from each business unit VPC to the shared VPC. Accept the VPC peering connections from the shared VPC console. Configure VPC routing tables to send traffic to the VPC peering connection.
- D. Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized business unit VPCs. Establish a Site-to-Site VPN connection from the business unit VPCs to the shared VPC. Configure VPC routing tables to send traffic to the VPN connection.

Correct Answer: B*Community vote distribution*

B (100%)

 **sat2008** Highly Voted 1 year, 10 months ago

B is the answer for me
Only way to get around overlapping IP range is using endpoint service
upvoted 7 times

 **0b43291** Most Recent 1 year, 1 month ago

Selected Answer: B
By using a VPC endpoint service with the "require endpoint acceptance" option, the company can securely and efficiently provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC, while addressing the requirements of overlapping CIDR blocks and controlled access.

A. AWS Transit Gateway: While Transit Gateway can connect multiple VPCs, it does not provide a mechanism to control access or handle overlapping CIDR blocks between VPCs.

C. VPC Peering: VPC peering does not support overlapping CIDR blocks between VPCs, which is a requirement in this scenario. Additionally, managing multiple VPC peering connections can become complex and difficult to maintain as the number of VPCs increases.

D. Site-to-Site VPN: No
upvoted 3 times

 **AzureDP900** 1 year, 1 month ago

By choosing Option B, you get secure, private connectivity between the client applications in the business unit VPCs and the centralized application in the shared VPC without introducing unnecessary complexity or costs.
This configuration provides secure, private connectivity between the client applications in the business unit VPCs and the centralized application in the shared VPC.
upvoted 1 times

 **Moghite** 1 year, 5 months ago

Selected Answer: B
only option to get around of IP overlapping
<https://aws.amazon.com/blogs/networking-and-content-delivery/connecting-networks-with-overlapping-ip-ranges/>
upvoted 2 times

 **43c89f4** 1 year, 8 months ago

A is actually. they never mentioned cost effect or less effort solution.

when they are not mentioned anything we need to prefer best option

upvoted 1 times

 **sarlos** 1 year, 7 months ago

Not possible, because TGW does not support overlapping ranges

upvoted 4 times

 **toma** 1 year, 5 months ago

"This requires that automatic route propagation to Transit Gateway be disabled as not all of the subnets in each VPC should be advertised." so it is B

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: B

option B

upvoted 1 times

 **arberod** 1 year, 10 months ago

Selected Answer: B

B is the answer

upvoted 2 times

 **HunkBunky** 1 year, 10 months ago

Selected Answer: B

Answer is B

Application already uses NLB so this is a best way for solve that task

upvoted 2 times

 **kejam** 1 year, 10 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/46708-exam-aws-certified-solutions-architect-professional-topic-1/>

<https://aws.amazon.com/blogs/networking-and-content-delivery/connecting-networks-with-overlapping-ip-ranges/>

upvoted 4 times

 **master9** 1 year, 10 months ago

Selected Answer: B

VPC Endpoint Service can do the job

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is A

upvoted 4 times

Question #432

Topic 1

A company wants to migrate its website to AWS. The website uses microservices and runs on containers that are deployed in an on-premises, self-managed Kubernetes cluster. All the manifests that define the deployments for the containers in the Kubernetes deployment are in source control.

All data for the website is stored in a PostgreSQL database. An open source container image repository runs alongside the on-premises environment.

A solutions architect needs to determine the architecture that the company will use for the website on AWS.

Which solution will meet these requirements with the LEAST effort to migrate?

- A. Create an AWS App Runner service. Connect the App Runner service to the open source container image repository. Deploy the manifests from on premises to the App Runner service. Create an Amazon RDS for PostgreSQL database.
- B. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that has managed node groups. Copy the application containers to a new Amazon Elastic Container Registry (Amazon ECR) repository. Deploy the manifests from on premises to the EKS cluster. Create an Amazon Aurora PostgreSQL DB cluster.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster that has an Amazon EC2 capacity pool. Copy the application containers to a new Amazon Elastic Container Registry (Amazon ECR) repository. Register each container image as a new task definition. Configure ECS services for each task definition to match the original Kubernetes deployments. Create an Amazon Aurora PostgreSQL DB cluster.
- D. Rebuild the on-premises Kubernetes cluster by hosting the cluster on Amazon EC2 instances. Migrate the open source container image repository to the EC2 instances. Deploy the manifests from on premises to the new cluster on AWS. Deploy an open source PostgreSQL database on the new cluster.

Correct Answer: B*Community vote distribution*

B (100%)

 **AzureDP900** 1 year, 1 month ago

Option B is actually a very good choice. Creating an Amazon Elastic Kubernetes Service (EKS) cluster that has managed node groups allows for a seamless migration of the existing Kubernetes deployment to AWS, while maintaining the flexibility and scalability of EKS.

upvoted 1 times

 **AloraCloud** 1 year, 2 months ago

B is an AWS Solutions/Sales team to a customer answer

upvoted 1 times

 **Spike2020** 1 year, 6 months ago

B is best to manage, but is it easiest to migrate? you still need to adjust manifest file for managed node groups and ECR repo. D is lift and shift.

upvoted 3 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: B

Option B: Some additional migration to EKS info

(1) <https://aws.amazon.com/blogs/architecture/field-notes-migrating-a-self-managed-kubernetes-cluster-on-ec2-to-amazon-eks/>

(2) <https://aws.amazon.com/blogs/containers/migrating-from-self-managed-kubernetes-to-amazon-eks-here-are-some-key-considerations/>

upvoted 3 times

 **career360guru** 1 year, 9 months ago

Selected Answer: B

Option B

upvoted 1 times

 **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: B

B is the best option

upvoted 1 times

✉  **arberod** 1 year, 10 months ago

Selected Answer: B

It is B

upvoted 1 times

✉  **HunkBunk** 1 year, 10 months ago

Selected Answer: B

Answer is B - because only in that case - we don't need to do any changes in application

A - is out, because we will need to create deployments for many micro-services

C - is out, because we will need to create ecs deployments for many micro-services

D - is out, because it will require a lot of overhead and efforts for self-managed K8S setup

upvoted 3 times

✉  **kejam** 1 year, 10 months ago

Selected Answer: B

Answer B: LEAST effort to migrate

Minor changes to the manifest files seems like the least amount of work compared to what needs to be done in the other answers.

upvoted 4 times

✉  **alexis123456** 1 year, 10 months ago

Correct answer is B

upvoted 3 times

Question #433

A company uses a mobile app on AWS to run online contests. The company selects a winner at random at the end of each contest. The contests run for variable lengths of time. The company does not need to retain any data from a contest after the contest is finished.

The company uses custom code that is hosted on Amazon EC2 instances to process the contest data and select a winner. The EC2 instances run behind an Application Load Balancer and store contest entries on Amazon RDS DB instances. The company must design a new architecture to reduce the cost of running the contests.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate storage of the contest entries to Amazon DynamoDB. Create a DynamoDB Accelerator (DAX) cluster. Rewrite the code to run as Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type. At the end of the contest, delete the DynamoDB table.
- B. Migrate the storage of the contest entries to Amazon Redshift. Rewrite the code as AWS Lambda functions. At the end of the contest, delete the Redshift cluster.
- C. Add an Amazon ElastiCache for Redis cluster in front of the RDS DB instances to cache the contest entries. Rewrite the code to run as Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type. Set the ElastiCache TTL attribute on each entry to expire each entry at the end of the contest.
- D. Migrate the storage of the contest entries to Amazon DynamoDB. Rewrite the code as AWS Lambda functions. Set the DynamoDB TTL attribute on each entry to expire each entry at the end of the contest.

Correct Answer: D

Community vote distribution

D (64%)

A (36%)

 **m1xa** Highly Voted 1 year, 7 months ago

Selected Answer: D

Lambda for choosing a winner (it's a short-term task) and TTL (known before the contest starts) make sense.
upvoted 6 times

 **tonytam1991** Most Recent 11 months ago

Selected Answer: A

This is what I hate AWS keep using impractical examples or unclear assumptions on their exam, it just train a lot of people just know yelling: "lambda is cheap, lambda is efficiency".
upvoted 2 times

 **eboehm** 2 weeks ago

its not even about that its that you dont need a container for this. This is a very simple function that runs once... perfect for Lambda... plus wtf do you need DAX for? A could of been a contender if it didnt needless mention DAX.
upvoted 1 times

 **eboehm** 2 weeks ago

if the architecture was about users checking the winning results, then yes DAX would be usefull
upvoted 1 times

 **SIJUTHOMASP** 1 year ago

Selected Answer: D

Here cost is the only concern and not performance, option A can be ruled out because no DAX is required. Simply Dynamo DB in option D would be more than sufficient.
upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option D

Migrate Storage: Migrating storage from RDS DB instances (which require a significant upfront cost) to DynamoDB (a fully managed NoSQL database service with low usage-based costs) will significantly reduce the company's expenses.

Lambda Functions: Rewriting code as AWS Lambda functions (serverless computing for code execution) will eliminate the need for EC2 instances, reducing costs even further. Lambda functions are also ideal for tasks that run infrequently or have short durations.

DynamoDB TTL Attribute: By using DynamoDB's TTL attribute to expire each entry at the end of the contest, the company can automatically clean up unused data without requiring manual deletion.
upvoted 1 times

 **Moghite** 1 year, 5 months ago

Selected Answer: D

Option D is the most cost Efficient
upvoted 2 times

 **vip2** 1 year, 5 months ago

Selected Answer: A

remove entire DynamoDB and DAX is used for reduce RCU
upvoted 1 times

 **Training** 1 year, 6 months ago

Should be A. With Variable lengths of time, Lambda is not the right choice.
upvoted 2 times

 **trungtd** 1 year, 6 months ago

Selected Answer: D

"the contests run for variable lengths of time" does not mean that those time periods are not known. We do not need a fixed value for TTL but can use Lambda to change timestamp depending on each contest.
upvoted 3 times

 **9f02c8d** 1 year, 6 months ago

Option D, The option A doesn't fulfill the requirement of cost effectiveness as there is no reason to use DAX
upvoted 2 times

 **red_panda** 1 year, 7 months ago

Selected Answer: A

Correct option is A here.
First of all, we don't know how much time the contest will last as per requirements, so fix the TTL it's a mistake.
Second point, we can delete the entire table as we didn't the file after the end of the context, so no data to retain.
Finally, for web contest, we don't know how much users will be online, and providing a cache layer might be a good solution.
upvoted 2 times

 **titi_r** 1 year, 8 months ago

Selected Answer: D

D - correct.
upvoted 2 times

 **tushar321** 1 year, 8 months ago

D. There is no in memory cache requirement here for DAX. So omitting A
upvoted 2 times

 **bjexamprep** 1 year, 8 months ago

Selected Answer: A

The question is looking for "MOST cost-effectively". I assume DAX + DynamoDB is cheaper than DynamoDB only. Cause DAX should be able to reduce the RCU cost and improve performance. This is an online contest, which means the RCU could be very high.
"the contests run for variable lengths of time" means you can't set a fix TTL for the record entry. And even you can have a fix time, the record being submitted 1 min before the deadline will still be kept for the TTL and keep generating cost.
upvoted 3 times

 **pangchn** 1 year, 8 months ago

Selected Answer: A

Vote for A here
reason as specified by zouwelaar
upvoted 4 times

 **zouwelaar** 1 year, 8 months ago

Selected Answer: A

You are forgetting that the contests run for variable lengths of time. So Lambda and TTL are out.
upvoted 4 times

 **w3ap0nx** 1 year, 8 months ago

Assuming each contest still has a set time from the start, D is most cost efficient, TTL is set based on each contest time. Lambda is only used to add/fetch entries and select random winner, runtime is minimal. I go with D here
upvoted 2 times

 **career360guru** 1 year, 9 months ago

Selected Answer: D

Option D
upvoted 2 times

 **duriselvan** 1 year, 10 months ago

Time To Live (TTL) for DynamoDB is a cost-effective method for deleting items that are no longer relevant. TTL allows you to define a per-item expiration timestamp that indicates when an item is no longer needed. DynamoDB automatically deletes expired items within a few days of their expiration time, without consuming write throughput.

upvoted 3 times

Question #434

A company has implemented a new security requirement. According to the new requirement, the company must scan all traffic from corporate AWS instances in the company's VPC for violations of the company's security policies. As a result of these scans, the company can block access to and from specific IP addresses.

To meet the new requirement, the company deploys a set of Amazon EC2 instances in private subnets to serve as transparent proxies. The company installs approved proxy server software on these EC2 instances. The company modifies the route tables on all subnets to use the corresponding EC2 instances with proxy software as the default route. The company also creates security groups that are compliant with the security policies and assigns these security groups to the EC2 instances.

Despite these configurations, the traffic of the EC2 instances in their private subnets is not being properly forwarded to the internet.

What should a solutions architect do to resolve this issue?

- A. Disable source/destination checks on the EC2 instances that run the proxy software.
- B. Add a rule to the security group that is assigned to the proxy EC2 instances to allow all traffic between instances that have this security group. Assign this security group to all EC2 instances in the VPC.
- C. Change the VPCs DHCP options set. Set the DNS server options to point to the addresses of the proxy EC2 instances.
- D. Assign one additional elastic network interface to each proxy EC2 instance. Ensure that one of these network interfaces has a route to the private subnets. Ensure that the other network interface has a route to the internet.

Correct Answer: A

Community vote distribution

A (76%)

D (24%)

 **kejam** Highly Voted 1 year, 10 months ago

Selected Answer: A

Answer A:

Proxies like NATs will need SrcDestCheck disabled

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html#EIP_Disable_SrcDestCheck
upvoted 9 times

 **0b43291** Most Recent 1 year, 1 month ago

Selected Answer: A

In an Amazon VPC, the source/destination check is a security feature that ensures that an instance cannot be used as a network gateway or router to forward traffic between resources. By default, this check is enabled on all EC2 instances.

When you want to use an EC2 instance as a transparent proxy or network appliance to forward traffic between resources, you need to disable the source/destination check on that instance. This allows the instance to receive and forward traffic that is not destined for itself.

The other options provided would not resolve the issue:

Option B (adding a security group rule) would not enable the proxy instances to forward traffic, as the source/destination check is a separate network configuration.

Option C (changing DHCP options) would not affect the ability of the proxy instances to forward traffic.

Option D (adding additional network interfaces) is not necessary, as the issue is related to the source/destination check and not the network interface configuration.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Option A resolves the issue by allowing the traffic of the EC2 instances in their private subnets to be properly forwarded to the internet.
upvoted 1 times

 **chris_spencer** 1 year, 2 months ago

With A i am missing the route to the internet via a NAT Gateway or NAT Instance via a ENI, with D i miss the scr/dst check
upvoted 2 times

 **ahrentom** 1 year, 3 months ago

Selected Answer: D

"the company deploys a set of Amazon EC2 instances in private subnets to serve as transparent proxies." How could a Proxy in a private Subnet communicate with the Internet? So we need a second network card with connection to an IGW. Anwser D

upvoted 2 times

 **Russs99** 1 year, 8 months ago

Selected Answer: D

While disabling security checks might seem like a solution, it's not recommended for production environments as it weakens security. The issue lies in routing, not security

upvoted 2 times

 **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: A

Answer is A, proxy

upvoted 1 times

 **HunkkBunky** 1 year, 10 months ago

Selected Answer: A

Answer is - A

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

Correct Answer is A

upvoted 3 times

Question #435

A company is running its solution on AWS in a manually created VPC. The company is using AWS CloudFormation to provision other parts of the infrastructure. According to a new requirement, the company must manage all infrastructure in an automatic way.

What should the company do to meet this new requirement with the LEAST effort?

- A. Create a new AWS Cloud Development Kit (AWS CDK) stack that strictly provisions the existing VPC resources and configuration. Use AWS CDK to import the VPC into the stack and to manage the VPC.
- B. Create a CloudFormation stack set that creates the VPC. Use the stack set to import the VPC into the stack.
- C. Create a new CloudFormation template that strictly provisions the existing VPC resources and configuration. From the CloudFormation console, create a new stack by importing the Existing resources.
- D. Create a new CloudFormation template that creates the VPC. Use the AWS Serverless Application Model (AWS SAM) CLI to import the VPC.

Correct Answer: C*Community vote distribution*

C (82%)

Other

 **saggy4** Highly Voted 1 year, 10 months ago

Selected Answer: C

D - SAM cannot be used for importing and currently we are already using CloudFormation
 B - Stacksets are used to create multiple stacks and currently we are using CloudFormation
 A - CDK, we will need to change all the entire stack from CloudFormation to CDK
 C - We can import existing resources in CloudFormation: <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/resource-import.html>
 upvoted 10 times

 **Soliner_Bilgi_Teknolojileri** Most Recent 3 months, 3 weeks ago

Selected Answer: C

C is correct because CloudFormation has a built-in feature called resource import. This allows you to take an existing manually created VPC and import it into a CloudFormation stack, so it becomes managed automatically without having to rebuild or recreate resources.
 upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option C provides a straightforward way to manage the existing infrastructure in an automatic way with minimal effort.
 upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: C

"Use the stack set to import the VPC into the stack."
 CloudFormation stack sets are designed for deploying stacks across multiple accounts and regions. They are NOT meant for importing existing resources into a single VPC or stack.
 upvoted 2 times

 **titi_r** 1 year, 8 months ago

Selected Answer: C

C - correct.
 upvoted 2 times

 **titi_r** 1 year, 8 months ago

Selected Answer: C

C - correct.
 upvoted 2 times

 **VerRi** 1 year, 9 months ago

Selected Answer: C

B means to create a stack set just for VPC, we don't need a stack set to handle just 1 resource
 upvoted 3 times

 **career360guru** 1 year, 9 months ago

Selected Answer: B

Option B
 upvoted 1 times

✉️  **marszalekm** 1 year, 10 months ago

Selected Answer: C

I discarded B, because IMO stack sets are not needed.

upvoted 3 times

✉️  **TheCloudGuruu** 1 year, 10 months ago

Selected Answer: B

Create a CloudFormation stack

upvoted 1 times

✉️  **arberod** 1 year, 10 months ago

Selected Answer: B

agree B

upvoted 1 times

✉️  **arberod** 1 year, 10 months ago

Changed to C

upvoted 1 times

✉️  **HunkyBunky** 1 year, 10 months ago

Selected Answer: C

I guess C

A - is out, because CDK not allow to import any exists resources

B - is out, because StackSets are used only for create multiple stacks and manage them from a single stack

D - is out, because AWS SAM cli - can't be used for import resources in CF

upvoted 4 times

✉️  **kejam** 1 year, 10 months ago

Selected Answer: B

Answer B: Because CloudFormation is already in use.

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

upvoted 2 times

✉️  **kejam** 1 year, 10 months ago

Selected Answer: A

Answer A:

<https://aws.amazon.com/blogs/devops/how-to-import-existing-resources-into-aws-cdk-stacks/>

<https://docs.aws.amazon.com/cdk/v2/guide/cli.html#cli-import>

upvoted 1 times

✉️  **kejam** 1 year, 10 months ago

Changing my answer to B:

Answer B: Because CloudFormation is already in use.

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

upvoted 1 times

✉️  **alexis123456** 1 year, 10 months ago

Correct Answer is B

upvoted 2 times

Question #436

Topic 1

A company has developed a new release of a popular video game and wants to make it available for public download. The new release package is approximately 5 GB in size. The company provides downloads for existing releases from a Linux-based, publicly facing FTP site hosted in an on-premises data center. The company expects the new release will be downloaded by users worldwide. The company wants a solution that provides improved download performance and low transfer costs, regardless of a user's location.

- A. Store the game files on Amazon EBS volumes mounted on Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
- B. Store the game files on Amazon EFS volumes that are attached to Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on each of the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
- C. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Use Amazon CloudFront for the website. Publish the game download URL for users to download the package.
- D. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Set Requester Pays for the S3 bucket. Publish the game download URL for users to download the package.

Correct Answer: C*Community vote distribution*

C (100%)

  **AzureDP900** 1 year, 1 month ago

Option C provides a scalable, secure, and cost-effective solution for serving the game files worldwide.
Here's why:

- Amazon Route 53: Provides fast and reliable DNS resolution for users to access the game files.
- Amazon S3 bucket: Stores the game files in a highly available and durable storage system. Upload the game files (5 GB) to the S3 bucket, which will be charged at the standard rate (approximately \$0.023 per GB).
- Amazon CloudFront: A content delivery network (CDN) that caches frequently accessed resources like the game files. This reduces the latency experienced by users worldwide and provides better download performance.

upvoted 3 times

  **career360guru** 1 year, 9 months ago**Selected Answer: C**

Option C

upvoted 2 times

  **TheCloudGuruu** 1 year, 10 months ago**Selected Answer: C**

C. S3 is the best option, no need for requestor pays

upvoted 2 times

  **arberod** 1 year, 10 months ago**Selected Answer: C**

It is C

upvoted 2 times

  **kejam** 1 year, 10 months ago**Selected Answer: C**

Answer C:

upvoted 2 times

  **alexis123456** 1 year, 10 months ago

Correct Answer is C

upvoted 2 times

Question #437

A company runs an application in the cloud that consists of a database and a website. Users can post data to the website, have the data processed, and have the data sent back to them in an email. Data is stored in a MySQL database running on an Amazon EC2 instance. The database is running in a VPC with two private subnets. The website is running on Apache Tomcat in a single EC2 instance in a different VPC with one public subnet. There is a single VPC peering connection between the database and website VPC.

The website has suffered several outages during the last month due to high traffic.

Which actions should a solutions architect take to increase the reliability of the application? (Choose three.)

- A. Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer.
- B. Provision an additional VPC peering connection.
- C. Migrate the MySQL database to Amazon Aurora with one Aurora Replica.
- D. Provision two NAT gateways in the database VPC.
- E. Move the Tomcat server to the database VPC.
- F. Create an additional public subnet in a different Availability Zone in the website VPC.

Correct Answer: ACF

Community vote distribution

ACF (100%)

 **kejam** Highly Voted 1 year, 10 months ago

Selected Answer: ACF

Answer: ACF

These increase reliability of the app.

F. Create an additional public subnet in a different Availability Zone in the website VPC.

A. Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer.

C. Migrate the MySQL database to Amazon Aurora with one Aurora Replica.

These do not.

B. Provision an additional VPC peering connection.

D. Provision two NAT gateways in the database VPC.

E. Move the Tomcat server to the database VPC. (good idea for security, but we're after reliability)

upvoted 8 times

 **AzureDP900** Most Recent 1 year, 1 month ago

ACF

These three options improve the reliability and scalability of the application by:

Reducing the likelihood of single points of failure

Improving data availability and durability

Providing an additional layer of redundancy

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: ACF

Option A, C, F

upvoted 1 times

 **sat2008** 1 year, 10 months ago

Selected Answer: ACF

You cant move Ec2 directly to another VPC need to migrate between VPCs

upvoted 2 times

 **arberod** 1 year, 10 months ago

Selected Answer: ACF

agree ACF

upvoted 2 times

 **HunkBunk** 1 year, 10 months ago

Selected Answer: ACF

B - not correct, because will not give us any benefit

D - not correct, because will not give us any benefit

E - looks not correct, because if we move website into database VPC - this VPC don't contains any public subnet, so it will be inaccessible
upvoted 2 times

 **alexis123456** 1 year, 10 months ago

correct answer is ACF

upvoted 4 times

Question #438

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

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

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

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

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

Correct Answer: AE

Community vote distribution

AE (100%)

 **pangchn** Highly Voted 1 year, 9 months ago

Selected Answer: AE

same question as page1 question 10

upvoted 7 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Option A allows for a simple and quick solution by hosting a custom error page on Amazon S3. No changes are required to Route 53, CloudFront, or the ALB.

Option E uses CloudFront to display a custom error page without modifying any other resources.

Both options A and E meet the requirement with minimal operational overhead, so choosing both of them is correct!

upvoted 1 times

 **career360guru** 1 year, 9 months ago

Selected Answer: AE

A and E

upvoted 1 times

 **arberod** 1 year, 10 months ago

Selected Answer: AE

it is AE

upvoted 2 times

 **kejam** 1 year, 10 months ago

Selected Answer: AE

Answer: AE

All other answers won't help for transient failures

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

upvoted 3 times

 **master9** 1 year, 10 months ago

Selected Answer: AE

answer is A and E

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

correct answer is A and E

upvoted 3 times

 **duriselvan** 1 year, 10 months ago

A,B, ans

upvoted 1 times

Question #439

Topic 1

A company wants to migrate an Amazon Aurora MySQL DB cluster from an existing AWS account to a new AWS account in the same AWS Region. Both accounts are members of the same organization in AWS Organizations.

The company must minimize database service interruption before the company performs DNS cutover to the new database.

Which migration strategy will meet this requirement? (Choose two.)

- A. Take a snapshot of the existing Aurora database. Share the snapshot with the new AWS account. Create an Aurora DB cluster in the new account from the snapshot.
- B. Create an Aurora DB cluster in the new AWS account. Use AWS Database Migration Service (AWS DMS) to migrate data between the two Aurora DB clusters.
- C. Use AWS Backup to share an Aurora database backup from the existing AWS account to the new AWS account. Create an Aurora DB cluster in the new AWS account from the snapshot.
- D. Create an Aurora DB cluster in the new AWS account. Use AWS Application Migration Service to migrate data between the two Aurora DB clusters.

Correct Answer: AB*Community vote distribution*

AB (71%)

B (29%)

 **juanife** 10 months, 2 weeks ago

Selected Answer: AB

I do not know why AWS writes its questions so badly. The question asks for a conjunction answer and then they give us TOTALLY different answers that do not work together. For me, it's B without any doubts since AWS DMS allows us to migrate while reducing the interruption on the source to be migrated and A could be an option as well but it obviously allows us to move certain amount of data until a certain point of time.

upvoted 1 times

 **GabrielShiao** 11 months ago

Selected Answer: AB

The only correct answer is B, Selecting A is to meet the question. A is not right because it will lose a certain period of data.

upvoted 2 times

 **trungtd** 1 year, 6 months ago

Selected Answer: B

A is unnecessary

upvoted 2 times

 **Dgix** 1 year, 9 months ago

Selected Answer: AB

The question says to choose two alternatives - but it doesn't say that they must work in conjunction. I.e., separate answers that stand on their own.

B is best, but A works too. Thus A+B.

upvoted 2 times

 **career360guru** 1 year, 9 months ago

Selected Answer: AB

A and B both are valid options.

upvoted 1 times

 **bjexamprep** 1 year, 9 months ago

Selected Answer: B

This question should have a single answer. A and C are both using a kind of back/restore strategy, and they cannot capture the changes happens during the restore stage. D is using Application Migration Service, which is not suitable for DB migration. Only B can do this job.

upvoted 3 times

 **07c2d2a** 1 year, 10 months ago

This really should be a single answer, or it should say which solutions would meet this requirement. But yes A and B are both possible.

upvoted 1 times

 **HunkBunk** 1 year, 10 months ago

Selected Answer: AB

I guess that the right answer - A \ B

A - Snapshots can be easily shared cross AWS accounts

B - With AWS DMS - you can sync databases

C - Out because - as I understood - you can't just SHARE AWS Backup with another AWS Account, you need to setup cross account AWS backup to store backups in both accounts

D - Out because AWS Application migration service - can't migrate RDS databases

upvoted 3 times

 **kejam** 1 year, 10 months ago

Selected Answer: AB

Answer AB: A is unnecessary, we really only need B. It works either way.

<https://aws.amazon.com/blogs/database/cross-account-amazon-aurora-postgresql-and-amazon-rds-for-postgresql-migration-with-reduced-downtime-using-aws-dms/>

upvoted 2 times

 **master9** 1 year, 10 months ago

Selected Answer: AB

have to us DMS or snapshot for DB migration

upvoted 1 times

 **alexis123456** 1 year, 10 months ago

correct answer is A and B

upvoted 3 times

Question #440

Topic 1

A software as a service (SaaS) company provides a media software solution to customers. The solution is hosted on 50 VPCs across various AWS Regions and AWS accounts. One of the VPCs is designated as a management VPC. The compute resources in the VPCs work independently.

The company has developed a new feature that requires all 50 VPCs to be able to communicate with each other. The new feature also requires one-way access from each customer's VPC to the company's management VPC. The management VPC hosts a compute resource that validates licenses for the media software solution.

The number of VPCs that the company will use to host the solution will continue to increase as the solution grows.

Which combination of steps will provide the required VPC connectivity with the LEAST operational overhead? (Choose two.)

- A. Create a transit gateway. Attach all the company's VPCs and relevant subnets to the transit gateway.
- B. Create VPC peering connections between all the company's VPCs.
- C. Create a Network Load Balancer (NLB) that points to the compute resource for license validation. Create an AWS PrivateLink endpoint service that is available to each customer's VPC. Associate the endpoint service with the NLB.
- D. Create a VPN appliance in each customer's VPC. Connect the company's management VPC to each customer's VPC by using AWS Site-to-Site VPN.
- E. Create a VPC peering connection between the company's management VPC and each customer's VPC.

Correct Answer: AC

Community vote distribution

AC (68%)	BC (26%)	5%
----------	----------	----

 **Malluchan** 3 months, 1 week ago

Selected Answer: AC

A. Transit Gateway as the hub — attach all tenant/customer VPCs and the company's VPCs to a single Transit Gateway. This gives transitive, managed routing between all VPCs so you don't need an N^2 mesh of peering connections as you scale. It centralizes route management and scales to many VPCs with minimal per-VPC effort.

C, PrivateLink (NLB → endpoint service) from management VPC — publish the license-validation service in the management VPC behind a Network Load Balancer and create an AWS PrivateLink endpoint service. Each customer's VPC creates an interface endpoint to that service; traffic flows from the customer VPC → local interface endpoint → AWS backbone → NLB in the management VPC. This gives exactly the required one-way, service-only access (consumers cannot initiate general VPC-to-VPC traffic) and it's cross-account friendly.
upvoted 1 times

 **Spike2020** 1 year ago

Selected Answer: BC

Private link for the customers and vpc peering for company VPCs. Transit gateway is only a regional construct.

upvoted 2 times

 **nimbus_00** 1 year ago

Selected Answer: AC

AWS PrivateLink now supports cross-region connectivity

<https://aws.amazon.com/about-aws/whats-new/2024/11/aws-privatelink-across-region-connectivity/>

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: AC

A. Create a transit gateway. Attach all the company's VPCs to it, establishing a mesh network where VPCs can communicate. This provides a scalable way to manage VPC connectivity, reducing operational overhead compared to VPC peering.

C. Create a Network Load Balancer (NLB) for the license validation compute resource. Create an AWS PrivateLink endpoint service associated with the NLB, available to each customer's VPC. This provides one-way access from customer VPCs to the management VPC for license validation, without internet gateways, NAT gateways, or VPNs. It simplifies network configuration and reduces operational overhead.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: AC

AWS Transit Gateway supports peering between transit gateways in different regions. This means that you can connect a Transit Gateway in one region to another Transit Gateway in a different region. This feature is known as Transit Gateway Peering (not VPC peering). AWS Transit Gateway also allows you to associate VPCs from different AWS accounts to the same transit gateway using AWS Resource Access Manager (RAM)

upvoted 2 times

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

AAAAAAAAAAACCCCCCCC

upvoted 2 times

✉ **ca5e9ba** 1 year, 7 months ago

AC; AWS Transit Gateway allows you to connect resources across different AWS regions. Here's how you can achieve this:

Create Transit Gateways:

Begin by creating Transit Gateways in the respective regions where you want to establish peering.

Ensure that the necessary VPCs are attached to each Transit Gateway.

Enable Peering:

Navigate to the AWS Management Console and select the Transit Gateway service.

Initiate the peering connection between the two Transit Gateways in different regions.

Update Route Tables:

Configure the route tables associated with each Transit Gateway to allow traffic between the regions.

Security Groups and Network ACLs:

Adjust security groups and network ACLs to permit the necessary traffic flow.

Connectivity Testing:

Verify connectivity by testing communication between resources in different regions.

upvoted 4 times

✉ **teo2157** 1 year, 7 months ago

Selected Answer: BC

As titi_r explained

upvoted 1 times

✉ **titi_r** 1 year, 8 months ago

Selected Answer: BC

B – Correct, even that it will be a routing madness. The default VPC peering quota is 50, but increaseable after request to 125. So, the company will be able to peer its 50 VPCs, but it must request a quota increase for a higher number - that's not mentioned in the answer. And also what's happening when/if they require more than 125 VPCs at one point?

<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-connection-quotas.html>

C – Correct. The PrivateLink endpoint service will provide a one-way access from each customer's VPC to the company's management VPC.

<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/use-case-examples.html>

upvoted 2 times

✉ **titi_r** 1 year, 8 months ago

A – Incorrect. It's not possible to attach a VPC from one Region to a TGW in another Region. You can only attach a VPC to a TGW in the same Region; additionally you can peer that TGW with another one, located in a different Region.

<https://content.cloudthat.com/resources/wp-content/uploads/2022/11/Picture220.png>

upvoted 3 times

✉ **titi_r** 1 year, 8 months ago

D – Incorrect. Unknown if even possible, but more COMPLEX than answer "B" anyway. The default Site-to-Site VPN connections per VGW quota is only 10 (it's increaseable, but the actual limit is not stated in the AWS documentation), however the company will need more than 50 and this sounds unrealistic. The default Site-to-Site VPN connections per Region quota is 50 – it will also require a request for quota increase.

<https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-limits.html>

E – Incorrect. In this case customer VPCs will not be able to communicate with each other, but only with the management VPC.

upvoted 1 times

✉ **backbencher2022** 1 year, 4 months ago

Transit Gateway allows both inter-region and intra-region VPC peering as per this AWS document -

<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering.html#:~:text=AWS%20Region%20considerations-,Transit%20gateway%20peering%20attachments%20in%20Amazon%20VPC%20Transit%20Gateways,and%20specify%20a%20transit%20gateway.>

upvoted 3 times

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

Creating a transit gateway peering allows VPCs in different regions to connect.

upvoted 2 times

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

"The number of VPCs that the company will use to host the solution will continue to increase as the solution grows" - it can go beyond 125 as well

upvoted 2 times

✉ **trap** 1 year, 8 months ago

It SHOULD be transit gateway but it isn't. The VPCs are hosted in several accounts and regions. You can't attach all VPCs in one transit gateway. You need several peered transit gws per region which is not the case here. Correct: B,C

upvoted 4 times

✉️ **trap** 1 year, 8 months ago

Actually you need a transit gw per VPC region and they must be peered.....

Very tricky question... Correct: B,C

upvoted 3 times

✉️ **Russ99** 1 year, 8 months ago

Selected Answer: AE

NLB and PrivateLink offer benefits, they are overkill for this scenario. NLB is for distributing traffic across multiple instances, which isn't necessary here. PrivateLink creates a private connection for a service within a VPC, but it's a more complex solution than a simple peering connection for the management VPC.

upvoted 1 times

✉️ **career360guru** 1 year, 9 months ago

Selected Answer: AC

A and C

upvoted 2 times

✉️ **arberod** 1 year, 10 months ago

Selected Answer: AC

answer AC

upvoted 3 times

✉️ **kejam** 1 year, 10 months ago

Selected Answer: AC

Answer AC:

Transit Gateway and Private Link for the WIN!

upvoted 3 times

✉️ **alexis123456** 1 year, 10 months ago

Correct Answer A and C

upvoted 4 times

Question #441

A company has multiple lines of business (LOBs) that roll up to the parent company. The company has asked its solutions architect to develop a solution with the following requirements:

- Produce a single AWS invoice for all of the AWS accounts used by its LOBs.
- The costs for each LOB account should be broken out on the invoice.
- Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy.
- Each LOB account should be delegated full administrator permissions, regardless of the governance policy.

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

- A. Use AWS Organizations to create an organization in the parent account for each LOB. Then invite each LOB account to the appropriate organization.
- B. Use AWS Organizations to create a single organization in the parent account. Then, invite each LOB's AWS account to join the organization.
- C. Implement service quotas to define the services and features that are permitted and apply the quotas to each LOB, as appropriate.
- D. Create an SCP that allows only approved services and features, then apply the policy to the LOB accounts.
- E. Enable consolidated billing in the parent account's billing console and link the LOB accounts.

Correct Answer: BD*Community vote distribution*

BD (63%)	BE (30%)	4%
----------	----------	----

 **7f6aef3** Highly Voted 1 year, 7 months ago

Selected Answer: BD

E: Is wrong --> Consolidated billing is already enabled by default when you create an organization

B: obvious

D: since there are no OUs, I assume that the SCP applies to each LOB account

upvoted 15 times

 **chelbsik** Highly Voted 1 year, 10 months ago

Selected Answer: BE

I choose BE

D conflicts with the last requirement

upvoted 8 times

 **e4bc18e** 1 year, 7 months ago

D does not conflict, they can be full administrators in their accounts but not have access to all services, one does not conflict with the other

upvoted 3 times

 **juanife** 1 year, 7 months ago

I agree with you on that point

upvoted 1 times

 **a178080** Most Recent 4 months, 2 weeks ago

Selected Answer: D

pls help me understand, why not A instead of B?

The costs for each LOB account should be broken out on the invoice

upvoted 1 times

 **studybuddy12** 6 months, 3 weeks ago

Selected Answer: BD

Note - By default, the organization is created with all features enabled. You can also create the organization with only consolidated billing features enabled.

upvoted 2 times

 **studybuddy12** 6 months, 3 weeks ago

Selected Answer: BC

"Note

By default, the organization is created with all features enabled. You can also create the organization with only consolidated billing features enabled."

upvoted 1 times

 **jimee11** 7 months, 1 week ago

Selected Answer: BD

The answer should be B, D, and E.

upvoted 2 times

 **jimee11** 7 months, 1 week ago

CORRECTION: B and D. Consolidated Billing done for you.

upvoted 1 times

 **874def1** 8 months, 2 weeks ago

Selected Answer: BD

Can someone confirm if C is completely wrong? I dont think service quotas can be used to limit the usage of services in an account under an organization?

upvoted 2 times

 **PSPaul** 12 months ago

Selected Answer: BD

This is a very interesting question. While the answer appears to be B + D, the solution could be further enhanced by including option E.

However, given the question's emphasis on restricting services within each Line of Business (LOB), B + D likely represents the most suitable choice.

upvoted 2 times

 **PSPaul** 12 months ago

Selected Answer: BD

It should be B and D

But it's not really true. To have B + D +E together is perfect

To response this question BD is would be ok

upvoted 2 times

 **pk0619** 1 year ago

Selected Answer: AD

If we choose E are we saying that we only enable Consolidated billing feature of Organization and not all features. Because then we cannot even use SCP ?

D is not entirely correct as well - SCP are there to Deny and set perimeter, instead of allowing

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: BD

B. Use AWS Organizations to create a single organization in the parent account and invite each LOB's AWS account to join. This allows: - Producing a single invoice for all accounts (consolidated billing). - Breaking out costs for each LOB account. - Delegating full administrator permissions to LOB accounts (through SCPs).

D. Create an SCP that allows only approved services and features based on the governance policy, and apply it to the LOB accounts. SCPs in AWS Organizations define rules for what services and resources can be used in member accounts. This restricts available services and features for LOB accounts while allowing full administrator permissions within defined boundaries.

upvoted 2 times

 **tgv** 1 year, 4 months ago

Selected Answer: BD

B D

D is required for governance

upvoted 2 times

 **zolthar_z** 1 year, 4 months ago

For SAP 01 version D and E were in the same option, so the answer is B - D+E

upvoted 2 times

 **trungtd** 1 year, 6 months ago

Selected Answer: BD

B D because Consolidated billing is already enabled by default when you create an organization

upvoted 2 times

 **naylinu** 1 year, 7 months ago

It should chose 3 A + E . And D is require for governance

upvoted 1 times

 **naylinu** 1 year, 7 months ago

Sorry B + E . And D is require for governance

upvoted 2 times

 **teo2157** 1 year, 7 months ago

Selected Answer: BE

We have to read carefully the question, it says "Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy.", Organizations itself provide that ability but the question is not saying anything about to apply SCPs immediately to the OUs but just to have that ability. So for me D is discarded due to that.

upvoted 4 times

 **seetpt** 1 year, 7 months ago

Selected Answer: BE

BE for me

upvoted 2 times

Question #442

A solutions architect has deployed a web application that serves users across two AWS Regions under a custom domain. The application uses Amazon Route 53 latency-based routing. The solutions architect has associated weighted record sets with a pair of web servers in separate Availability Zones for each Region.

The solutions architect runs a disaster recovery scenario. When all the web servers in one Region are stopped, Route 53 does not automatically redirect users to the other Region.

Which of the following are possible root causes of this issue? (Choose two.)

- A. The weight for the Region where the web servers were stopped is higher than the weight for the other Region.
- B. One of the web servers in the secondary Region did not pass its HTTP health check.
- C. Latency resource record sets cannot be used in combination with weighted resource record sets.
- D. The setting to evaluate target health is not turned on for the latency alias resource record set that is associated with the domain in the Region where the web servers were stopped.
- E. An HTTP health check has not been set up for one or more of the weighted resource record sets associated with the stopped web servers.

Correct Answer: DE

Community vote distribution

DE (100%)

 **0b43291** 1 year, 1 month ago

D. The "Evaluate Target Health" setting is not enabled for the latency alias record set associated with the stopped Region. When using latency routing, this setting must be enabled so Route 53 considers the health status of associated resources and stops routing traffic to unavailable servers.

E. HTTP health checks are not set up for one or more weighted record sets associated with the stopped web servers. Without health checks, Route 53 cannot detect unhealthy or unavailable servers and will continue routing traffic to them.

upvoted 3 times

 **trungtd** 1 year, 6 months ago

Selected Answer: DE

Route 53 latency-based routing does not inherently perform health checks. If a web server in one region goes down, Route 53 won't automatically redirect traffic to the other region unless health checks are properly configured and associated with your DNS records.

upvoted 4 times

 **career360guru** 1 year, 9 months ago

Selected Answer: DE

Option D and E

upvoted 1 times

 **Russs99** 1 year, 10 months ago

Selected Answer: DE

DE are the correct answers for the given scenario

upvoted 1 times

 **kejam** 1 year, 10 months ago

Selected Answer: DE

Answer DE:

An antique/classic question, answers are in a different order and wording slightly changed.

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

upvoted 4 times

 **alexis123456** 1 year, 10 months ago

Selected Answer: DE

correct answer is D an E

upvoted 2 times

Question #443

A flood monitoring agency has deployed more than 10,000 water-level monitoring sensors. Sensors send continuous data updates, and each update is less than 1 MB in size. The agency has a fleet of on-premises application servers. These servers receive updates from the sensors, convert the raw data into a human readable format, and write the results to an on-premises relational database server. Data analysts then use simple SQL queries to monitor the data.

The agency wants to increase overall application availability and reduce the effort that is required to perform maintenance tasks. These maintenance tasks, which include updates and patches to the application servers, cause downtime. While an application server is down, data is lost from sensors because the remaining servers cannot handle the entire workload.

The agency wants a solution that optimizes operational overhead and costs. A solutions architect recommends the use of AWS IoT Core to collect the sensor data.

What else should the solutions architect recommend to meet these requirements?

- A. Send the sensor data to Amazon Kinesis Data Firehose. Use an AWS Lambda function to read the Kinesis Data Firehose data, convert it to .csv format, and insert it into an Amazon Aurora MySQL DB instance. Instruct the data analysts to query the data directly from the DB instance.
- B. Send the sensor data to Amazon Kinesis Data Firehose. Use an AWS Lambda function to read the Kinesis Data Firehose data, convert it to Apache Parquet format, and save it to an Amazon S3 bucket. Instruct the data analysts to query the data by using Amazon Athena.
- C. Send the sensor data to an Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) application to convert the data to .csv format and store it in an Amazon S3 bucket. Import the data into an Amazon Aurora MySQL DB instance. Instruct the data analysts to query the data directly from the DB instance.
- D. Send the sensor data to an Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) application to convert the data to Apache Parquet format and store it in an Amazon S3 bucket. Instruct the data analysts to query the data by using Amazon Athena.

Correct Answer: B

Community vote distribution

B (70%)	A (16%)	14%
---------	---------	-----

 **CCMC** Highly Voted 1 year, 9 months ago

Selected Answer: B

Kinesis Data Firehose is well-suited for ingesting and processing streaming data at scale, such as the continuous updates from the water-level monitoring sensors. It can reliably capture and deliver data to various destinations, including S3, without requiring additional application code.

Storing the data in Apache Parquet format in S3 offers several benefits. Parquet is a columnar storage format optimized for analytics workloads, providing efficient compression and query performance. This format is suitable for data analysis and querying using tools like Athena.

Using AWS Lambda to transform the data from Kinesis Data Firehose into Parquet format reduces the maintenance effort associated with managing traditional servers. Lambda automatically scales with the incoming workload, ensuring continuous data processing without downtime.

upvoted 7 times

 **mifune** Highly Voted 1 year, 7 months ago

Selected Answer: B

Lambda functions integrates with Data Firehouse better than sending the data to Apache Flink and then implement a solution to transform the data into the Parquet Format to be sent to S3. From AWS Documentation: "With Amazon Managed Service for Apache Flink, you can use Java, Scala, Python, or SQL to process and analyze streaming data". So, Flink does not make any automatic data transformation. The correct option is B.

upvoted 5 times

 **dv1** Most Recent 1 year ago

Selected Answer: B

Managed service for apache flink cannot ingest streaming data directly. This means that anything flink is out. Best remaining answer is B.
upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: B

Option B is the most suitable solution as it leverages serverless and scalable services (Kinesis Data Firehose, Lambda, S3, and Athena) to handle data ingestion, transformation, and analysis with minimal operational overhead and optimized costs.

upvoted 1 times

 **sammyhaj** 1 year, 4 months ago

Selected Answer: A

It says convert to human readable, that isn't Parquet, its CSV

upvoted 3 times

 **altonh** 10 months, 1 week ago

KDF Aurora DB directly, and the lambda function that KDF invoked is for transformation only.

upvoted 1 times

 **altonh** 10 months, 1 week ago

KDF cannot directly write to Aurora DB, and the lambda function that KDF invoked is for transformation only.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

The statement does not say that it is necessary to continue storing the data in human readable form.

The statement says that the agency wants to increase overall application availability and reduce the effort that is required to perform maintenance tasks. These are the requirements.

upvoted 1 times

 **nileshlg** 1 year, 7 months ago

D seems to be the correct option as its a managed service

upvoted 3 times

 **seetpt** 1 year, 7 months ago

Selected Answer: B

B for me

upvoted 2 times

 **titi_r** 1 year, 8 months ago

Selected Answer: B

"B" seems to be the correct ans. Amazon Data Firehose can ingest data streams from IoT and convert them to into Parquet format using Lambda function. The destination of the stream can be S3.

<https://aws.amazon.com/firehose/>

<https://d1.awsstatic.com/pdp-how-it-works-assets/Product-Pate-Diagram-Amazon-Kinesis-Data-Firehose%402x.39ea068e48494676c0f4386535f85a966e9ac252.png>

upvoted 3 times

 **tushar321** 1 year, 8 months ago

D seems a better fit as Apache flink is a managed services for steaming as well as transformation. makes things simpler

upvoted 2 times

 **VerRi** 1 year, 8 months ago

Selected Answer: B

Both B and D are work.

B - KDF&Lambda for data transformation

D - KDA for real-time analysis

upvoted 4 times

 **Wilson_S** 1 year, 9 months ago

Selected Answer: D

Using a managed service for data transformation optimizes operational overhead.

upvoted 2 times

 **oayoade** 1 year, 9 months ago

Selected Answer: A

"human readable format", I go with CSV

upvoted 3 times

 **Russ99** 1 year, 9 months ago

Selected Answer: B

Although option D call work, it introduces unnecessary complexity for the given scenario.

upvoted 3 times

 **Dgix** 1 year, 9 months ago

Selected Answer: D

Answer is D.

upvoted 3 times

 **Sathya** 1 year, 9 months ago

Answer is D

upvoted 2 times

Question #444

A public retail web application uses an Application Load Balancer (ALB) in front of Amazon EC2 instances running across multiple Availability Zones (AZs) in a Region backed by an Amazon RDS MySQL Multi-AZ deployment. Target group health checks are configured to use HTTP and pointed at the product catalog page. Auto Scaling is configured to maintain the web fleet size based on the ALB health check.

Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated query response times.

Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? (Choose two.)

- A. Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.
- B. Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- C. Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- D. Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.
- E. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier.

Correct Answer: BE

Community vote distribution

BE (69%)	AB (19%)	6%
----------	----------	----

 **pangchn**  1 year, 8 months ago

Selected Answer: BE

My answer is a bit difference.
It doesn't mentioned read-only scnerio so read replica in A may not able to help
compare B and C, both pro and con. I lean to B from both the real world and in this particual question to bypass the database
upvoted 9 times

 **Capt_Leonidas**  1 year, 8 months ago

Selected Answer: BE

<https://www.examtopics.com/discussions/amazon/view/46826-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 8 times

 **Malluchan**  3 months, 1 week ago

Selected Answer: BE

Why not A - The non-Aurora RDS doesn't provide a single "reader endpoint" the way Aurora does
Why not C (TCP health checks) - TCP only confirms a port is open, not that the web server is healthy.
upvoted 1 times

 **EzKkk** 1 month ago

- I think A can be done using RDS proxy and the question didn't strictly enforce how this is done
 - E is not a good option since it only caches frequently accessed data which is not suitable for growth potential especially in retail domain where data changes very frequently
- upvoted 1 times

 **AI8282** 5 months, 1 week ago

Selected Answer: AB

I'll have to go against the grain and pick A & B. Reading from a read only node is best practices anyways. In cases where in the future we do want a independent caching layer which has additional overhead and cost, we should be reading from a reader node anyways. Reading from the main node to cache results itself can cause service issues due to putting on more load.

upvoted 1 times

 **eboehm** 2 weeks ago

single reader endpoints is an aurora thing... not for mysql RDS

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: BE

B and E works as expectation.
Due to web app is normal, A and C can not help
CloudWatch alarm can not support so complicated action
upvoted 1 times

 **michele_scar** 1 year, 6 months ago

Selected Answer: BE

When you talking about a product catalog page, you need to cache information (text, images) to leverage the load on the data tier.
ElastiCache is the solution (or a CDN).

upvoted 2 times

 **9f02c8d** 1 year, 7 months ago

A & E is correct answer as the monitoring aspect is not part of the problem statement
upvoted 1 times

 **red_panda** 1 year, 7 months ago

Selected Answer: AB

A and B are my answers.
A instead of E only because we have no tips that indicate the necessity to have a caching systems. For example, it say "high load on database", but nothing about same record read more time.
So for me A and B
upvoted 3 times

 **seetpt** 1 year, 7 months ago

Selected Answer: BE

BE for me
upvoted 3 times

 **titi_r** 1 year, 8 months ago

Selected Answer: BE

B and E.
upvoted 4 times

 **w3ap0nx** 1 year, 8 months ago

Selected Answer: BE

"for future growth" -> E (cache in front of the DB)
upvoted 5 times

 **ovladan** 1 year, 8 months ago

Selected Answer: BE
B: Will improve web app
D: Will improve database high load issue and query response times.
upvoted 4 times

 **VerRi** 1 year, 8 months ago

Selected Answer: AB

TCP check is like a heartbeat check, too rough.
upvoted 2 times

 **failexamonly** 1 year, 9 months ago

Selected Answer: AC

read replica to reduce load.
tcp check to see if ec2 is reachable
upvoted 2 times

 **AWSPro1234** 1 year, 9 months ago

I agree with A and B .
upvoted 2 times

 **Russ99** 1 year, 9 months ago

Selected Answer: A

A and B are my picks
upvoted 3 times

 **Dgix** 1 year, 9 months ago

By the way, ExamTopics, we get a 503 when submitting voting comments. Please change my previous submission to that type, specifying A and C.
upvoted 1 times

Question #445

A company has an on-premises data center and is using Kubernetes to develop a new solution on AWS. The company uses Amazon Elastic Kubernetes Service (Amazon EKS) clusters for its development and test environments.

The EKS control plane and data plane for production workloads must reside on premises. The company needs an AWS managed solution for Kubernetes management.

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

- A. Install an AWS Outposts server in the on-premises data center. Deploy Amazon EKS by using a local cluster configuration on the Outposts server for the production workloads.
- B. Install Amazon EKS Anywhere on the company's hardware in the on-premises data center. Deploy the production workloads on an EKS Anywhere cluster.
- C. Install an AWS Outposts server in the on-premises data center. Deploy Amazon EKS by using an extended cluster configuration on the Outposts server for the production workloads.
- D. Install an AWS Outposts server in the on-premises data center. Install Amazon EKS Anywhere on the Outposts server. Deploy the production workloads on an EKS Anywhere cluster.

Correct Answer: A*Community vote distribution*

A (80%)

14% 6%

 **pangchn**  1 year, 9 months ago

Selected Answer: A

A

3 things to consider fromr question requirement
 control plane location - onprem
 data plane location - onprem
 management - AWS
 EKS anywhere it managed by customer so BD out
<https://anywhere.eks.amazonaws.com/docs/concepts/eksafeatures/#comparing-amazon-eks-anywhere-to-amazon-eks>

Extended clusters – Run the Kubernetes control plane in an AWS Region and nodes on your Outpost.
 Local clusters – Run the Kubernetes control plane and nodes on your Outpost

<https://docs.aws.amazon.com/eks/latest/userguide/eks-deployment-options.html>
<https://docs.aws.amazon.com/eks/latest/userguide/eks-outposts.html>

upvoted 14 times

 **0b43291**  1 year, 1 month ago

Selected Answer: A

The correct answer is A. Install an AWS Outposts server in the on-premises data center. Deploy Amazon EKS by using a local cluster configuration on the Outposts server for the production workloads.

The key requirement is that the company needs an AWS managed solution for Kubernetes management. While EKS Anywhere provides a consistent Kubernetes experience with Amazon EKS, it is a self-managed solution where the customer is responsible for managing the underlying infrastructure and control plane.

On the other hand, AWS Outposts allows running AWS services, including Amazon EKS, on-premises. When deploying Amazon EKS on an Outposts server using a local cluster configuration, the EKS control plane and data plane reside on the Outposts server in your data center, meeting the requirement of having the production workloads on-premises.

Additionally, Amazon EKS on Outposts is fully managed by AWS, handling provisioning, upgrading, and lifecycle management of the Kubernetes control plane, providing the least operational overhead.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: A

With EKS LOCAL clusters on Outposts, you can run the Amazon EKS control plane and data plane entirely on the Outposts hardware on-premises. Also, it's an AWS managed solution.

upvoted 2 times

 **asquared16** 1 year, 4 months ago

Selected Answer: A

It's A, EKS Everywhere = Operational Overhead, and it said it needs to be managed by AWS
upvoted 1 times

luuthang2011 1 year, 4 months ago

B
Option A (AWS Outposts with local EKS cluster): While this can run EKS on premises, managing an AWS Outposts server and the associated EKS infrastructure might involve more overhead compared to EKS Anywhere.
Option C (AWS Outposts with extended EKS cluster): Similar to option A, this involves managing the Outposts server and integrating it with your on-premises environment, which could increase the complexity and operational overhead.
Option D (AWS Outposts with EKS Anywhere): This combines managing an Outposts server with deploying EKS Anywhere, which adds unnecessary complexity and overhead compared to deploying EKS Anywhere directly on the company's hardware.

upvoted 1 times

salekali01 1 year, 5 months ago

Selected Answer: B

EKS anywhere!!!

upvoted 1 times

JoeTromundo 1 year, 2 months ago

Can't be B. The company needs an AWS managed solution for Kubernetes management. EKS Anywhere is not an AWS managed solution. It's a self-managed solution.

upvoted 2 times

HelpnoseNse 1 year, 6 months ago

Selected Answer: A

Vote A because by using outpostM EKS is AWS managed service but running on local. Question require AWS managed solution for Kubernetes management. If EKS Anywhere with control plane on prem not AWS cloud, then it's self managed cluster.

upvoted 2 times

4bc91ae 1 year, 6 months ago

Selected Answer: A

A - Control Plane has to be on-prem (not case for Outpost)

upvoted 1 times

9f02c8d 1 year, 7 months ago

B - Correct. The requirement is to use on-premise hardware with AWS managed EKS that means EKS Anywhere which leverages on-premise hardware with full control over both the control plane and data plane

upvoted 2 times

titi_r 1 year, 8 months ago

Selected Answer: A

A - correct.

upvoted 1 times

TonytheTiger 1 year, 9 months ago

Option A: requirement is ask for AWS Managed Solution and AWS Outpost give you that option <https://docs.aws.amazon.com/managedservices/latest/userguide/outposts.html>

Not Option B : Unlike Amazon EKS in AWS Cloud, EKS Anywhere is a user-managed product that runs on user-managed infrastructure. You are responsible for cluster lifecycle operations and maintenance of your EKS Anywhere clusters.
<https://anywhere.eks.amazonaws.com/docs/overview/>

upvoted 2 times

failexamonly 1 year, 9 months ago

Selected Answer: A

<https://anywhere.eks.amazonaws.com/docs/concepts/eksafeatures/#:~:text=With%20Amazon%20EKS%20on%20Outposts,with%20EKS%20Anywhere%20automation%20tooling>.

upvoted 1 times

yog927 1 year, 9 months ago

Correct answer is A.

It is not C because EKS Anywhere cluster is a customer-managed product that runs on customer-managed infrastructure.

Ref: <https://aws.amazon.com/eks/eks-anywhere/faqs/>

upvoted 1 times

ahmadraufsyahputra 1 year, 9 months ago

Correct answer is A

You can use Amazon EKS to run on-premises Kubernetes applications on AWS Outposts. You can deploy Amazon EKS on Outposts in the following ways:

Extended clusters – Run the Kubernetes control plane in an AWS Region and nodes on your Outpost.

Local clusters – Run the Kubernetes control plane and nodes on your Outpost.

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

upvoted 2 times

 **gustori99** 1 year, 9 months ago

Selected Answer: A

The correct answer is A: when deploying EKS on an Outpost server in a local cluster configuration, the control plane and data plane reside on-premises, but the control plane is AWS-managed.

B is incorrect. Although for EKS-A, the control plane and data plane reside on-premises, it is not AWS-managed but completely customer-managed (both control plane and data plane).

C is incorrect because in an extended cluster configuration on AWS Outpost, the control plane runs inside the AWS cloud, not on the outpost server on-premises.

D is incorrect because you do not combine EKS-A and Outpost.

upvoted 3 times

 **k23319** 1 year, 9 months ago

Selected Answer: B

Answer is B. The requirement is that both control plane and data plane will reside on premise. If you deploy EKS using extended cluster the control plane lies within AWS region. You need a local cluster for the control plane to reside on outpost.

Please refer to url below.

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

upvoted 2 times

 **oayoade** 1 year, 9 months ago

Selected Answer: A

<https://docs.aws.amazon.com/eks/latest/userguide/eks-deployment-options.html>

upvoted 2 times

Question #446

A company uses AWS Organizations to manage its development environment. Each development team at the company has its own AWS account. Each account has a single VPC and CIDR blocks that do not overlap.

The company has an Amazon Aurora DB cluster in a shared services account. All the development teams need to work with live data from the DB cluster.

Which solution will provide the required connectivity to the DB cluster with the LEAST operational overhead?

- A. Create an AWS Resource Access Manager (AWS RAM) resource share for the DB cluster. Share the DB cluster with all the development accounts.
- B. Create a transit gateway in the shared services account. Create an AWS Resource Access Manager (AWS RAM) resource share for the transit gateway. Share the transit gateway with all the development accounts. Instruct the developers to accept the resource share. Configure networking.
- C. Create an Application Load Balancer (ALB) that points to the IP address of the DB cluster. Create an AWS PrivateLink endpoint service that uses the ALB. Add permissions to allow each development account to connect to the endpoint service.
- D. Create an AWS Site-to-Site VPN connection in the shared services account. Configure networking. Use AWS Marketplace VPN software in each development account to connect to the Site-to-Site VPN connection.

Correct Answer: B

Community vote distribution

B (82%)	Other
---------	-------

 matheusrdo Highly Voted 1 year, 8 months ago

Selected Answer: B

The question asks about working with live data and providing CONNECTIVITY to the DB cluster. B is the correct as it provides both upvoted 10 times

 pangchn Highly Voted 1 year, 8 months ago

Selected Answer: B

B
I originally chose A since I thought Aurora DB cluster is sharable
<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html#shareable-aur>
But as Verri mentioned, with that share, it only allows you to CLONE the db rather than use it as live
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Clone.html#Aurora.Managing.Clone.Cross-Account>
upvoted 9 times

 AzureDP900 Most Recent 1 year, 1 month ago

Creating a transit gateway (Option B) can be an effective way to provide connectivity to your Amazon Aurora DB cluster while minimizing operational overhead.
upvoted 1 times

 vip2 1 year, 5 months ago

Selected Answer: B

for live data, it should be B
upvoted 1 times

 red_panda 1 year, 7 months ago

Selected Answer: A

For me it's A.
We need to use the RAM only for the Aurora DB. We don't need to peer the VPCs with TransitGateway. Also less ops effort is option A. So Option B is unuseful complicated.
upvoted 1 times

 titi_r 1 year, 8 months ago

Selected Answer: B

Correct ans "B".
upvoted 3 times

 spencer_sharp 1 year, 9 months ago

Selected Answer: A

Seemed A since B requires a lot setup work

upvoted 1 times

 **mav3r1ck** 1 year, 9 months ago

Selected Answer: A

LEAST operational overhead is "A".

You can share DB Cluster. <https://docs.aws.amazon.com/ram/latest/userguide/shareable.html#shareable-aur>

upvoted 1 times

 **c22ddd8** 1 year, 5 months ago

Live data is catch here, A is for clone

upvoted 1 times

 **VerRi** 1 year, 9 months ago

Selected Answer: B

A: Sharing DB cluster with RAM allows you to CLONE a shared, centrally managed DB cluster

C: PrivateLink needs NLB not ALB

D: WTF

upvoted 8 times

 **pangchn** 1 year, 9 months ago

Selected Answer: A

I will go for A as the ref link provided by JOKERO
if not, the transit gateway would be ideal too.

upvoted 1 times

 **c22ddd8** 1 year, 5 months ago

Live data is catch here, A is for clone

upvoted 1 times

 **gustori99** 1 year, 9 months ago

Selected Answer: B

C is wrong because for Private Link you need to use NLB not ALB.

Correct answer is B.

upvoted 5 times

 **JOKERO** 1 year, 9 months ago

Selected Answer: A

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html#shareable-aur>

upvoted 4 times

 **txxxxxf** 1 year, 9 months ago

Selected Answer: B

AWS PrivateLink requires an NLB (Network Load Balancer). Since the question mentions that IP addresses should not overlap, sharing via Transit Gateway might be a good approach.

upvoted 6 times

 **CMMC** 1 year, 9 months ago

Selected Answer: C

Utilizing AWS PrivateLink to enable private connectivity between VPCs without the need for public IP addresses or internet gateways. Creating an ALB pointing to the DB cluster's IP address and then creating a PrivateLink endpoint service that uses the ALB allows each development account to securely connect to the DB cluster. This approach minimizes operational overhead and simplifies network connectivity.

upvoted 1 times

Question #447

Topic 1

A company used AWS CloudFormation to create all new infrastructure in its AWS member accounts. The resources rarely change and are properly sized for the expected load. The monthly AWS bill is consistent.

Occasionally, a developer creates a new resource for testing and forgets to remove the resource when the test is complete. Most of these tests last a few days before the resources are no longer needed.

The company wants to automate the process of finding unused resources. A solutions architect needs to design a solution that determines whether the cost in the AWS bill is increasing. The solution must help identify resources that cause an increase in cost and must automatically notify the company's operations team.

Which solution will meet these requirements?

- A. Turn on billing alerts. Use AWS Cost Explorer to determine the costs for the past month. Create an Amazon CloudWatch alarm for total estimated charges. Specify a cost threshold that is higher than the costs that Cost Explorer determined. Add a notification to alert the operations team if the alarm threshold is breached.
- B. Turn on billing alerts. Use AWS Cost Explorer to determine the average monthly costs for the past 3 months. Create an Amazon CloudWatch alarm for total estimated charges. Specify a cost threshold that is higher than the costs that Cost Explorer determined. Add a notification to alert the operations team if the alarm threshold is breached.
- C. Use AWS Cost Anomaly Detection to create a cost monitor that has a monitor type of Linked account. Create a subscription to send daily AWS cost summaries to the operations team. Specify a threshold for cost variance.
- D. Use AWS Cost Anomaly Detection to create a cost monitor that has a monitor type of AWS services. Create a subscription to send daily AWS cost summaries to the operations team. Specify a threshold for cost variance.

Correct Answer: D

Community vote distribution

D (79%)

C (21%)

 **titi_r**  1 year, 8 months ago

Selected Answer: D

Ans "D" - more granular.

Q: What is the difference between a linked account monitor in a payer account, and a services monitor in a linked account?

A linked account monitor in a payer account will monitor the spend of all services, in total, for that linked account.

A services monitor in a linked account will monitor the individual spend for each service for that linked account.

For example, if there is a spike in S3 spending, but a dip in EC2 spending of the same amount (net neutral change), the linked account monitor in the payer account will not detect this because it is monitoring the total account spend across all services. However, the services monitor in the linked account would detect the S3 spike since it is monitoring each service spend individually.

upvoted 14 times

 **titi_r** 1 year, 8 months ago

<https://aws.amazon.com/aws-cost-management/aws-cost-anomaly-detection/faqs/#:~:text=What%20is%20the%20difference%20between%20a%20linked%20account%20monitor%20in%20a%20payer%20account,%20and%20a%20services%20monitor%20in%20a%20linked%20account>

upvoted 1 times

 **sarlos** 1 year, 7 months ago

Thanks for the explanation

upvoted 2 times

 **Dgix**  1 year, 9 months ago

Selected Answer: D

On reconsideration: D, as it deals with the individual services in an account, not just the total cost.

upvoted 5 times

 **Soliner_Bilgi_Teknolojileri**  3 months, 3 weeks ago

Selected Answer: D

AWS Cost Anomaly Detection with "AWS Services" monitor type uses machine learning to automatically detect unusual spending patterns and identifies exactly which service (EC2, RDS, etc.) is causing cost increases - perfect for catching forgotten test resources.

CloudWatch billing alarms (A&B) only show total cost increases but can't identify which specific resources caused the spike, while option C only monitors at account level without service-level detail.

upvoted 1 times

 **Denizka** 4 months, 1 week ago

Selected Answer: C

AWS Cost Anomaly Detection is purpose-built to spot unexpected cost increases automatically and notify teams. Creating a cost monitor with monitor type = Linked account lets you detect anomalies at the account level (useful for a multi-account Organization where developers create test resources). It will automatically surface anomalous cost spikes and you can subscribe the operations team (via SNS/email) to receive alerts and daily summaries. Once alerted, Cost Explorer and the Cost & Usage Report (CUR) can be used to drill down to the specific service, resource IDs, and tags that caused the spike so the operations team can identify and remove unneeded test resources.

upvoted 1 times

 **Ob43291** 1 year, 1 month ago

Selected Answer: D

By creating a cost monitor with the monitor type set to "AWS services," Cost Anomaly Detection will monitor the individual spend for each service within the linked account. This would allow the company to detect anomalies or spikes in spending for specific services, even if there is a corresponding decrease in another service that offsets the overall account spend.

Given the requirement to identify resources that cause an increase in cost, monitoring at the service level would provide more granular visibility and enable the company to pinpoint the specific services or resources responsible for cost increases.

Creating a subscription to send daily AWS cost summaries to the operations team and specifying a threshold for cost variance would ensure that the team is notified when the cost increase for any individual service exceeds the defined threshold.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Option D:

Using AWS Cost Anomaly Detection to create a cost monitor with a monitor type of AWS services: This option focuses on individual AWS services, making it easier to identify which specific resource is causing the increase in costs.

This approach provides detailed insights into each service's contribution to your company's overall expenses, making it easier to pinpoint the issue and take corrective action.

Considering all options, Option D seems to be the most suitable solution for identifying resources that cause an increase in costs and automatically notifying the company's operations team. This approach offers real-time monitoring, detailed insights into individual services' contributions, and automatic notifications when costs exceed specified thresholds.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: D

For those who think the correct answer is C: A Linked Account monitor detects anomalies at the account level. While it can identify which account has unusual spending, it does NOT pinpoint the SPECIFIC SERVICES or RESOURCES causing the increase, as the statement requires.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: D

"identify resources that cause an increase in cost "

D for sure

upvoted 1 times

 **salekali01** 1 year, 5 months ago

Selected Answer: C

Monitoring at the AWS service level can be useful, but it may not provide the same comprehensive view of costs across accounts as the linked account monitor type.

Therefore, option C provides a more adaptive and comprehensive solution for detecting cost anomalies and notifying the operations team.

upvoted 1 times

 **seetpt** 1 year, 7 months ago

Selected Answer: D

D for me

upvoted 1 times

 **tushar321** 1 year, 8 months ago

D.

An AWS service monitor will be applicable to all customers since it tracks and detects anomalies across any service they deploy
<https://aws.amazon.com/aws-cost-management/aws-cost-anomaly-detection/faqs/#:~:text=An%20AWS%20service%20monitor%20will%20be%20applicable%20to%20all%20customers%20since%20it%20tracks%20and%20detects%20anomalies%20across%20any%20service%20they%20deploy>

upvoted 1 times

 **thotwielder** 1 year, 8 months ago

Selected Answer: D

c: identify abnormal accounts

d: identify abnormal service, which is desired.

upvoted 3 times

 **pangchn** 1 year, 8 months ago

Selected Answer: D

vote D here

A linked account monitor can track up to 10 different linked accounts. A linked account monitor tracks spending aggregated across all of the designated linked accounts. For example, if a linked account monitor tracks Account A and Account B, and then Account A's usage spikes while Account B's usage dips by the same amount, there will be no anomaly detected because it is a net neutral change.

ref

<https://aws.amazon.com/aws-cost-management/aws-cost-anomaly-detection/faqs/>

upvoted 3 times

 **steed47** 1 year, 9 months ago

Selected Answer: C

C more granular

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

Selected Answer: C

Option C and Not Option D : Linked account - This monitor evaluates the total spend of an individual, or group of, member accounts. If your Organizations need to segment spend by team, product, services, or environment, this monitor is useful. The maximum number of member accounts that you can select for each monitor is 10.

<https://docs.aws.amazon.com/cost-management/latest/userguide/getting-started-ad.html#monitor-type-def>

upvoted 1 times

 **VerRi** 1 year, 9 months ago

Selected Answer: C

I will go with C because the scenario says, "to create all new infrastructure in its AWS member accounts."

upvoted 1 times

 **pangchn** 1 year, 9 months ago

Selected Answer: D

D seems more granular to detect which resource in which account generated the bill.

C seem only care about the balance across accounts as below

"linked account monitor can track up to 10 different linked accounts. A linked account monitor tracks spending aggregated across all of the designated linked accounts. For example, if a linked account monitor tracks Account A and Account B, and then Account A's usage spikes while Account B's usage dips by the same amount, there will be no anomaly detected because it is a net neutral change"

<https://aws.amazon.com/aws-cost-management/aws-cost-anomaly-detection/faqs/>

upvoted 4 times

Question #448

A company is deploying a new web-based application and needs a storage solution for the Linux application servers. The company wants to create a single location for updates to application data for all instances. The active dataset will be up to 100 GB in size. A solutions architect has determined that peak operations will occur for 3 hours daily and will require a total of 225 MiBps of read throughput.

The solutions architect must design a Multi-AZ solution that makes a copy of the data available in another AWS Region for disaster recovery (DR). The DR copy has an RPO of less than 1 hour.

Which solution will meet these requirements?

- A. Deploy a new Amazon Elastic File System (Amazon EFS) Multi-AZ file system. Configure the file system for 75 MiBps of provisioned throughput. Implement replication to a file system in the DR Region.
- B. Deploy a new Amazon FSx for Lustre file system. Configure Bursting Throughput mode for the file system. Use AWS Backup to back up the file system to the DR Region.
- C. Deploy a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume with 225 MiBps of throughput. Enable Multi-Attach for the EBS volume. Use AWS Elastic Disaster Recovery to replicate the EBS volume to the DR Region.
- D. Deploy an Amazon FSx for OpenZFS file system in both the production Region and the DR Region. Create an AWS DataSync scheduled task to replicate the data from the production file system to the DR file system every 10 minutes.

Correct Answer: A

Community vote distribution

A (60%)

D (40%)

 **e4bc18e** Highly Voted 1 year, 7 months ago

So practically everyone here is wrong. because it is A. Here is why B is wrong because one there is no such thing as bursting mode for Lustre that is an EFS thing, but also Backup will not work for the RPO. C is wrong obviously because GP3 can't be shared. D is wrong because Datasync tasks cannot be scheduled for any more frequent than hourly so no D is wrong because you cannot schedule data sync tasks less than hourly so you don't meet the RPO. So all of those are easily wrong because they have bad information. They fooled everyone on A because all they say is the 'Active working set is 100GB" not the entire filesystem. EFS accumulates bursting credits so for every 100GB of filesystem size you can burst up to 300MiBps for up to 72 minutes. So you provision 75MiBps because that would average out over time so you aren't being overcharged for the provisioned size.

upvoted 22 times

 **AzureDP900** 1 year, 1 month ago

I agree with your explanation, I will go with A

upvoted 1 times

 **pangchn** Highly Voted 1 year, 9 months ago

Selected Answer: D

D

a sneaky question since my first impression is go for A but it is wrong due to the 75M throughput mode. What's the calculation here? one region has 3 AZ? so $75 \times 3 = 225$? EFS is not provisioned in that way. Even that, the 225 is the total throughput where question asked 225 for read. Implied the total would be more like 225+XXX. Anyway, A is wrong.
<https://docs.aws.amazon.com/efs/latest/ug/performance.html>

C is wrong since EBS multi attach don't support gp3

<https://docs.aws.amazon.com/ebs/latest/userguide/ebs-volumes-multi.html>

upvoted 5 times

 **pangchn** 1 year, 9 months ago

B is wrong where the hourly AWS backup job won't meet the RPO requirement (less than 1 hour)

The backup frequency determines how often AWS Backup creates a snapshot backup. Using the console, you can choose a frequency of every hour, 12 hours, daily, weekly, or monthly. You can also create a cron expression that creates snapshot backups as frequently as hourly.
<https://docs.aws.amazon.com/aws-backup/latest/devguide/creating-a-backup-plan.html>

upvoted 3 times

 **aka1177** Most Recent 3 weeks, 6 days ago

Selected Answer: A

from all information here I would go with A.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: A

A scheduled task runs at a frequency that you specify, with a minimum interval of 1 hour.

<https://docs.aws.amazon.com/datasync/latest/userguide/task-scheduling.html>

upvoted 3 times

 **Helpnose** 1 year, 6 months ago

Selected Answer: A

A. EFS support cross region replication. e4bc18e already point why D is wrong.

upvoted 4 times

 **trungtd** 1 year, 6 months ago

Selected Answer: A

big thank to e4bc18e

upvoted 4 times

 **Zas1** 1 year, 7 months ago

Selected Answer: A

A

Solution write by e4bc18e

upvoted 3 times

 **titi_r** 1 year, 8 months ago

Selected Answer: D

D is correct.

"You can use DataSync to transfer files between two FSx for OpenZFS file systems, and also move data to a file system in a different AWS Region or AWS account. You can also use DataSync with FSx for OpenZFS file systems for other tasks. For example, you can perform one-time data migrations, periodically ingest data for distributed workloads, and schedule replication for data protection and recovery."

<https://docs.aws.amazon.com/fsx/latest/OpenZFSGuide/migrate-files-to-fsx-datasync.html>

upvoted 3 times

 **e4bc18e** 1 year, 7 months ago

This is wrong a DataSync task cannot be scheduled for any more frequent than one hour so the under 1 hour RPO is not met.

upvoted 2 times

 **titi_r** 1 year, 7 months ago

@e4bc18e, it seems you are right. Indeed, DataSync can go as granular as 1 hour.

Found this:

"If the file system's baseline throughput exceeds the Provisioned throughput amount, then it automatically uses the Bursting throughput..."

For 1 TiB of metered data in Standard storage, it can burst to 300 MiBps read-only for 12 hours per day.

<https://docs.aws.amazon.com/efs/latest/ug/performance.html#throughput-modes>

upvoted 1 times

 **ovladan** 1 year, 8 months ago

Selected Answer: B

<https://docs.aws.amazon.com/fsx/latest/LustreGuide/performance.html#fsx-aggregate-perf>

upvoted 1 times

 **titi_r** 1 year, 8 months ago

"B" is wrong because with AWS Backup you can do a backup as frequent as 1 hour, but the RPO must be less than 1 hour.

<https://docs.aws.amazon.com/aws-backup/latest/devguide/creating-a-backup-plan.html#create-backup-plan-console>

upvoted 1 times

 **adelyn|||||||** 1 year, 9 months ago

D:

The throughput is related to size of the EFS, but the question said the active set of the data will be only up to 100GB, with that size, the throughput will be lower than requested.

so D:

upvoted 1 times

 **VerRi** 1 year, 9 months ago

Selected Answer: A

D involves managing separate file systems that do not natively offer a "single location" experience across regions without additional configuration and replication mechanisms.

upvoted 3 times

 **Dgix** 1 year, 9 months ago

Selected Answer: D

D is the answer. A would also have worked.

upvoted 2 times

👤 CMMC 1 year, 9 months ago

Selected Answer: D

Amazon FSx for OpenZFS is a fully managed file system service that supports native replication between regions, making it well-suited for DR scenarios with a low RPO requirement. Using AWS DataSync for replication every 10 minutes ensures that the DR copy stays up to date with minimal data loss. This solution provides the required read throughput, data replication, and DR capabilities with less operational overhead.

upvoted 2 times

👤 e4bc18e 1 year, 7 months ago

Wrong Datasync tasks cannot be scheduled to be more frequent than hourly, so you cannot schedule data sync tasks to be every 10 Minutes. Apparently everyone is forgetting about burst credits for EFS. Probably something is missing but it only says the "Active working set" is 100GB" not the entire filesystem. For every 100GB of data of provisioned EFS space you can burst to 300MiBps for 72 minutes.

upvoted 1 times

Question #449

Topic 1

A company needs to gather data from an experiment in a remote location that does not have internet connectivity. During the experiment, sensors that are connected to a local network will generate 6 TB of data in a proprietary format over the course of 1 week. The sensors can be configured to upload their data files to an FTP server periodically, but the sensors do not have their own FTP server. The sensors also do not support other protocols. The company needs to collect the data centrally and move the data to object storage in the AWS Cloud as soon as possible after the experiment.

Which solution will meet these requirements?

- A. Order an AWS Snowball Edge Compute Optimized device. Connect the device to the local network. Configure AWS DataSync with a target bucket name, and unload the data over NFS to the device. After the experiment, return the device to AWS so that the data can be loaded into Amazon S3.
- B. Order an AWS Snowcone device, including an Amazon Linux 2 AMI. Connect the device to the local network. Launch an Amazon EC2 instance on the device. Create a shell script that periodically downloads data from each sensor. After the experiment, return the device to AWS so that the data can be loaded as an Amazon Elastic Block Store (Amazon EBS) volume.
- C. Order an AWS Snowcone device, including an Amazon Linux 2 AMI. Connect the device to the local network. Launch an Amazon EC2 instance on the device. Install and configure an FTP server on the EC2 instance. Configure the sensors to upload data to the EC2 instance. After the experiment, return the device to AWS so that the data can be loaded into Amazon S3.
- D. Order an AWS Snowcone device. Connect the device to the local network. Configure the device to use Amazon FSx. Configure the sensors to upload data to the device. Configure AWS DataSync on the device to synchronize the uploaded data with an Amazon S3 bucket. Return the device to AWS so that the data can be loaded as an Amazon Elastic Block Store (Amazon EBS) volume.

Correct Answer: C

Community vote distribution

C (92%) 8%

✉  **JackeyLin** 1 month ago

Selected Answer: A

AWS SnowCone discontinued in 2024. We can only use AWS SnowBall.
upvoted 1 times

✉  **AzureDP900** 1 year, 1 month ago

D sounds good to me.Option D proposes using an AWS Snowcone device:

Configuring it to use Amazon FSx.

Configuring the sensors to upload data to the device.

Setting up AWS DataSync on the device to synchronize the uploaded data with an Amazon S3 bucket.
This approach allows for seamless data collection, synchronization, and loading into Amazon S3 without requiring additional configuration or latency introduced by EC2 instances or shell scripts.
Therefore, Option D is the most suitable choice given the requirements.

upvoted 1 times

✉  **speet** 7 months, 2 weeks ago

"remote location that does not have internet connectivity"

upvoted 1 times

✉  **trungtd** 1 year, 6 months ago

Selected Answer: C

Since the sensors only support FTP for data upload, installing and configuring an FTP server on the EC2 instance is essential. This setup allows the sensors to periodically upload their data files to the Snowcone device.
upvoted 2 times

✉  **sarlos** 1 year, 7 months ago

Snowcone is specialized for huge data migration.

upvoted 2 times

✉  **VerRi** 1 year, 9 months ago

Selected Answer: C

Snowcone edge computing + FTP data transfer
upvoted 2 times

VerRi 1 year, 9 months ago

Selected Answer: C

C, because of FTP
upvoted 2 times

pangchn 1 year, 9 months ago

Selected Answer: C

agree on C, since need FTP server which is the only supported method. AWS snowball seems support EC2 too, but not in any answer
upvoted 1 times

Dgix 1 year, 9 months ago

Selected Answer: C

C, for FTP.
upvoted 1 times

djangoUnchained 1 year, 9 months ago

Selected Answer: C

C is the only one which uses FTP
upvoted 2 times

CMMC 1 year, 9 months ago

Selected Answer: C

Sensors only support FTP protocol. Leverage the native capabilities of Snowcone and EC2, providing an efficient method for collecting data.

upvoted 2 times

Question #450

A company that has multiple business units is using AWS Organizations with all features enabled. The company has implemented an account structure in which each business unit has its own AWS account. Administrators in each AWS account need to view detailed cost and utilization data for their account by using Amazon Athena.

Each business unit can have access to only its own cost and utilization data. The IAM policies that govern the ability to set up AWS Cost and Usage Reports are in place. A central Cost and Usage Report that contains all data for the organization is already available in an Amazon S3 bucket.

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

- A. In the organization's management account, use AWS Resource Access Manager (AWS RAM) to share the Cost and Usage Report data with each member account.
- B. In the organization's management account, configure an S3 event to invoke an AWS Lambda function each time a new file arrives in the S3 bucket that contains the central Cost and Usage Report. Configure the Lambda function to extract each member account's data and to place the data in Amazon S3 under a separate prefix. Modify the S3 bucket policy to allow each member account to access its own prefix.
- C. In each member account, access AWS Cost Explorer. Create a new report that contains relevant cost information for the account. Save the report in Cost Explorer. Provide instructions that the account administrators can use to access the saved report.
- D. In each member account, create a new S3 bucket to store Cost and Usage Report data. Set up a Cost and Usage Report to deliver the data to the new S3 bucket.

Correct Answer: B

Community vote distribution

B (49%)	D (43%)	8%
---------	---------	----

 **Dgix** Highly Voted 1 year, 9 months ago

Selected Answer: B

LEAST operational complexity, considering the report already is available in the bucket: B. After the initial setup, the process is fully automatic, which means the operational complexity involving separate actions by account managers isn't needed.

upvoted 9 times

 **mike5656** 1 year ago

"Modify the S3 bucket policy to allow each member account to access its own prefix". What happens when you have new accounts in the organization? :D

upvoted 1 times

 **trap** Highly Voted 1 year, 8 months ago

Correct: D

The option talks about LEAST operational complexity not LEAST operational overhead. Option B is quite complex

upvoted 9 times

 **matt200** Most Recent 4 months, 2 weeks ago

Selected Answer: D

Option D: Individual Cost and Usage Reports per account

Each account sets up its own Cost and Usage Report

Data is automatically isolated by account

Direct integration with Athena

Simple one-time setup per account

No custom code or complex sharing mechanisms

The answer is D.

Option D has the least operational complexity because:

It uses native AWS functionality without custom code

Data isolation is automatic (each account only sees its own data)

Once set up, it runs automatically with no maintenance

Each account can directly query their data with Athena

Scales easily as new accounts are added

upvoted 1 times

 **SIJUTHOMASP** 1 year ago

Selected Answer: B

Multiple accounts since multiple business units has their own account. So, it is complex to do it in each member account rather than lambda solution in option B.

upvoted 1 times

 **Spike2020** 1 year ago

Selected Answer: D

It is easy to setup CUR. B works but unnecessarily complicated.

upvoted 3 times

 **Ob43291** 1 year, 1 month ago

Selected Answer: B

After the initial setup of the S3 event, Lambda function, and bucket policy modifications, the process becomes fully automatic, minimizing the ongoing operational complexity involving separate actions by account managers.

upvoted 1 times

 **sashenka** 1 year, 1 month ago

Selected Answer: D

A Lambda-based solution for sharing Cost and Usage Reports, while powerful, introduces significant operational complexity due to the need to manage and maintain multiple AWS services and components. This includes Lambda functions, S3 events, S3 bucket policy, etc. The solution requires ongoing code maintenance, careful configuration management, and monitoring of multiple services, making it more complex than simpler alternatives like setting up individual CURs in member accounts. While it offers flexibility and automation capabilities, the added complexity might outweigh the benefits for basic cost-sharing requirements across AWS accounts.

upvoted 2 times

 **sashenka** 1 year, 1 month ago

Key Differences between Operational Complexity and Operational Overhead

Scope

Complexity: Describes the system's inherent intricacy and difficulty level

Overhead: Represents the actual cost and effort needed to keep the system running

Measurement

Complexity: Often measured in terms of system architecture and integration points

Overhead: Measured in terms of time, money, and resource consumption

Management

Complexity: Managed through system design and architecture decisions

Overhead: Managed through efficient processes, automation, and resource allocation

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Configures an S3 event that triggers a Lambda function every time a new file arrives in the central Cost and Usage Report bucket. The Lambda function extracts each member account's data from the central report.

Stores the extracted data under separate prefixes for each member account in Amazon S3.

Modifies the S3 bucket policy to grant access to each member account's prefix.

By automating this process, Option B minimizes operational complexity while ensuring that each member account has access to its own cost and usage data without requiring manual setup or maintenance.

upvoted 1 times

 **Danm86** 1 year, 2 months ago

Already its mentioned the consolidated billing report is available in centralized bucket. Here if option D has to be chosen, then the Cost and Usage report have to be configured in individual accounts separately again at individual accounts, which could add operational complexity, hence Option B seems to be right.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: B

In addition to what user Dgix commented, the fact that the S3 bucket must be in the account that creates the CUR does not make option B unfeasible. On the contrary, this option already assumes that the initial configuration of the bucket and the processing of the CUR report happen in the management account. Option B remains the recommended solution because it: Automates the data segmentation process. Ensures compliance with documentation by keeping the S3 bucket in the management account. Simplifies access control by using bucket policies to ensure that each account sees only its own data. Meets the requirement of lower operational complexity by centralizing the processing of the CUR. Therefore, even with the restriction that the S3 bucket must be in the management account, option B remains the best choice to meet the business requirements with the least operational effort.

upvoted 2 times

 **asquared16** 1 year, 4 months ago

Selected Answer: D

B sounds like quite the adventure.

upvoted 3 times

 **asquared16** 1 year, 4 months ago

"Each business unit can have access to only its own cost and utilization data"

upvoted 1 times

 **neta1o** 1 year, 4 months ago

Selected Answer: D

B would be very complex to parse the incoming files and separate by prefix. Then managing all the individual prefix shares. For that reason D seems like a better choice. Also the question mentions having the right permissions setup so they can configure their own CUR.
upvoted 2 times

 **tqphuong** 1 year, 5 months ago

Answer: Option D

First Reason: The Cost and Usage Report (CUR) cannot be set up for cross-account delivery. According to the AWS documentation, "The account that creates the Cost and Usage Report must also own the Amazon S3 bucket that AWS sends the reports to." This means each account must set up its own S3 bucket to receive its respective CUR.

<https://docs.aws.amazon.com/cur/latest/userguide/cur-consolidated-billing.html>

Second Reason: The question asks for the solution with the least operational complexity. Option D simplifies the process by allowing each account to independently manage its own CUR setup without requiring complex configurations or custom Lambda functions.

upvoted 2 times

 **trungtd** 1 year, 6 months ago

Selected Answer: A

After some investigation, I found A could be a suitable choice, however it lacks a few details

By using AWS RAM, you can share the S3 bucket (or specific prefixes within the bucket) containing the Cost and Usage Report with the member accounts.

Each member account can set up Athena queries to access and analyze their own cost and utilization data from the shared S3 bucket. This approach ensures that each business unit can view its own data without accessing other units' data.

B: too complicated

C: Cost Explorer doesn't provide the raw cost and usage data that might be needed for detailed analysis with Athena.

D: multiple Cost and Usage Reports, one for each account => out

upvoted 3 times

 **altonh** 10 months, 1 week ago

Not true. You can only S3 on outpost

upvoted 1 times

 **trungtd** 1 year, 6 months ago

Selected Answer: B

The question asks for LEAST operational complexity

But it seems that only the most complex option can solve the problem

upvoted 2 times

 **red_panda** 1 year, 7 months ago

Selected Answer: D

Why B? The question talk about LEAST operations. D for me

upvoted 5 times

 **VerRi** 1 year, 9 months ago

Selected Answer: B

The most straightforward option

upvoted 2 times

Question #451

Topic 1

A company is designing an AWS environment for a manufacturing application. The application has been successful with customers, and the application's user base has increased. The company has connected the AWS environment to the company's on-premises data center through a 1 Gbps AWS Direct Connect connection. The company has configured BGP for the connection.

The company must update the existing network connectivity solution to ensure that the solution is highly available, fault tolerant, and secure.

Which solution will meet these requirements MOST cost-effectively?

- A. Add a dynamic private IP AWS Site-to-Site VPN as a secondary path to secure data in transit and provide resilience for the Direct Connect connection. Configure MACsec to encrypt traffic inside the Direct Connect connection.
- B. Provision another Direct Connect connection between the company's on-premises data center and AWS to increase the transfer speed and provide resilience. Configure MACsec to encrypt traffic inside the Direct Connect connection.
- C. Configure multiple private VIFs. Load balance data across the VIFs between the on-premises data center and AWS to provide resilience.
- D. Add a static AWS Site-to-Site VPN as a secondary path to secure data in transit and to provide resilience for the Direct Connect connection.

Correct Answer: D

Community vote distribution

D (69%)

A (31%)

 **oayoade** Highly Voted 1 year, 9 months ago

Selected Answer: D

MACsec is only supported on 10gbps and 100gbps Direct Connect

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-mac-sec-getting-started.html>

upvoted 12 times

 **Daniel76** 1 year, 3 months ago

This URL was updated as it supports 400gbps. (it does not change the answer).

upvoted 2 times

 **Daniel76** 1 year, 3 months ago

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/MACsec.html>

upvoted 1 times

 **Curious76** Most Recent 5 months, 4 weeks ago

Selected Answer: A

The type of routing that you select can depend on the make and model of your customer gateway device. If your customer gateway device supports Border Gateway Protocol (BGP), specify dynamic routing when you configure your Site-to-Site VPN connection. If your customer gateway device does not support BGP, specify static routing.

upvoted 1 times

 **Curious76** 6 months, 1 week ago

Selected Answer: A

Static VPN doesn't use BGP — so no automatic failover, more manual effort or config needed compared to dynamic VPN.

upvoted 2 times

 **TomTom** 1 year, 1 month ago

Why not C?

Adding multiple VIFs to your Direct Connect connection is a cost-effective way to increase redundancy and improve performance.

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/direct-connect.html#:~:text=Option%201%3A%20Create%20a%20private,allowing%20you%20to%20connect%20to>

upvoted 1 times

 **nimbus_00** 1 year ago

A single AWS Direct Connect connection with multiple private virtual interfaces (VIFs) does not provide redundancy, as all the VIFs share the same underlying physical connection.

upvoted 1 times

 **trungtd** 1 year, 6 months ago

Selected Answer: D

mentioned by oayoade.

upvoted 1 times

 **titi_r** 1 year, 8 months ago

Selected Answer: D

Answer: D

To encrypt data over DX, you use MACsec for 10 Gbps and 100 Gbps links, and S2S VPN for slower links (e.g. 1 Gbps).

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-site-to-site-vpn.html>

<https://repost.aws/knowledge-center/create-vpn-direct-connect>

<https://aws.amazon.com/blogs/networking-and-content-delivery/adding-macsec-security-to-aws-direct-connect-connections/>

upvoted 1 times

 **pangchn** 1 year, 8 months ago

Selected Answer: D

vote for D too

upvoted 1 times

 **ArunRav** 1 year, 8 months ago

Selected Answer: D

D as mentioned by oayoade.

upvoted 1 times

 **zawminhtay.it.ucsm** 1 year, 9 months ago

Selected Answer: D

same as oayosde mentioned,

upvoted 1 times

 **joseribas89** 1 year, 9 months ago

Selected Answer: D

as oayoade says we need at least 10gbps to use MACsec, so option D

upvoted 2 times

 **pangchn** 1 year, 9 months ago

Selected Answer: D

D as mentioned by oayoade.

upvoted 1 times

 **k23319** 1 year, 9 months ago

Selected Answer: A

MACSec is the difference here for the additional security for Direct Connect.

upvoted 2 times

 **ahmadraufsyahputra** 1 year, 9 months ago

A because dynamic IP is more resilience than static IP

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: A

A is the correct answer.

D uses static routing which is less suitable.

upvoted 1 times

 **djangoUnchained** 1 year, 9 months ago

Selected Answer: D

With A the VPN is dependent on the DX connection, so not adding any resilience. VPN is encrypted by default, D.

upvoted 2 times

 **ovladan** 1 year, 9 months ago

Solution: A

If we look at the request "MOST cost-effectively" we can eliminate the answer under B.

If we look at this part of the requirement "the solution is highly available, fault tolerant" we can eliminate C.

If we look at this part "The company has configured BGP for the connection" and "the solution is ... secure" we can eliminate D, because the current Direct Connect connection is not encrypted and answer under D does not offer a solution to encrypt the traffic.

Base on this answer under A is right choice.

upvoted 1 times

 **CMMC** 1 year, 9 months ago

Selected Answer: A

Provide resilience for the Direct Connect connection. Configure MACsec to encrypt traffic inside the Direct Connect connection. More cost effective than the static Site-to-Site VPN in Option D (which does not have the MACsec encryption for additional security).

upvoted 4 times

Question #452

Topic 1

A company needs to modernize an application and migrate the application to AWS. The application stores user profile data as text in a single table in an on-premises MySQL database.

After the modernization, users will use the application to upload video files that are up to 4 GB in size. Other users must be able to download the video files from the application. The company needs a video storage solution that provides rapid scaling. The solution must not affect application performance.

Which solution will meet these requirements?

- A. Migrate the database to Amazon Aurora PostgreSQL by using AWS Database Migration Service (AWS DMS). Store the videos as base64-encoded strings in a TEXT column in the database.
- B. Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as objects in Amazon S3. Store the S3 key in the corresponding DynamoDB item.
- C. Migrate the database to Amazon Keyspaces (for Apache Cassandra) by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as objects in Amazon S3. Store the S3 object identifier in the corresponding Amazon Keyspaces entry.
- D. Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as base64-encoded strings in the corresponding DynamoDB item.

Correct Answer: B*Community vote distribution*

B (100%)

 **VerRi** 1 year, 3 months ago

Selected Answer: B

No doubt

upvoted 1 times

 **pangchn** 1 year, 3 months ago

Selected Answer: B

B

4GB in file size would be S3

Amazon Keyspaces (for Apache Cassandra) is not relevant at all

upvoted 2 times

 **Dgix** 1 year, 3 months ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

 **CMMC** 1 year, 3 months ago

Selected Answer: B

Storing the videos as objects in S3 is scalable and cost-effective for storing large files. DynamoDB can store video metadata (including the S3 key), allowing for efficient retrieval and management of the videos.

upvoted 3 times

Question #453

Topic 1

A company stores and manages documents in an Amazon Elastic File System (Amazon EFS) file system. The file system is encrypted with an AWS Key Management Service (AWS KMS) key. The file system is mounted to an Amazon EC2 instance that runs proprietary software.

The company has enabled automatic backups for the file system. The automatic backups use the AWS Backup default backup plan.

A solutions architect must ensure that deleted documents can be recovered within an RPO of 100 minutes.

Which solution will meet these requirements?

- A. Create a new IAM role. Create a new backup plan. Use the new IAM role to create backups. Update the KMS key policy to allow the new IAM role to use the key. Implement an hourly backup schedule for the file system.
- B. Create a new backup plan. Update the KMS key policy to allow the AWSServiceRoleForBackup IAM role to use the key. Implement a custom cron expression to run a backup of the file system every 30 minutes.
- C. Create a new IAM role. Use the existing backup plan. Update the KMS key policy to allow the new IAM role to use the key. Enable continuous backups for point-in-time recovery.
- D. Use the existing backup plan. Update the KMS key policy to allow the AWSServiceRoleForBackup IAM role to use the key. Enable Cross-Region Replication for the file system.

Correct Answer: A*Community vote distribution*

A (88%)

8%

 **VerRi** Highly Voted 1 year, 9 months ago

Selected Answer: A

The default backup plan is once a day, which cannot meet the RPO, so C and D are out.
We need both EventBridge and Lambda functions to frequently backup the EFS, so B is out.
upvoted 8 times

 **Syre** Most Recent 1 year, 2 months ago

Selected Answer: A

<https://community.aws/content/2iCkeS4XUmYdFf8Mlz6C7DFg5K3/protecting-amazon-s3-using-aws-backup>
upvoted 1 times

 **053081f** 1 year, 5 months ago

Selected Answer: A

I checked the AWS Backup console and you cannot setup backup plan less than 1 hour, so 30 min backup(B) will be excluded.
upvoted 4 times

 **titi_r** 1 year, 8 months ago

Selected Answer: A

Answer A.
upvoted 1 times

 **Aesthet** 1 year, 8 months ago

Selected Answer: A

C is not supported, see here: <https://docs.aws.amazon.com/aws-backup/latest/devguide/backup-feature-availability.html#features-by-resource>
B is not possible (minimum is 1 hour, according to <https://aws.amazon.com/blogs/storage/automating-backups-and-optimizing-backup-costs-for-amazon-efs-using-aws-backup/#:~:text=cron%20expression%20that%20creates%20backups%20as%20frequently%20as%20hourly>).
So I vote for A
upvoted 4 times

 **pangchn** 1 year, 9 months ago

Selected Answer: B

B
Using the AWS Backup console, you can choose a frequency of every 12 hours, daily, weekly, or monthly. You can also create a cron expression that creates backups as frequently as hourly
ref:
<https://aws.amazon.com/blogs/storage/automating-backups-and-optimizing-backup-costs-for-amazon-efs-using-aws-backup/>

PITR is not supported for EFS mentioned by djangoUnchained, so C is out
From AWS console, the most frequently backup is daily.

upvoted 2 times

 **chris_spencer** 1 year, 2 months ago

A: I've tried it and it doesn't work, you get an error message "
Error in some rules due to : The interval between backup jobs shouldn't be less than 60 minutes."
upvoted 2 times

 **AWSPro1234** 1 year, 9 months ago

Answer C.
upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: A
First of all, using the existing default backup plan means backups only once a day, which disqualifies both C and D. We are thus left with A and B, which both fulfil the RPO. B is slightly more wasteful in that 30-minute backups are overkill. Also, B requires a custom cron task to be set up using EventBridge as it is a non-standard one for AWS Backup.

A, however, can be accomplished without extra operational overhead. Therefore, A.
upvoted 4 times

 **CMMC** 1 year, 9 months ago

Selected Answer: C
Creating a new IAM role and updating the KMS key policy to allow the role to use the key ensures that the backup mechanism has the necessary permissions for encryption. Enabling continuous backups for point-in-time recovery increases the likelihood of being able to recover deleted documents within the specified RPO of 100 minutes.
upvoted 1 times

 **djangoUnchained** 1 year, 9 months ago

It seems PITR is not supported for EFS <https://docs.aws.amazon.com/aws-backup/latest/devguide/point-in-time-recovery.html>
upvoted 3 times

Question #454

Topic 1

A solutions architect must provide a secure way for a team of cloud engineers to use the AWS CLI to upload objects into an Amazon S3 bucket. Each cloud engineer has an IAM user, IAM access keys, and a virtual multi-factor authentication (MFA) device. The IAM users for the cloud engineers are in a group that is named S3-access. The cloud engineers must use MFA to perform any actions in Amazon S3.

Which solution will meet these requirements?

- A. Attach a policy to the S3 bucket to prompt the IAM user for an MFA code when the IAM user performs actions on the S3 bucket. Use IAM access keys with the AWS CLI to call Amazon S3.
- B. Update the trust policy for the S3-access group to require principals to use MFA when principals assume the group. Use IAM access keys with the AWS CLI to call Amazon S3.
- C. Attach a policy to the S3-access group to deny all S3 actions unless MFA is present. Use IAM access keys with the AWS CLI to call Amazon S3.
- D. Attach a policy to the S3-access group to deny all S3 actions unless MFA is present. Request temporary credentials from AWS Security Token Service (AWS STS). Attach the temporary credentials in a profile that Amazon S3 will reference when the user performs actions in Amazon S3.

Correct Answer: D*Community vote distribution*

D (100%)

 **pangchn** Highly Voted 1 year, 9 months ago

Selected Answer: D

D

STS seems to be the answer

<https://advancedweb.hu/aws-how-to-secure-access-keys-with-mfa/>https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html

upvoted 5 times

 **0b43291** Most Recent 1 year, 1 month ago

Selected Answer: D

The other options have limitations or do not fully meet the requirements:

Option A (bucket policy with MFA prompt) does not enforce MFA for all S3 actions and may not work consistently with the AWS CLI.

Option B (trust policy update for the group) does not enforce MFA for S3 actions specifically and may not work as intended with the AWS CLI.

Option C (deny policy without temporary credentials) would require the cloud engineers to use their long-term IAM access keys, which is less secure and does not follow the principle of least privilege.

By using temporary credentials obtained from AWS STS with MFA enforcement and attaching them to a named profile in the AWS CLI, you can provide a secure way for the cloud engineers to perform S3 operations while ensuring that MFA is required for those actions.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option D uses IAM access keys with the AWS CLI and requests temporary credentials from AWS Security Token Service (AWS STS) that include MFA. This solution ensures that cloud engineers must use MFA when performing actions in Amazon S3 while also providing a secure way to use the AWS CLI.

This approach aligns with the requirements of using MFA for S3 actions, minimizing security risks, and ensuring compliance with organizational policies.

upvoted 1 times

 **VerRi** 1 year, 9 months ago

Selected Answer: D

access keys with AWS CLI will just skip the MFA

upvoted 4 times

 **Dgix** 1 year, 9 months ago

Selected Answer: D

D is the correct answer, as STS is required here.

upvoted 1 times

 **CMMC** 1 year, 9 months ago

Selected Answer: D

A & C are incorrect - Using IAM access keys with the AWS CLI would bypass the requirement for MFA.

Not B - MFA should be required for specific actions, not just when assuming a role or group.

upvoted 1 times

Question #455

Topic 1

A company needs to migrate 60 on-premises legacy applications to AWS. The applications are based on the .NET Framework and run on Windows.

The company needs a solution that minimizes migration time and requires no application code changes. The company also does not want to manage the infrastructure.

Which solution will meet these requirements?

- A. Refactor the applications and containerize them by using AWS Toolkit for .NET Refactoring. Use Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to host the containerized applications.
- B. Use the Windows Web Application Migration Assistant to migrate the applications to AWS Elastic Beanstalk. Use Elastic Beanstalk to deploy and manage the applications.
- C. Use the Windows Web Application Migration Assistant to migrate the applications to Amazon EC2 instances. Use the EC2 instances to deploy and manage the applications.
- D. Refactor the applications and containerize them by using AWS Toolkit for .NET Refactoring. Use Amazon Elastic Kubernetes Service (Amazon EKS) with the Fargate launch type to host the containerized applications.

Correct Answer: B

Community vote distribution

B (80%)

A (20%)

 **sergza888** 8 months, 2 weeks ago

Selected Answer: A

Beanstalk simplifies the process but it still requires managing infrastructure. While Beanstalk automatically handles many infrastructure tasks, it still involves creating and managing environments, deploying applications, and configuring various settings. I would vote for A
upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: B

By using the Windows Web Application Migration Assistant and AWS Elastic Beanstalk, the company can migrate their .NET applications to AWS with minimal migration time, no code changes, and without the need to manage the underlying infrastructure, meeting all the stated requirements.

The other options have limitations or do not fully meet the requirements:

Options A and D (containerization with ECS or EKS) would require refactoring the applications, which goes against the requirement of avoiding code changes. Additionally, these options would require more infrastructure management compared to Elastic Beanstalk.

Option C (migration to EC2 instances) would require the company to manage the EC2 instances, configure networking, load balancing, and auto-scaling, which contradicts the requirement of not managing the infrastructure.

upvoted 3 times

 **AzureDP900** 1 year, 1 month ago

Option B uses the Windows Web Application Migration Assistant, a tool specifically designed for .NET Framework-based applications on Windows. It helps migrate these applications to AWS Elastic Beanstalk without requiring code changes or manual infrastructure management. Elastic Beanstalk then takes care of deploying and managing the applications, meeting the company's requirements. This approach ensures a smooth migration with minimal disruption, while also avoiding any significant changes to the application code or infrastructure management responsibilities.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: B

Elastic Beanstalk abstracts the infrastructure, so the company won't need to manage EC2 instances, scaling, load balancing, or patching. Elastic Beanstalk takes care of these tasks automatically, which fits the requirement of not managing infrastructure. This is not the same thing as serverless (which is NOT a requirement), as Zas1 commented.

The answer can't be A because refactoring=code change, as asquared16 have already commented.

upvoted 2 times

 **asquared16** 1 year, 4 months ago

Selected Answer: B

Refactoring = Code Change

upvoted 2 times

 **titi_r** 1 year, 8 months ago

Selected Answer: B

Getting started with Windows .NET on Elastic Beanstalk
<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/dotnet-getstarted.html>

upvoted 3 times

 **AwsZora** 1 year, 8 months ago

Selected Answer: A

No, AWS Elastic Beanstalk is not a serverless platform.
upvoted 1 times

 **Zas1** 1 year, 7 months ago

B, Not word Serverless appears: "The company also does not want to manage the infrastructure."
<https://aws.amazon.com/elasticbeanstalk>

Quickly launch web applications: Deploy scalable web applications in minutes without the complexity of provisioning and managing underlying infrastructure.

upvoted 3 times

 **VerRi** 1 year, 9 months ago

Selected Answer: B

This is a typical Beanstalk feature.
Refactoring and containerizing applications often involve some level of code change.
upvoted 2 times

 **pangchn** 1 year, 9 months ago

Selected Answer: B

I vote for B
when googling Windows Web Application Migration Assistant, all top 3 are using EB.
<https://github.com/awslabs/windows-web-app-migration-assistant>
Compare to EC2 in C, the question mentioned do not manage infrastructure
See below wording
With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications
<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>
upvoted 2 times

 **pangchn** 1 year, 9 months ago

AC
AWS Toolkit will change code in some way
<https://aws.amazon.com/visual-studio-net/>
upvoted 1 times

 **yog927** 1 year, 9 months ago

Selected Answer: A

A
Not B as company does not want to manage the infra.
upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: B

Correct answer is B, use Beanstalk. It's a classic use for Beanstalk: remember - no application changes is a requirement.

A involves quite a bit of work and application changes. AWS Toolkit for .NET is a help, but there's operational overhead. Also, moving to ECS Fargate, serverless as it is, requires containerising the application, which also adds overhead.
upvoted 2 times

 **CMMC** 1 year, 9 months ago

Selected Answer: A

Refactoring the applications and containerizing them using AWS Toolkit for .NET Refactoring allows for easy migration without needing to modify application code. Using Amazon ECS with the Fargate launch type is optimized for running containers (when comparing to #D) and allows the provisioning and scaling of containers. #A provides a streamlined migration process with minimal management overhead.
upvoted 1 times

 **ovladan** 1 year, 9 months ago

Solution: B
If you look at the request "Company needs a solution that minimizes migration time and requires no changes to application code," you can eliminate the answer under A & D (refactoring suggested).
The answers under B & C are fine, but the "minimize migration time" part, the better solution is under B.
upvoted 2 times

Question #456

Topic 1

A company needs to run large batch-processing jobs on data that is stored in an Amazon S3 bucket. The jobs perform simulations. The results of the jobs are not time sensitive, and the process can withstand interruptions.

Each job must process 15-20 GB of data when the data is stored in the S3 bucket. The company will store the output from the jobs in a different Amazon S3 bucket for further analysis.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a serverless data pipeline. Use AWS Step Functions for orchestration. Use AWS Lambda functions with provisioned capacity to process the data.
- B. Create an AWS Batch compute environment that includes Amazon EC2 Spot Instances. Specify the SPOT_CAPACITY_OPTIMIZED allocation strategy.
- C. Create an AWS Batch compute environment that includes Amazon EC2 On-Demand Instances and Spot Instances. Specify the SPOT_CAPACITY_OPTIMIZED allocation strategy for the Spot Instances.
- D. Use Amazon Elastic Kubernetes Service (Amazon EKS) to run the processing jobs. Use managed node groups that contain a combination of Amazon EC2 On-Demand Instances and Spot Instances.

Correct Answer: B

Community vote distribution

B (100%)

 **VerRi** Highly Voted 1 year, 9 months ago

Selected Answer: B

"large batch-processing jobs" -> Batch
"not time sensitive, and the process can withstand interruptions" -> Spot
upvoted 9 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Option B utilizes AWS Batch with EC2 Spot Instances and the SPOT_CAPACITY_OPTIMIZED allocation strategy. This approach takes advantage of the Spot Instance pricing model, which provides a significant discount compared to On-Demand pricing. By using this configuration, the company can process large batch jobs at a lower cost while still meeting the specified requirements.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

B is right because The results of the jobs are not time sensitive, and the process can withstand interruptions
upvoted 1 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: B

Option B - AWS Blog
<https://aws.amazon.com/blogs/compute/cost-effective-batch-processing-with-amazon-ec2-spot/>
upvoted 2 times

 **pangchn** 1 year, 9 months ago

Selected Answer: B

B
C is wrong due to the following
AWS Batch selects one or more instance types that are large enough to meet the requirements of the jobs in the queue. Instance types that are less likely to be interrupted are preferred. This allocation strategy is only available for Spot Instance compute resources.
<https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html>
upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: B

The correct answer is B.
upvoted 1 times

 **CMMC** 1 year, 9 months ago

Selected Answer: B

AWS Batch with Spot instances given not time sensitive
upvoted 1 times

Question #457

Topic 1

A company has an application that analyzes and stores image data on premises. The application receives millions of new image files every day. Files are an average of 1 MB in size. The files are analyzed in batches of 1 GB. When the application analyzes a batch, the application zips the images together. The application then archives the images as a single file in an on-premises NFS server for long-term storage.

The company has a Microsoft Hyper-V environment on premises and has compute capacity available. The company does not have storage capacity and wants to archive the images on AWS. The company needs the ability to retrieve archived data within 1 week of a request.

The company has a 10 Gbps AWS Direct Connect connection between its on-premises data center and AWS. The company needs to set bandwidth limits and schedule archived images to be copied to AWS during non-business hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy an AWS DataSync agent on a new GPU-based Amazon EC2 instance. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Glacier Instant Retrieval. After the successful copy, delete the data from the on-premises storage.
- B. Deploy an AWS DataSync agent as a Hyper-V VM on premises. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Glacier Deep Archive. After the successful copy, delete the data from the on-premises storage.
- C. Deploy an AWS DataSync agent on a new general purpose Amazon EC2 instance. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Standard. After the successful copy, delete the data from the on-premises storage. Create an S3 Lifecycle rule to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 day.
- D. Deploy an AWS Storage Gateway Tape Gateway on premises in the Hyper-V environment. Connect the Tape Gateway to AWS. Use automatic tape creation. Specify an Amazon S3 Glacier Deep Archive pool. Eject the tape after the batch of images is copied.

Correct Answer: B

Community vote distribution

B (100%)

 **TonytheTiger** 1 year, 1 month ago

Selected Answer: B

Option B: AWS Blog -
<https://aws.amazon.com/blogs/storage/protect-your-file-and-backup-archives-using-aws-datasync-and-amazon-s3-glacier/>

How do I use AWS DataSync to archive cold data? - <https://aws.amazon.com/datasync/faqs/>
upvoted 2 times

 **VerRi** 1 year, 2 months ago

Selected Answer: B

Deploy the DataSync agent to the source.
upvoted 1 times

 **Dgix** 1 year, 3 months ago

Selected Answer: B

A is out because of Glacier Instant Retrieval (milliseconds)
B is the correct answer: goes directly to Glacier Deep Archive
C needlessly stores data in S3 Standard for a day
D is an awkward use case.
upvoted 4 times

 **CMMC** 1 year, 3 months ago

Selected Answer: B

deploy the AWS DataSync in Hyper-V env, use more cost efficient S3 Glacier Deep Archive
upvoted 1 times

Question #458

Topic 1

A company wants to record key performance indicators (KPIs) from its application as part of a strategy to convert to a user-based licensing schema. The application is a multi-tier application with a web-based UI. The company saves all log files to Amazon CloudWatch by using the CloudWatch agent. All logins to the application are saved in a log file.

As part of the new license schema, the company needs to find out how many unique users each client has on a daily basis, weekly basis, and monthly basis.

Which solution will provide this information with the LEAST change to the application?

- A. Configure an Amazon CloudWatch Logs metric filter that saves each successful login as a metric. Configure the user name and client name as dimensions for the metric.
- B. Change the application logic to make each successful login generate a call to the AWS SDK to increment a custom metric that records user name and client name dimensions in CloudWatch.
- C. Configure the CloudWatch agent to extract successful login metrics from the logs. Additionally, configure the CloudWatch agent to save the successful login metrics as a custom metric that uses the user name and client name as dimensions for the metric.
- D. Configure an AWS Lambda function to consume an Amazon CloudWatch Logs stream of the application logs. Additionally, configure the Lambda function to increment a custom metric in CloudWatch that uses the user name and client name as dimensions for the metric.

Correct Answer: A

Community vote distribution

A (56%)

D (41%)

 **thotwielder** Highly Voted 1 year, 8 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/MonitoringLogData.html>
upvoted 5 times

 **Curious76** Most Recent 6 months, 1 week ago

Selected Answer: A

D-Requires setting up a Lambda function to process logs and send metrics — more complex and operational overhead compared to metric filters.
upvoted 2 times

 **Kaps443** 6 months, 1 week ago

Selected Answer: D

Use a Lambda function with a CloudWatch Logs subscription to deduplicate logins and emit custom metrics or store in DynamoDB.
No app change, full control, accurate unique-user tracking.
upvoted 2 times

 **Longc** 7 months, 3 weeks ago

Selected Answer: D

D
No Application Changes: The existing logging setup (saving logs to CloudWatch) remains unchanged.

Lambda Processes Logs: A Lambda function can subscribe to the CloudWatch Logs stream, parse login events, and track unique user-client combinations.

Use a database (e.g., DynamoDB with Time-to-Live) to store temporary state and ensure unique counts per period.

Increment custom CloudWatch metrics with user and client dimensions for each unique login.

Flexible Aggregation: CloudWatch metrics can then be aggregated (e.g., SUM, SampleCount) over daily/weekly/monthly periods.

A: Metric filters cannot deduplicate logins (they count total logins, not unique users).

B: Requires code changes to integrate AWS SDK calls, violating the "least change" requirement.

C: The CloudWatch agent cannot natively deduplicate logins or track unique users.

upvoted 2 times

 **874def1** 8 months, 2 weeks ago

Selected Answer: A

I would go with A.

In May 2021 they introduced the ability to specify up to 3 dimensions.

'For example, you can use this feature to extract fields from webserver access logs allowing you to measure the bytes transferred per event type'

<https://aws.amazon.com/about-aws/whats-new/2021/05/amazon-cloudwatch-logs-announces-dimension-support-for-metric-filters/>
upvoted 3 times

✉ **itsjunukim** 9 months, 1 week ago

Selected Answer: D

Metric Filters only provide simple pattern counting functionality and cannot handle duplicate users.
upvoted 1 times

✉ **GabrielShiao** 11 months ago

Selected Answer: A

Both A and B are workable. A is the simplest and has no code development effort
upvoted 2 times

✉ **0b43291** 1 year, 1 month ago

Selected Answer: D

With <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/MonitoringLogData.html>
the documentation states that CloudWatch Logs metric filters can extract and publish metrics based on log data, but the dimensions for these metrics are limited to the following:

LogGroupName
LogStreamName
Namespace (optional)

There is no mention of the ability to use custom dimensions like user name or client name with CloudWatch Logs metric filters.

Given this limitation, the solution that would provide the required information with the least change to the application is:

D. Configure an AWS Lambda function to consume an Amazon CloudWatch Logs stream of the application logs. Additionally, configure the Lambda function to increment a custom metric in CloudWatch that uses the user name and client name as dimensions for the metric.
upvoted 3 times

✉ **pk0619** 1 year ago

You can use up to 3 custom dimensions in cw logs metric filter and thereby capture the username and client name from the logs.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntaxForMetricFilters.html#logs-metric-filters-dimensions>
upvoted 2 times

✉ **AzureDP900** 1 year, 1 month ago

Option A involves configuring a CloudWatch Logs metric filter to extract login metrics from log files. This approach can provide the required KPIs with minimal changes to the application, as it does not require modifying the application code or adding additional services. The solution also uses dimensions to capture user name and client name information, which will help identify unique users for each client on a daily, weekly, and monthly basis.

upvoted 3 times

✉ **Danm86** 1 year, 2 months ago

Answer seems to be option D. Metric Filters can only count the occurrence of a pattern in the log, they cannot extract specific data fields like user name or client name. Metric Filters do not automatically create custom metrics in CloudWatch. They only send the counted values to an existing metric.

upvoted 1 times

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

Selected Answer: D

was at first for A but then for D.. ChatGPT is also for D:

D: This option provides the most flexibility and capability for processing data. AWS Lambda can process the incoming log stream to apply more complex logic, such as checking for and ignoring duplicate entries within a set time frame (daily, weekly, monthly) before incrementing the metrics. This allows for the implementation of logic to ensure that users are only counted once per period, effectively tracking unique logins.

Conclusion:

Among the given options, Option D using an AWS Lambda function is best equipped to handle the requirement of counting unique user logins accurately over specified periods. Lambda functions offer the flexibility to implement any necessary logic to filter duplicates and manage counts over time, aligning with the need to track unique users on a daily, weekly, and monthly basis.

upvoted 2 times

✉ **Syre** 1 year, 3 months ago

Selected Answer: D

A is not because Metric filters can't directly solve the problem of counting unique users across different time periods. They can count how many logins happened, but not how many distinct users logged in during those time periods.

upvoted 4 times

✉ **VerRi** 1 year, 9 months ago

Selected Answer: A

With existing logs, we don't have to make changes to the application.

upvoted 2 times

 **pangchn** 1 year, 9 months ago

Selected Answer: A

I would go for A

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/MonitoringPolicyExamples.html>

upvoted 2 times

 **AWSPro1234** 1 year, 9 months ago

Answer is C.

upvoted 2 times

 **Dgix** 1 year, 9 months ago

Selected Answer: A

A is the correct answer: it has the least changes to the application. C and D are rubbish.

upvoted 3 times

 **CMMC** 1 year, 9 months ago

Selected Answer: C

No app code change by configuring the agent to extract & save successful login metrics as custom metrics with user name and client name dimensions.

#A and #B requires app changes.

#D needs additional lambda infra and increase complexity

upvoted 1 times

Question #459

Topic 1

A company is using GitHub Actions to run a CI/CD pipeline that accesses resources on AWS. The company has an IAM user that uses a secret key in the pipeline to authenticate to AWS. An existing IAM role with an attached policy grants the required permissions to deploy resources.

The company's security team implements a new requirement that pipelines can no longer use long-lived secret keys. A solutions architect must replace the secret key with a short-lived solution.

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

- A. Create an IAM SAML 2.0 identity provider (IdP) in AWS Identity and Access Management (IAM). Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRole API call. Attach the existing IAM policy to the new IAM role. Update GitHub to use SAML authentication for the pipeline.
- B. Create an IAM OpenID Connect (OIDC) identity provider (IdP) in AWS Identity and Access Management (IAM). Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRoleWithWebIdentity API call from the GitHub OIDC IdP. Update GitHub to assume the role for the pipeline.
- C. Create an Amazon Cognito identity pool. Configure the authentication provider to use GitHub. Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRoleWithWebIdentity API call from the GitHub authentication provider. Configure the pipeline to use Cognito as its authentication provider.
- D. Create a trust anchor to AWS Private Certificate Authority. Generate a client certificate to use with AWS IAM Roles Anywhere. Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRole API call. Attach the existing IAM policy to the new IAM role. Configure the pipeline to use the credential helper tool and to reference the client certificate public key to assume the new IAM role.

Correct Answer: B

Community vote distribution

B (100%)

 **Dgix**  1 year, 9 months ago

Selected Answer: B

A is incorrect because GitHub doesn't support the aging SAML protocol.
B is correct because GitHub does support OIDC.
C is hysterically overengineered for this use case.
D even more so.

upvoted 8 times

 **lasithasilva709** 1 year, 9 months ago

<https://aws.amazon.com/blogs/devops/integrating-with-github-actions-ci-cd-pipeline-to-deploy-a-web-app-to-amazon-ec2/>
upvoted 2 times

 **pangchn** 1 year, 9 months ago

B

as in your KB link:

The GitHub Actions workflows must access resources in your AWS account. Here we are using IAM OpenID Connect identity provider and IAM role with IAM policies to access CodeDeploy and Amazon S3 bucket. OIDC lets your GitHub Actions workflows access resources in AWS without needing to store the AWS credentials as long-lived GitHub secrets

upvoted 4 times

 **AzureDP900**  1 year, 1 month ago

Option B involves creating an IAM OpenID Connect (OIDC) identity provider in AWS Identity and Access Management (IAM). This will allow the company to use GitHub OIDC authentication, which provides a short-lived token for authentication. The solution also creates a new IAM role with the appropriate trust policy that allows the sts:AssumeRoleWithWebIdentity API call from the GitHub OIDC IdP. This ensures that the pipeline can assume the necessary permissions without using long-lived secret keys.

upvoted 2 times

 **VerRi** 1 year, 9 months ago

Selected Answer: B

A and D are out because of sts:AssumeRole.

B with the least operational overhead.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

In summary, the feedback suggests that options A and D are not suitable because they involve the sts:AssumeRole API call, which typically requires long-lived credentials. Instead, option B, which uses the sts:AssumeRoleWithWebIdentity API call with GitHub's OIDC

identity provider, is recommended as the solution with the least operational overhead for replacing the long-lived secret key with a short-lived solution.

upvoted 1 times

Question #460

Topic 1

A company is running a web-crawling process on a list of target URLs to obtain training documents for machine learning training algorithms. A fleet of Amazon EC2 t2.micro instances pulls the target URLs from an Amazon Simple Queue Service (Amazon SQS) queue. The instances then write the result of the crawling algorithm as a .csv file to an Amazon Elastic File System (Amazon EFS) volume. The EFS volume is mounted on all instances of the fleet.

A separate system adds the URLs to the SQS queue at infrequent rates. The instances crawl each URL in 10 seconds or less.

Metrics indicate that some instances are idle when no URLs are in the SQS queue. A solutions architect needs to redesign the architecture to optimize costs.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Use m5.8xlarge instances instead of t2.micro instances for the web-crawling process. Reduce the number of instances in the fleet by 50%.
- B. Convert the web-crawling process into an AWS Lambda function. Configure the Lambda function to pull URLs from the SQS queue.
- C. Modify the web-crawling process to store results in Amazon Neptune.
- D. Modify the web-crawling process to store results in an Amazon Aurora Serverless MySQL instance.
- E. Modify the web-crawling process to store results in Amazon S3.

Correct Answer: BE

Community vote distribution

BE (100%)

 **AzureDP900** 1 year, 1 month ago

Option B involves converting the web-crawling process into an AWS Lambda function, which will allow the company to pay only for the compute time consumed by the function. This approach can help reduce costs compared to running EC2 instances.

Converting the web-crawling process to a Lambda function also eliminates the need to maintain and monitor a fleet of EC2 instances, reducing operational costs.

Option E involves modifying the web-crawling process to store results in Amazon S3, which is an object storage service that can store large amounts of data. This approach can help reduce costs compared to storing data on EFS or other block-based file systems.

Storing results in S3 also provides high availability and durability for the data, meeting the requirements of a production-grade system.

upvoted 1 times

 **pangchn** 1 year, 9 months ago

Selected Answer: BE

BE

lamda + S3

the process don't need a database

upvoted 3 times

 **Dgix** 1 year, 9 months ago

Selected Answer: BE

A is utter rubbish - scaling out is not what we need

B is optimal in terms of cost

C and D involve fairly expensive databases not suitable for this use case. Moreover, Neptune must run in a VPC.

E is optimal in terms of accessibility and cost

upvoted 3 times

 **CMMC** 1 year, 9 months ago

Selected Answer: BE

use lambda instead of a fleet of EC2, and store the results into cost-effective S3

upvoted 1 times

Question #461

Topic 1

A company needs to migrate its website from an on-premises data center to AWS. The website consists of a load balancer, a content management system (CMS) that runs on a Linux operating system, and a MySQL database.

The CMS requires persistent NFS-compatible storage for a file system. The new solution on AWS must be able to scale from 2 Amazon EC2 instances to 30 EC2 instances in response to unpredictable traffic increases. The new solution also must require no changes to the website and must prevent data loss.

Which solution will meet these requirements?

- A. Create an Amazon Elastic File System (Amazon EFS) file system. Deploy the CMS to AWS Elastic Beanstalk with an Application Load Balancer and an Auto Scaling group. Use .ebextensions to mount the EFS file system to the EC2 instances. Create an Amazon Aurora MySQL database that is separate from the Elastic Beanstalk environment.
- B. Create an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume. Deploy the CMS to AWS Elastic Beanstalk with a Network Load Balancer and an Auto Scaling group. Use .ebextensions to mount the EBS volume to the EC2 instances. Create an Amazon RDS for MySQL database in the Elastic Beanstalk environment.
- C. Create an Amazon Elastic File System (Amazon EFS) file system. Create a launch template and an Auto Scaling group to launch EC2 instances to support the CMS. Create a Network Load Balancer to distribute traffic. Create an Amazon Aurora MySQL database. Use an EC2 Auto Scaling scale-in lifecycle hook to mount the EFS file system to the EC2 instances.
- D. Create an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume. Create a launch template and an Auto Scaling group to launch EC2 instances to support the CMS. Create an Application Load Balancer to distribute traffic. Create an Amazon ElastiCache for Redis cluster to support the MySQL database. Use EC2 user data to attach the EBS volume to the EC2 instances.

Correct Answer: A*Community vote distribution*

A (93%) 7%

✉  **AzureDP900** 1 year, 1 month ago

Option A involves creating an Amazon Elastic File System (Amazon EFS) file system, which provides a highly available and scalable file system that can be accessed by multiple EC2 instances.

Deploying the CMS to AWS Elastic Beanstalk with an Application Load Balancer and an Auto Scaling group will allow the website to scale from 2 EC2 instances to 30 EC2 instances in response to unpredictable traffic increases, meeting the first requirement.

The use of EFS ensures that the file system is preserved across instance replacements or terminations during scale-in operations, preventing data loss.

upvoted 1 times

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

Selected Answer: A

C is wrong because lifehook cannot mount EFS

upvoted 4 times

✉  **VerRi** 1 year, 9 months ago

Selected Answer: A

B and D are out because NFS->EFS

C scale-in lifecycle hook to mount the EFS?????

upvoted 2 times

✉  **yog927** 1 year, 9 months ago

Selected Answer: A

A is correct

upvoted 1 times

✉  **pangchn** 1 year, 9 months ago

Selected Answer: A

A

EBS is out first.

For C, the NLB is weird but couldn't say its wrong. The scale-in policy to mount EFS is wrong, since mounting task should happens during scale-out process.

upvoted 3 times

✉  **lasithasilva709** 1 year, 9 months ago

Selected Answer: A

B and D are out because Amazon EBS is not NFS-compatible
C is out because scale-in lifecycle hook triggers when the instance is about to terminate - no point of mounting the EFS file system here

References:

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

upvoted 2 times

 **ahmadraufsyahputra** 1 year, 9 months ago

A because I think Network Load Balancer is not the answer for this case

upvoted 2 times

 **Dgix** 1 year, 9 months ago

Selected Answer: A

B and D are out because of EBS Multi-Attach volumes not working across AZs and have a max number of 16 instances in one zone.

A is the correct answer because of no code changes (yes!).

C is not optimal because of the NLB which isn't optimal as it doesn't support HTTP/HTTPS as such, working on the TCP level and doesn't do path-based routing. Also, having to set up autoscaling explicitly adds overhead.

Therefore, A.

upvoted 1 times

 **CMMC** 1 year, 9 months ago

Selected Answer: C

Change to #C since #A could involve website changes

upvoted 1 times

 **CMMC** 1 year, 9 months ago

Selected Answer: A

EFS for persistent storage, Beanstalk for deploying with ALB and auto-scaling

upvoted 1 times

Question #462

Topic 1

A company needs to implement disaster recovery for a critical application that runs in a single AWS Region. The application's users interact with a web frontend that is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The application writes to an Amazon RDS for MySQL DB instance. The application also outputs processed documents that are stored in an Amazon S3 bucket.

The company's finance team directly queries the database to run reports. During busy periods, these queries consume resources and negatively affect application performance.

A solutions architect must design a solution that will provide resiliency during a disaster. The solution must minimize data loss and must resolve the performance problems that result from the finance team's queries.

Which solution will meet these requirements?

- A. Migrate the database to Amazon DynamoDB and use DynamoDB global tables. Instruct the finance team to query a global table in a separate Region. Create an AWS Lambda function to periodically synchronize the contents of the original S3 bucket to a new S3 bucket in the separate Region. Launch EC2 instances and create an ALB in the separate Region. Configure the application to point to the new S3 bucket.
- B. Launch additional EC2 instances that host the application in a separate Region. Add the additional instances to the existing ALB in the separate Region, create a read replica of the RDS DB instance. Instruct the finance team to run queries against the read replica. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, promote the read replica to a standalone DB instance. Configure the application to point to the new S3 bucket and to the newly promoted read replica.
- C. Create a read replica of the RDS DB instance in a separate Region. Instruct the finance team to run queries against the read replica. Create AMIs of the EC2 instances that host the application frontend. Copy the AMIs to the separate Region. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, promote the read replica to a standalone DB instance. Launch EC2 instances from the AMIs and create an ALB to present the application to end users. Configure the application to point to the new S3 bucket.
- D. Create hourly snapshots of the RDS DB instance. Copy the snapshots to a separate Region. Add an Amazon ElastiCache cluster in front of the existing RDS database. Create AMIs of the EC2 instances that host the application frontend. Copy the AMIs to the separate Region. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, restore the database from the latest RDS snapshot. Launch EC2 instances from the AMIs and create an ALB to present the application to end users. Configure the application to point to the new S3 bucket.

Correct Answer: C

Community vote distribution

C (92%) 8%

 **pangchn** Highly Voted 1 year, 9 months ago

Selected Answer: C

C

A is out since periodic lambda will have data loss
B is out since ALB is regional service. Can't add EC2 to ALB if in different region
D is out since hourly backup will have data loss

upvoted 7 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Option C involves creating a read replica of the RDS DB instance in a separate Region, which addresses the performance issue caused by the finance team's queries. This approach also ensures that the database is available during a disaster. Additionally, this option uses S3 Cross-Region Replication (CRR) to synchronize data across Regions, ensuring minimal data loss in case of a disaster. The use of a read replica and CRR provides a more efficient solution compared to options A or D, which involve synchronizing entire databases or restoring from snapshots.

upvoted 1 times

 **ahrentom** 1 year, 2 months ago

Selected Answer: B

I'll go with B, because

1. C did not promote the Read Replica into a Standalone instance.
 2. C did not redirect S3 traffic to the separate region, if the main region fails.
- Cost is not in focus, so we can preinstall the needed EC2 instances.

upvoted 1 times

 **ahrentom** 1 year, 2 months ago

<https://aws.amazon.com/de/blogs/aws/amazon-rds-for-mysql-promote-read-replica/>
upvoted 1 times

 **altonh** 10 months, 1 week ago

"Launch additional EC2 instances that host the application in a separate Region. Add the additional instances to the existing ALB"

You cannot add instances from the new region to the existing region.

upvoted 1 times

 **lasithasilva709** 1 year, 9 months ago

Selected Answer: C

A is out because relational database is suited here

D is out because ElastiCache is not required and hourly snapshots of the RDS DB instance would not minimise data loss

B is out because as per the requirements (no RTO is mentioned), there is no need to launch EC2 instances in DR site and keep them idle

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: C

C is the answer.

upvoted 1 times

 **txxxxxf** 1 year, 9 months ago

Selected Answer: C

This solution involves creating a Read Replica of the RDS DB instance in another region and directing the finance team to execute queries on it, minimizing application performance impact. AMIs of EC2 instances are created and copied for rapid deployment. S3 Cross-Region Replication ensures data safety. In a disaster, the Read Replica becomes a standalone DB, and EC2 instances from AMIs with a new ALB serve the application, all reconfigured to the new S3 bucket. This approach addresses disaster recovery, minimizes data loss, and mitigates query-induced performance issues with minimal application changes.

upvoted 2 times

 **CMMC** 1 year, 9 months ago

Selected Answer: C

Read replica for reporting, CRR to replicate S3 in another region, launch EC2 from AMI and ALB and promote the read replicate in the separate region during DR

upvoted 1 times

Question #463

Topic 1

A company has many services running in its on-premises data center. The data center is connected to AWS using AWS Direct Connect (DX) and an IPSec VPN. The service data is sensitive and connectivity cannot traverse the internet. The company wants to expand into a new market segment and begin offering its services to other companies that are using AWS.

Which solution will meet these requirements?

- A. Create a VPC Endpoint Service that accepts TCP traffic, host it behind a Network Load Balancer, and make the service available over DX.
- B. Create a VPC Endpoint Service that accepts HTTP or HTTPS traffic, host it behind an Application Load Balancer, and make the service available over DX.
- C. Attach an internet gateway to the VPC, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.
- D. Attach a NAT gateway to the VPC, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.

Correct Answer: A

Community vote distribution

A (89%)	11%
---------	-----

 **backbencher2022** 1 year, 4 months ago

Selected Answer: A

A is the correct option. There is no direct support for ALB with Private Link / VPC Endpoint service. ALB can be a target group for NLB so, we can use ALB with NLB but not ALB directly. Check this page for more details - <https://aws.amazon.com/about-aws/whats-new/2021/09/application-load-balancer-aws-privatelink-static-ip-addresses-network-load-balancer/>
upvoted 3 times

 **asquared16** 1 year, 4 months ago

What do we know that makes B not a valid answer? It feels like the question is missing something.

upvoted 2 times

 **kgpoj** 1 year, 3 months ago

VPC Endpoint doesn't directly work with ALB, so B is wrong

upvoted 2 times

 **gfhbox0083** 1 year, 5 months ago

A, for sure.

Connectivity cannot traverse the internet

upvoted 2 times

 **trungtd** 1 year, 6 months ago

Selected Answer: A

A, VPC endpoint used with NLB

upvoted 2 times

 **VerRi** 1 year, 9 months ago

Selected Answer: A

VPC endpoint + NLB = PrivateLink

upvoted 2 times

 **yog927** 1 year, 9 months ago

Selected Answer: A

A, VPC endpoint used with NLB

upvoted 1 times

 **pangchn** 1 year, 9 months ago

Selected Answer: A

A

This is a privatelink scenrio. Can't find a hard evidence but the Privatelink seem can only work with NLB. If need ALB, it will be Privatelink -> NLB -> ALB

one evidence is the link lasithasilva709 posted

another evidence is compare of ALB/NLB

<https://aws.amazon.com/elasticloadbalancing/features/?nc=sn&loc=2&dn=1>

3rd evidence

<https://aws.amazon.com/about-aws/whats-new/2021/09/application-load-balancer-aws-privatelink-static-ip-addresses-network-load-balancer/>

upvoted 4 times

✉️ **pangchn** 1 year, 8 months ago

Also in question only mentioned services but doesn't mention port, where TCP (NLB) can cover all ports but HTTP/HTTPS (ALB) is restricted

upvoted 2 times

✉️ **lasithasilva709** 1 year, 9 months ago

Selected Answer: A

My understanding is that NLB should be used for a VPC endpoint service.

Here are some resources:

1. To use AWS PrivateLink, create a Network Load Balancer for your application in your VPC, and create a VPC endpoint service configuration pointing to that load balancer.

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/aws-privatelink.html>

2. <https://aws.amazon.com/blogs/networking-and-content-delivery/application-load-balancer-type-target-group-for-network-load-balancer/>

upvoted 2 times

✉️ **AWSPro1234** 1 year, 9 months ago

Answer is A.

Many services is a key word , option B is for http and https.

upvoted 2 times

✉️ **Dgix** 1 year, 9 months ago

Selected Answer: B

B is just as safe as A — TCP is not inherently safer. However, HTTPS and HTTP are much more commonly used when providing services to other companies. As we don't have any information as to the nature of the service, a safer bet (pun intended) is B.

upvoted 2 times

✉️ **CMMC** 1 year, 9 months ago

Selected Answer: A

#C & #D are out given the connectivity cannot traverse the internet. #A enables secure VPC endpoint to privately expose to other companies' VPCs without traversing the internet, and TCP to provide more controlled and secure comm protocol for sensitive data

upvoted 2 times

Question #464

A company uses AWS Organizations to manage its AWS accounts. A solutions architect must design a solution in which only administrator roles are allowed to use IAM actions. However, the solutions architect does not have access to all the AWS accounts throughout the company.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an SCP that applies to all the AWS accounts to allow IAM actions only for administrator roles. Apply the SCP to the root OU.
- B. Configure AWS CloudTrail to invoke an AWS Lambda function for each event that is related to IAM actions. Configure the function to deny the action if the user who invoked the action is not an administrator.
- C. Create an SCP that applies to all the AWS accounts to deny IAM actions for all users except for those with administrator roles. Apply the SCP to the root OU.
- D. Set an IAM permissions boundary that allows IAM actions. Attach the permissions boundary to every administrator role across all the AWS accounts.

Correct Answer: C

Community vote distribution

C (100%)

 **Dgix** Highly Voted 1 year, 9 months ago

Selected Answer: C

A: SCPs don't allow, they deny
 B: is reactive, not preventive
 C: is correct
 D: Boundary Permissions don't allow, they set maximum permissions.
 upvoted 5 times

 **Spike2020** Most Recent 1 year ago

Selected Answer: C

I will go with C. But between A & C it is very confusing. You can understand the question that SCP deny actions by default and hence you need to allow actions, or if you are white listing you need to deny actions explicitly.
 upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option C involves creating an SCP that denies IAM actions for all users except those with administrator roles. This approach ensures that only administrators can perform IAM actions, meeting one of the key requirements.
 The use of an SCP to deny permissions also provides a more centralized and scalable solution compared to options A or D, which focus on allowing specific permissions for administrators.
 Applying this SCP to the root OU will ensure it applies to all child OUs and their respective AWS accounts, meeting the requirement of enforcing the policy across multiple accounts.
 upvoted 1 times

 **ff32d79** 1 year, 4 months ago

If an SCP allows certain IAM actions specifically for administrator roles or groups, it implicitly denies those actions for all other roles and users in the accounts where the SCP is applied.

You do not need to explicitly deny the actions for non-administrator roles and users. The implicit deny happens automatically because SCPs define the maximum permissible permissions.

So it is A. With C at every new role you have to define it. And Administrators by default have in their IAM permission the capacity to do the modifications.

upvoted 2 times

 **dv1** 1 year ago

By default, AWS Org has the SCP "FullAWSAccess" that allows access to every operation. If you explicitly allow IAM actions for administrators without deleting this policy (not mentioned in the answer), you have done nothing. So C is best approach.

upvoted 1 times

 **pangchn** 1 year, 9 months ago

Selected Answer: C

C
 using SCP deny
 upvoted 3 times

 **CMMC** 1 year, 9 months ago

Selected Answer: C

Applying SCP to the root OU with specified deny rule
upvoted 3 times

Question #465

Topic 1

A company uses an organization in AWS Organizations to manage multiple AWS accounts. The company hosts some applications in a VPC in the company's shared services account.

The company has attached a transit gateway to the VPC in the shared services account.

The company is developing a new capability and has created a development environment that requires access to the applications that are in the shared services account. The company intends to delete and recreate resources frequently in the development account. The company also wants to give a development team the ability to recreate the team's connection to the shared services account as required.

Which solution will meet these requirements?

- A. Create a transit gateway in the development account. Create a transit gateway peering request to the shared services account. Configure the shared services transit gateway to automatically accept peering connections.
- B. Turn on automatic acceptance for the transit gateway in the shared services account. Use AWS Resource Access Manager (AWS RAM) to share the transit gateway resource in the shared services account with the development account. Accept the resource in the development account. Create a transit gateway attachment in the development account.
- C. Turn on automatic acceptance for the transit gateway in the shared services account. Create a VPC endpoint. Use the endpoint policy to grant permissions on the VPC endpoint for the development account. Configure the endpoint service to automatically accept connection requests. Provide the endpoint details to the development team.
- D. Create an Amazon EventBridge rule to invoke an AWS Lambda function that accepts the transit gateway attachment when the development account makes an attachment request. Use AWS Network Manager to share the transit gateway in the shared services account with the development account. Accept the transit gateway in the development account.

Correct Answer: B*Community vote distribution*

B (93%)

7%

 **AzureDP900** 1 year, 1 month ago

Option B uses AWS Resource Access Manager (RAM) to share the transit gateway resource with the development account. This eliminates the need for manual peering requests and allows the development team to access the shared services account without requiring intervention on both sides.

The use of RAM also simplifies the process of granting permissions and managing resources, making it a suitable solution for this use case.

Option B is more straightforward and easier to implement than Option C, which involves creating a VPC endpoint and configuring an endpoint service.

upvoted 2 times

 **dman** 1 year, 4 months ago

Selected Answer: A

The dev account has frequent changes and needs to connect with the ShareServices account hence connection request is from Dev -> SS
upvoted 1 times

 **trungtd** 1 year, 6 months ago

Selected Answer: B

A is incorrect: creating and managing another transit gateway in the development account and setting up peering. This adds unnecessary complexity and management overhead.

B is correct: the development account can create transit gateway attachments without needing manual intervention every time an attachment is made.

C is incorrect: Not usecase of VPC endpoints. VPC endpoints are typically used for connecting to AWS services privately without traversing the public internet. This option does not align well with the requirement to access applications in a VPC through a transit gateway.

D is incorrect: too complicated

upvoted 3 times

 **titi_r** 1 year, 7 months ago

Selected Answer: B

"B" is correct.

"C" is wrong: Endpoint services require either a Network Load Balancer or a Gateway Load Balancer. However, the answer does not mention the creation of a NLB.

<https://docs.aws.amazon.com/vpc/latest/privatelink/create-endpoint-service.html>

upvoted 2 times

✉️ **pangchn** 1 year, 9 months ago

Selected Answer: B

B

Auto accept shared attachments

<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-transit-gateways.html>

Then, create TGW attachment in dev account

upvoted 3 times

✉️ **Dgix** 1 year, 9 months ago

Selected Answer: B

B is correct.

A is wrong because TGW peering is done between regions, not accounts.

C is rubbish

D is overengineered and weird, using Network Manager for sharing the TGW rather than RAM which is best practice.

upvoted 3 times

✉️ **dman** 1 year, 4 months ago

Intra region peering is allowed, A is also valid

upvoted 1 times

✉️ **CMMC** 1 year, 9 months ago

Selected Answer: B

Provide the flexibility needed for the development team to recreate their connection to the shared services account

upvoted 2 times

Question #466

Topic 1

A company wants to migrate virtual Microsoft workloads from an on-premises data center to AWS. The company has successfully tested a few sample workloads on AWS. The company also has created an AWS Site-to-Site VPN connection to a VPC. A solutions architect needs to generate a total cost of ownership (TCO) report for the migration of all the workloads from the data center.

Simple Network Management Protocol (SNMP) has been enabled on each VM in the data center. The company cannot add more VMs in the data center and cannot install additional software on the VMs. The discovery data must be automatically imported into AWS Migration Hub.

Which solution will meet these requirements?

- A. Use the AWS Application Migration Service agentless service and the AWS Migration Hub Strategy Recommendations to generate the TCO report.
- B. Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Evaluator to generate the TCO report.
- C. Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Hub to generate the TCO report.
- D. Use the AWS Migration Readiness Assessment tool inside the VPC. Configure Migration Evaluator to generate the TCO report.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

agentless collector to scan the on-premise VMs using SNMP:
https://d1.awsstatic.com/migration-evaluator-resources/agentless_collector_overview.pdf

Here lists Migration Evaluator as one of the tools for tco report:
<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/aws-pricingtco-tools.html>
upvoted 5 times

 **pangchn** Most Recent 1 year, 3 months ago

Selected Answer: B

B
Migration Evaluator will generate a report. The financial forecast (TCO) is included. Example of report can be found here
<https://aws.amazon.com/migration-evaluator/resources/>
upvoted 1 times

 **AWSPro1234** 1 year, 3 months ago

Answer is C.
<https://aws.amazon.com/migration-hub/faqs/>
Migration Hub is the AWS service that analyzes collected data and produces the TCO report.
upvoted 3 times

 **Dgix** 1 year, 3 months ago

Selected Answer: B

A doesn't do TCO reports
B is correct, uses SNMP and generates the report
C doesn't do TCO reports
D doesn't do TCO reports that way
upvoted 1 times

 **CMMC** 1 year, 3 months ago

Selected Answer: B

agentless collector to scan the on-premise VMs using SNMP to gather the data and generate the TCO report
upvoted 1 times

 **CMMC** 1 year, 3 months ago

agentless collector to scan the on-premise VMs using SNMP to gather the data and generate the TCO report
upvoted 2 times

Question #467

A company that is developing a mobile game is making game assets available in two AWS Regions. Game assets are served from a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The company requires game assets to be fetched from the closest Region. If game assets become unavailable in the closest Region, they should be fetched from the other Region.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution. Create an origin group with one origin for each ALB. Set one of the origins as primary.
- B. Create an Amazon Route 53 health check for each ALB. Create a Route 53 failover routing record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.
- C. Create two Amazon CloudFront distributions, each with one ALB as the origin. Create an Amazon Route 53 failover routing record pointing to the two CloudFront distributions. Set the Evaluate Target Health value to Yes.
- D. Create an Amazon Route 53 health check for each ALB. Create a Route 53 latency alias record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.

Correct Answer: D

Community vote distribution

D (54%)	A (38%)	7%
---------	---------	----

 **VerRi** Highly Voted 1 year, 8 months ago

Selected Answer: D

- A - Need to set cache behaviour for another origin
 - B - Failover routing record cannot point to 2 ALBs
 - C - Works but does not meet the requirement. By default, when there is no unhealthy distribution, the traffic will always be sent to the primary but not the closest region.
 - D - Sending the traffic to the closest region unless the closest region becomes unhealthy
- upvoted 12 times

 **gustori99** Highly Voted 1 year, 9 months ago

Selected Answer: A

It is either A or D but both are not perfect. In A Cloudfront will always fetch from the primary region not the closest region. In D latency based routing might not choose the closest region but the one with best latency. For the following reasons I go with A:

A is correct: the user will always use the nearest edge location in the closest region to fetch the game assets. Cloudfront will either respond from the cache or load the game assets from the primary origin (or in case the primary origin is not available from the fail over origin).

B is incorrect because the game assets would always be fetched from the primary region.

C is wrong because this setup is essentially the same as A but much more complicated.

D is wrong because latency based routing does not necessarily choose the nearest region but the region with the best latency (geolocation routing policy would be the correct to fulfill the requirement)

upvoted 6 times

 **EzKkk** Most Recent 3 weeks, 2 days ago

Selected Answer: C

- A - No healthcheck
- B - Doesn't have latency based routing
- C - Doesn't have health check by default, you have to integrate with failover record also

Answer: C

Reason: CloudFront can be served with geolocation restriction so we can serve only in 2 aforementioned regions, and since it serves content at edge, it serves content latency based by nature. Then we can use failover to increase the resiliency

upvoted 1 times

 **aka1177** 3 weeks, 6 days ago

Selected Answer: A

I would say A is correct.

Only the first request will be served from origin and then cached on the nearest edge location. If you have two origins and use Geo-based routing (using Lambda@Edge / CloudFront Functions), you can serve the first request from the origin that is geographically closest to the user, ensuring minimal latency before the content is cached.

If you choose D meaning choose Route 53 latency-based routing, you will still experience much higher latency compared to using CloudFront.

In real life in such situation you always use CloudFront !!!

upvoted 1 times

✉ **Soliner_Bilgi_Teknolojileri** 3 months, 3 weeks ago

Selected Answer: D

D is correct because Route 53 latency-based routing always sends users to the Region with the lowest latency (effectively the closest). If that Region's ALB becomes unhealthy, Route 53 health checks remove it from DNS answers, and traffic automatically fails over to the other Region.

A is not correct because CloudFront origin groups always use the primary origin first.

Even though users connect to the nearest CloudFront edge, if the requested asset is not cached, CloudFront will fetch it from the primary Region only.

The secondary Region is used only when the primary is unhealthy, not for "closest Region" selection.

upvoted 2 times

✉ **0dc6cac** 6 months ago

Selected Answer: A

Question is a bit vague, can we have certain downtime when the closest region is failed? if that's the case, we can use route53 routing. If we want high availability, we use primary/secondary CF origins. I'd pick A to prevent any issues upon failover.

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

upvoted 1 times

✉ **eesa** 9 months ago

Selected Answer: D

D: Route 53 health check for each ALB + latency alias record

- Latency-based routing chooses the closest ALB
- Health checks ensure traffic is routed only to healthy endpoints
- Automatic failover if one Region becomes unavailable
- Fully satisfies both requirements
- This is the correct and most efficient solution

upvoted 2 times

✉ **Spike2020** 1 year ago

Selected Answer: D

A is not possible. You can have only 1 active origin behind CFN

upvoted 2 times

✉ **TomTom** 1 year ago

Selected Answer: B

Option B is more appropriate. Below explanation:

If the primary goal is to ensure that if one Region's assets become unavailable, traffic should seamlessly switch to another Region without user impact, Option B is more appropriate due to its explicit failover mechanism. However, if minimizing latency is also a critical factor alongside availability, Option D could be a viable solution but may require additional considerations for handling complete failures in one Region.

upvoted 1 times

✉ **AzureDP900** 1 year, 1 month ago

C is right in my opinion. By using CloudFront distributions with ALBs as origins and setting up a failover routing record in Route 53 (Option C), you can create a setup where traffic is directed to the distribution (and thus the ALB) in the closer region, and automatically switched to the other Region if game assets become unavailable in the first one. This approach meets all of the requirements specified in the question.

upvoted 1 times

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

Selected Answer: A

A - This option leverages Amazon CloudFront, which is a global content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. By setting up an origin group with the ALBs as origins and designating a primary origin, CloudFront automatically routes traffic to the second origin if the primary is unavailable. This setup addresses both the latency (by serving content from the nearest location due to CloudFront's global presence) and failover requirements effectively.

B - does not serve geographic location

C - works to but A is less complex

D - It lacks a CDN which is preferred for this kind of solution

upvoted 2 times

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

Selected Answer: D

Option D is the best solution because it uses Route 53 latency alias records to ensure that users access the closest AWS Region and provides failover capability with health checks, fulfilling both the proximity and reliability requirements.

For option A to be correct, it should be described as CloudFront with Origin Groups. This allows you to set up a primary and a secondary

origin. If the primary origin (the ALB in the primary Region) becomes unavailable, CloudFront automatically switches to the secondary origin (the ALB in the secondary Region).

This provides the failover functionality, which means if the assets are unavailable in one Region, they can be fetched from the other Region.

upvoted 2 times

 **Spike2020** 1 year, 3 months ago

D - closest region indicate DNS based on latency. Not a failover scenario.

upvoted 1 times

 **neta1o** 1 year, 4 months ago

Selected Answer: D
There are many factors in this question. But this "The company requires game assets to be fetched from the closest Region" points to 'D' latency based routing R53.

upvoted 1 times

 **Moghite** 1 year, 5 months ago

Selected Answer: A
Option D incorrect because there is no automatic failover like in cloudFront option A

upvoted 2 times

 **michele_scar** 1 year, 6 months ago

Selected Answer: A
We are talking about "GAME ASSETS" that by definitions are STATIC CONTENT. So for this reason we should keep A or C (CDN). The correct is A.

upvoted 3 times

 **sashenka** 1 year, 1 month ago

Even though the content may be static, it still gets fetched from the origin on various occasions such as the first time it's hit, or when the TTL expires, etc. Thus it will not be fetched from the closet Region.

upvoted 1 times

 **titi_r** 1 year, 8 months ago

Selected Answer: D

Answer: D.

upvoted 1 times

Question #468

Topic 1

A company deploys workloads in multiple AWS accounts. Each account has a VPC with VPC flow logs published in text log format to a centralized Amazon S3 bucket. Each log file is compressed with gzip compression. The company must retain the log files indefinitely.

A security engineer occasionally analyzes the logs by using Amazon Athena to query the VPC flow logs. The query performance is degrading over time as the number of ingested logs is growing. A solutions architect must improve the performance of the log analysis and reduce the storage space that the VPC flow logs use.

Which solution will meet these requirements with the LARGEST performance improvement?

- A. Create an AWS Lambda function to decompress the gzip files and to compress the files with bzip2 compression. Subscribe the Lambda function to an s3:ObjectCreated:Put S3 event notification for the S3 bucket.
- B. Enable S3 Transfer Acceleration for the S3 bucket. Create an S3 Lifecycle configuration to move files to the S3 Intelligent-Tiering storage class as soon as the files are uploaded.
- C. Update the VPC flow log configuration to store the files in Apache Parquet format. Specify hourly partitions for the log files.
- D. Create a new Athena workgroup without data usage control limits. Use Athena engine version 2.

Correct Answer: C*Community vote distribution*

C (100%)

  **AzureDP900** 1 year, 1 month ago

C is correct -- The Parquet format is designed for efficient querying, and hourly partitions allow Athena to quickly scan through the logs. This combination will result in the largest performance improvement for log analysis compared to other options.

upvoted 2 times

  **TonytheTiger** 1 year, 8 months ago**Selected Answer: C**

Option C : <https://aws.amazon.com/about-aws/whats-new/2021/10/amazon-vpc-flow-logs-parquet-hive-prefixes-partitioned-files/>

New features to make it faster, easier and more cost efficient to store and run analytics on your Amazon VPC Flow Logs
upvoted 4 times

  **pangchn** 1 year, 9 months ago**Selected Answer: C**

C

Using AWS Athena with parquet files is faster and cheaper than using other formats like CSV and JSON based file structures, according to AWS Athena pricing "compressing your data allows Athena to scan less data, and converting your data to columnar formats allows Athena to selectively read only required columns to process the data, which leads to cost savings and improved performance

<https://www.linkedin.com/pulse/aws-athena-parquet-vs-csv-ahmed-fayed/>

upvoted 4 times

  **lasithasilva709** 1 year, 9 months ago**Selected Answer: C**

Apache Parquet is compressed, efficient columnar data representation

<https://parquet.apache.org/docs/overview/motivation/>

upvoted 2 times

  **Dgix** 1 year, 9 months ago**Selected Answer: C**

C is correct.

upvoted 1 times

  **CMMC** 1 year, 9 months ago**Selected Answer: C**

Apache Parquet format to enable a highly optimized columnar storage format and partitioning by hour for improving the Athena query performance

upvoted 1 times

Question #469

Topic 1

A company wants to establish a dedicated connection between its on-premises infrastructure and AWS. The company is setting up a 1 Gbps AWS Direct Connect connection to its account VPC. The architecture includes a transit gateway and a Direct Connect gateway to connect multiple VPCs and the on-premises infrastructure.

The company must connect to VPC resources over a transit VIF by using the Direct Connect connection.

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

- A. Update the 1 Gbps Direct Connect connection to 10 Gbps.
- B. Advertise the on-premises network prefixes over the transit VIF.
- C. Advertise the VPC prefixes from the Direct Connect gateway to the on-premises network over the transit VIF.
- D. Update the Direct Connect connection's MACsec encryption mode attribute to must_encrypt.
- E. Associate a MACsec Connection Key Name/Connectivity Association Key (CKN/CAK) pair with the Direct Connect connection.

Correct Answer: BC

Community vote distribution

BC (100%)

 **AzureDP900** 1 year, 1 month ago

Option B and Option C are correct because they enable connectivity between on-premises infrastructure and AWS VPCs by advertising network prefixes. Option B enables the on-premises network to reach AWS, while option C allows the AWS VPCs to communicate with on-premises resources over a transit VIF.

upvoted 2 times

 **tushar321** 1 year, 8 months ago

BC

MACsec is ruled out as this needs 10 gbps <https://aws.amazon.com/about-aws/whats-new/2021/03/aws-direct-connect-announces-macsec-encryption-for-dedicated-10gbps-and-100gbps-connections-at-select-locations/>

upvoted 2 times

 **pangchn** 1 year, 9 months ago

Selected Answer: BC

BC

just need to add routing at both sides.

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

<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-prefix-lists.html>

ADE seems not relevant

upvoted 4 times

 **ahmadraufsyahputra** 1 year, 9 months ago

BC because we need to advertise the VPC prefixes and on-premise prefixes so the on-premise and VPC can connect

upvoted 3 times

 **Dgix** 1 year, 9 months ago

Selected Answer: BC

B and C are correct.

A is not required, D needlessly involves encryption, and E doesn't create connectivity.

upvoted 3 times

Question #470

A company wants to use Amazon WorkSpaces in combination with thin client devices to replace aging desktops. Employees use the desktops to access applications that work with Clinical trial data. Corporate security policy states that access to the applications must be restricted to only company branch office locations. The company is considering adding an additional branch office in the next 6 months.

Which solution meets these requirements with the MOST operational efficiency?

- A. Create an IP access control group rule with the list of public addresses from the branch offices. Associate the IP access control group with the WorkSpaces directory.
- B. Use AWS Firewall Manager to create a web ACL rule with an IPSet with the list of public addresses from the branch office locations. Associate the web ACL with the WorkSpaces directory.
- C. Use AWS Certificate Manager (ACM) to issue trusted device certificates to the machines deployed in the branch office locations. Enable restricted access on the WorkSpaces directory.
- D. Create a custom WorkSpace image with Windows Firewall configured to restrict access to the public addresses of the branch offices. Use the image to deploy the WorkSpaces.

Correct Answer: A
Community vote distribution

A (88%)	13%
---------	-----

 **aka1177** 3 weeks, 6 days ago

Selected Answer: A

A is correct, since this is default method to add trusted networks to workspace. (You do not always use Firewall and especially FW manager in AWS)

upvoted 1 times

 **backbencher2022** 1 year, 4 months ago

Selected Answer: A

A is correct. B is incorrect because WAF web ACLs don't work with Amazon Workspaces. A web access control list (web ACL) gives you fine-grained control over all of the HTTP(S) web requests that your protected resource responds to. You can protect Amazon CloudFront, Amazon API Gateway, Application Load Balancer, AWS AppSync, Amazon Cognito, AWS App Runner, and AWS Verified Access resources.

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html>

upvoted 3 times

 **trungtd** 1 year, 6 months ago

Selected Answer: A

This is not usecase of AWS Firewall Manager and web ACL, and A work

upvoted 2 times

 **iulian0585** 1 year, 7 months ago

Selected Answer: A

B. AWS Firewall Manager and web ACL: While this could work, it is generally used for managing rules across multiple AWS accounts and resources, which might be an overcomplication for this specific use case. It is more complex to set up and manage compared to IP access control groups.

upvoted 1 times

 **red_panda** 1 year, 7 months ago

Selected Answer: B

From an operational simplicity point of view (which is what is required) it is clearly B.

It is much easier to manage IPs with Firewall manager than in a custom way, which by the way remains vague. For me, the correct answer is B.

upvoted 1 times

 **neta1o** 1 year, 4 months ago

A would be done once for the entire WorkSpaces directory so it would be easy to manage and done centrally.

<https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-ip-access-control-groups.html#associate-ip-access-control-group>

upvoted 1 times

 **titi_r** 1 year, 8 months ago

Selected Answer: A

Answer: A

From the AWS Console: "Create an IP access control group that you can add to a WorkSpaces Directory. Users will only be able to access

WorkSpaces from these IP addresses."

upvoted 3 times

tushar321 1 year, 8 months ago

A

<https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-ip-access-control-groups.html>

upvoted 3 times

BrijMohan08 1 year, 8 months ago

Selected Answer: B

Using AWS Firewall Manager to create a web ACL rule with an IPSet containing the list of public addresses from the branch office locations and associating it with the WorkSpaces directory is the most operationally efficient solution. AWS Firewall Manager allows you to centrally manage and apply web access control lists (web ACLs) across multiple AWS resources, including WorkSpaces. This approach ensures that the access control policy is consistently applied across the WorkSpaces environment, and it can be easily updated as the company adds a new branch office location in the next 6 months.

upvoted 1 times

leliodesouza 1 year, 8 months ago

Selected Answer: B

According to ChatGPT:

"Among these options, option B, using AWS Firewall Manager to create a web ACL rule with an IPSet, offers the most operational efficiency. It allows for centralized management of access control rules across multiple WorkSpaces and easily scales to accommodate future changes, such as adding a new branch office. Additionally, it aligns with the company's security policy by restricting access based on IP addresses. Therefore, option B is the best choice."

upvoted 1 times

AzureDP900 1 year, 1 month ago

ChatGPT not always provide right answers as we know. in my opinion A is correct

upvoted 2 times

pangchn 1 year, 9 months ago

Selected Answer: A

A

<https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-ip-access-control-groups.html>

upvoted 4 times

AWSPro1234 1 year, 9 months ago

Selected Answer: A

Correct answer is A.

upvoted 1 times

ahmadraufsyahputra 1 year, 9 months ago

correct answer A , need to add ip public for the branch offices to restrict access from branch offices only

upvoted 1 times

Dgix 1 year, 9 months ago

Selected Answer: A

A is the correct answer. It is the most operationally efficient as it uses IP access control groups.

upvoted 4 times

oayoade 1 year, 9 months ago

Selected Answer: A

Trust me

upvoted 2 times

Question #471

Topic 1

A company uses AWS Organizations. The company runs two firewall appliances in a centralized networking account. Each firewall appliance runs on a manually configured highly available Amazon EC2 instance. A transit gateway connects the VPC from the centralized networking account to VPCs of member accounts. Each firewall appliance uses a static private IP address that is then used to route traffic from the member accounts to the internet.

During a recent incident, a badly configured script initiated the termination of both firewall appliances. During the rebuild of the firewall appliances, the company wrote a new script to configure the firewall appliances at startup.

The company wants to modernize the deployment of the firewall appliances. The firewall appliances need the ability to scale horizontally to handle increased traffic when the network expands. The company must continue to use the firewall appliances to comply with company policy. The provider of the firewall appliances has confirmed that the latest version of the firewall code will work with all AWS services.

Which combination of steps should the solutions architect recommend to meet these requirements MOST cost-effectively? (Choose three.)

- A. Deploy a Gateway Load Balancer in the centralized networking account. Set up an endpoint service that uses AWS PrivateLink.
- B. Deploy a Network Load Balancer in the centralized networking account. Set up an endpoint service that uses AWS PrivateLink.
- C. Create an Auto Scaling group and a launch template that uses the new script as user data to configure the firewall appliances. Create a target group that uses the instance target type.
- D. Create an Auto Scaling group. Configure an AWS Launch Wizard deployment that uses the new script as user data to configure the firewall appliances. Create a target group that uses the IP target type.
- E. Create VPC endpoints in each member account. Update the route tables to point to the VPC endpoints.
- F. Create VPC endpoints in the centralized networking account. Update the route tables in each member account to point to the VPC endpoints.

Correct Answer: ACF

Community vote distribution

ACF (52%)	ACE (43%)	4%
-----------	-----------	----

 **yog927**  1 year, 9 months ago

Selected Answer: ACF

Refer this <https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-inspection-architecture-with-aws-gateway-load-balancer-and-aws-transit-gateway/>

The endpoint is created in the centralized account only.
upvoted 14 times

 **titi_r** 1 year, 8 months ago
No doubt that "A" and "C" are correct.

E – it's a valid config, but it's against any logic – having a TGW and at the same time paying for GWLBs in each member account's VPC.
F – The answer says "Update the route tables in each member account to point to the VPC endpoints." – this is NOT possible. The route tables of the member/spoke accounts point to the TGW's ENI (for 0.0.0.0/0) in their own VPC; they cannot point to the (GWLB) VPC endpoints in another VPC.

Check the route table of Spoke1 VPC in below diagram – Destination: 0.0.0.0/0, Target: tgw-id (NOT vpce-az-a-id):
https://d2908q01vomqb2.cloudfront.net/5b384ce32d8cdef02bc3a139d4cac0a22bb029e8/2022/04/14/GWLB_TGW FIGURE2.jpg

P.S. Who wrote this question is an incompetent.
upvoted 9 times

 **altonh** 10 months, 1 week ago
I think the TGW is a distraction, so in E, you need to "Update the route tables to point to the VPC endpoints.".
upvoted 1 times

 **blackname**  1 year, 7 months ago

Selected Answer: ACF

A - Gateway Load Balancer is LB type used to redirect traffic to traffic inspection devices like firewalls, this is done via GENEVE network protocol. (correct)
B - NLB could not be used, NLB does not support GENEVE protocol. (incorrect)
C - ASG is the way to go for this scenario, in addition could be add Autoscaling policies to add more instances during traffic spikes and reduce when no traffic spikes (correct)

D - Launch wizard work directly with resource EC2 and EBS, I didn't see any integration with ASG (incorrect)
 E - Works but it's not cost effective, VPCE have a price of 0.01\$/hour/az each, so if you have GWLB in multi-az you would pay (1VPCE * number of AZs * number of member account) (incorrect - not cost effective)
 F - Since transit gateway is used, all traffic could be routed to the centralized networking account, and in there 0.0.0.0/0 traffic would go to the GWLB endpoints, so instead of multiple vpc endpoints you would only have 1VPCE * number of AZs (correct)
 upvoted 8 times

 **Malluchan** Most Recent ⓘ 3 months, 1 week ago

Selected Answer: ACE

A — Gateway Load Balancer (GWLB) + PrivateLink endpoint service.
 C — Auto Scaling group + launch template + instance target type
 E — Create the GWLB (VPC endpoints) in each member account and update route tables
 F is wrong - (endpoints in centralized account) — endpoints must be in the consumer/member VPCs so traffic is routed locally to the endpoint that connects to the central GWLB service.

upvoted 1 times

 **zhen234** 11 months ago

Selected Answer: ACE

VPC endpoints need to be created in member accounts, not the centralized account.

upvoted 1 times

 **TomTom** 1 year, 1 month ago

Selected Answer: ACE

ACE
 Can meet the requirement with most cost-effective

upvoted 1 times

 **TomTom** 1 year ago

Typo, it should be ACF.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: ACF

Gateway Load Balancer (Step A): The Gateway Load Balancer (GWLB) is designed specifically for centralized inspection architectures, where traffic needs to be inspected or processed by third-party virtual appliances, such as the firewall appliances in this scenario. GWLB provides a cost-effective and scalable solution for distributing traffic across the firewall appliances.

Auto Scaling Group and Launch Template (Step C): As mentioned in my previous response, creating an Auto Scaling group and a launch template that uses the new script as user data allows for automated and consistent deployment of the firewall appliances, as well as horizontal scaling to handle increased traffic.

VPC Endpoints in the Centralized Networking Account (Step F): Creating VPC endpoints in the centralized networking account and updating the route tables in each member account to point to these VPC endpoints enables secure and private communication between the member accounts and the firewall appliances, without the need for an internet gateway or NAT gateway.

upvoted 2 times

 **milesToGo** 1 year, 1 month ago

Guys, The answer is ACE.

AWS PrivateLink — A technology that provides private connectivity between VPCs and services.

VPC endpoint — The entry point in your VPC that enables you to connect privately to a service.

So Got to choose E - Create VPC endpoints in each member account. Update the route tables to point to the VPC endpoints.

Check ChatGPT, Check Google Gemini

(Do you create a VPC endpoint in centralized account or each member account if Gateway Load Balancer in the centralized networking account is set up as endpoint service using AWS PrivateLink)

Go to Concepts and read under service name

<https://docs.aws.amazon.com/vpc/latest/privatelink/concepts.html>

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

The correct answers are A, C, and E.

Option A: Deploying a Gateway Load Balancer allows for efficient routing and scaling, while setting up an endpoint service using AWS PrivateLink enables secure and private connectivity between the load balancer and member accounts.

Option C: Creating an Auto Scaling group with a launch template that uses the new script as user data ensures consistent configuration of firewall appliances. Additionally, creating a target group with the instance target type allows for efficient routing of traffic to the scaled instances.

Option E: Creating VPC endpoints in each member account enables direct access to the centralized networking account's resources without the need for public IP addresses or NAT devices. This is particularly beneficial when deploying highly available and scalable firewall appliances.

upvoted 1 times

 **Danm86** 1 year, 2 months ago

Between E and F, I vote for option E, because already there is transit gateway for communication from centralized account to member accounts.

upvoted 1 times

 **kgpoj** 1 year, 3 months ago

Selected Answer: ACE

A has VPC Endpoint Service in central VPC
Then we should have VPC endpoints in member accounts
upvoted 1 times

 **testo001** 1 year, 4 months ago

Selected Answer: ACE
Main discussion about E and F
upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: ACE
Main discussion about E and F
it combine Member VPC, Centralize networking, Endpoint Service, VPC Endpoint
Accoring to statement and answer A and C, that mean
Transit-GW is in memeber VPC
Firewall in Centralize VPC which already has Endpoint Service in PrivateLink, So, MUST have VPC Endpoint in Memeber account, not Centralized
Another important is 'Each firewall appliance uses a static private IP address that is then used to route traffic from the member accounts to the internet ', which prevent use one IP from transit-GW as endpoint.
upvoted 3 times

 **vip2** 1 year, 5 months ago

Main discussion about E and F
it combine Member VPC, Centralize networking, Endpoint Service, VPC Endpoint
Accoring to statement and answer A and C, that mean
Transit-GW is in memeber VPC
Firewall in Centralize VPC which already has Endpoint Service in PrivateLink, So, MUST have VPC Endpoint in Memeber account, not Centralized
Another important is 'Each firewall appliance uses a static private IP address that is then used to route traffic from the member accounts to the internet ', which prevent use one IP from transit-GW as endpoint.
upvoted 1 times

 **grandcanyon** 1 year, 5 months ago

Selected Answer: ACE
<https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway-load-balancer.html>
upvoted 5 times

 **trungtd** 1 year, 6 months ago

Selected Answer: ACF
Having multiple VPC endpoints will make connection unscalable
upvoted 3 times

 **Zas1** 1 year, 7 months ago

Selected Answer: ACE
F discard because update route. Explain "titi_r"
upvoted 3 times

 **2aa610e** 1 year, 7 months ago

Selected Answer: ACE
gateway loadbalancer endpoint needs to be in the spoke VPC. <https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-network-traffic-inspection-using-aws-gateway-load-balancer/>
upvoted 3 times

Question #472

Topic 1

A solutions architect must implement a multi-Region architecture for an Amazon RDS for PostgreSQL database that supports a web application. The database launches from an AWS CloudFormation template that includes AWS services and features that are present in both the primary and secondary Regions.

The database is configured for automated backups, and it has an RTO of 15 minutes and an RPO of 2 hours. The web application is configured to use an Amazon Route 53 record to route traffic to the database.

Which combination of steps will result in a highly available architecture that meets all the requirements? (Choose two.)

- A. Create a cross-Region read replica of the database in the secondary Region. Configure an AWS Lambda function in the secondary Region to promote the read replica during a failover event.
- B. In the primary Region, create a health check on the database that will invoke an AWS Lambda function when a failure is detected. Program the Lambda function to recreate the database from the latest database snapshot in the secondary Region and update the Route 53 host records for the database.
- C. Create an AWS Lambda function to copy the latest automated backup to the secondary Region every 2 hours.
- D. Create a failover routing policy in Route 53 for the database DNS record. Set the primary and secondary endpoints to the endpoints in each Region.
- E. Create a hot standby database in the secondary Region. Use an AWS Lambda function to restore the secondary database to the latest RDS automatic backup in the event that the primary database fails.

Correct Answer: AD*Community vote distribution*

AD (89%)

11%

 aka1177 2 weeks, 5 days ago

Selected Answer: AD

The question and requirements are really poorly written
upvoted 1 times

 ForDummies 7 months, 3 weeks ago

Selected Answer: A

If you're creating failover records in a PHZ, you must assign a public IP address to the instance in the VPC, because R53 health checkers are outside VPC. Option D doesn't make any sense, because we're talking about DB.
upvoted 1 times

 AzureDP900 1 year, 1 month ago

Here's a breakdown of the correct steps:
Step A: Cross-Region Read Replica: Create a cross-Region read replica of the database in the secondary Region. This ensures continuous data replication between Regions, minimizing data loss and ensuring business continuity.
Step D: Failover Routing Policy: Create a failover routing policy in Route 53 for the database DNS record. Set the primary and secondary endpoints to the endpoints in each Region. This allows for swift failover to the standby database in case of a failure.
These two steps together ensure:
Continuous data replication between Regions, minimizing data loss and ensuring business continuity.
Swift failover to the standby database in case of a failure, with minimal disruption to services.
upvoted 1 times

 trungtd 1 year, 6 months ago

Selected Answer: AD

Classic question
upvoted 2 times

 Russ99 1 year, 9 months ago

Selected Answer: AD

Option C involves copying the latest automated backup to the secondary Region every 2 hours, which does not provide a standby database instance and may not meet the RTO requirement.
upvoted 1 times

 Dgix 1 year, 9 months ago

Selected Answer: AD

- A is required to meet the RTO as well as the RPO.
- B will not meet the RTO.
- C meets the RPO but doesn't handle failover
- D handles failover
- E is incomplete and says nothing of how backups arrive in the secondary region and will most likely not meet the RTO.
upvoted 2 times

CMMC 1 year, 9 months ago

Selected Answer: AD

cross region read replicate at secondary region, promote during failover, together with Route 53 failover routing policy
upvoted 2 times

Question #473

An ecommerce company runs an application on AWS. The application has an Amazon API Gateway API that invokes an AWS Lambda function. The data is stored in an Amazon RDS for PostgreSQL DB instance.

During the company's most recent flash sale, a sudden increase in API calls negatively affected the application's performance. A solutions architect reviewed the Amazon CloudWatch metrics during that time and noticed a significant increase in Lambda invocations and database connections. The CPU utilization also was high on the DB instance.

What should the solutions architect recommend to optimize the application's performance?

- A. Increase the memory of the Lambda function. Modify the Lambda function to close the database connections when the data is retrieved.
- B. Add an Amazon ElastiCache for Redis cluster to store the frequently accessed data from the RDS database.
- C. Create an RDS proxy by using the Lambda console. Modify the Lambda function to use the proxy endpoint.
- D. Modify the Lambda function to connect to the database outside of the function's handler. Check for an existing database connection before creating a new connection.

Correct Answer: C*Community vote distribution*

C (71%)	D (21%)	4%
---------	---------	----

 **titi_r** Highly Voted 1 year, 8 months ago

Selected Answer: C

Some guys got confused whether it's possible to create a DB proxy from the Lambda console Yes, you CAN create a proxy from within the Lambda console: open a function -> Configuration -> RDS databases -> Add Proxy, then select a radio button with two options:

- Create a new database proxy
- Choose an existing database proxy

Said that, "C" is correct.

upvoted 13 times

 **YOUSSEFWAID** 1 year, 7 months ago

Create a new database not RDS proxy!

Use an existing database

Create a new database

upvoted 1 times

 **oayoade** Highly Voted 1 year, 9 months ago

Selected Answer: C

<https://repost.aws/knowledge-center/lambda-rds-database-proxy>

upvoted 7 times

 **AI8282** Most Recent 5 months, 1 week ago

Selected Answer: C

Lambda console offers a way to create a RDS Proxy:

Navigate to your Lambda function: Open the Lambda console and select the function you want to connect to an RDS database.

Go to the Configuration tab: Choose the "Configuration" tab and then select "RDS databases".

Connect to RDS database: Click on "Connect to RDS database".

Choose an RDS database: Select the RDS database you want to connect to.

Add a database proxy: Follow the wizard to add a database proxy. You'll need to provide a proxy identifier, select your RDS database, choose a Secrets Manager secret (for credentials), and an IAM role.

Configure network settings: AWS Lambda will automatically configure the necessary network settings, including the VPC, subnets, and security groups, based on your selections.

Connect to the proxy: Once the proxy is created and available, you can connect to it using the proxy endpoint provided.

upvoted 1 times

 **0dc6cac** 6 months, 1 week ago

Selected Answer: D

I think B/C/D all work, the question isn't specific enough to know for sure. I pick D because it's a very simple solution, doesn't cost anything, and fixes the connections issue.

upvoted 1 times

 **altonh** 10 months, 1 week ago

Selected Answer: B

I think B will solve the database connection and the DB CPU utilization.

upvoted 1 times

 **skydev** 11 months ago

Selected Answer: B

As for me, the correct answer is B.

"The CPU utilization also was high on the DB instance" - DB Utilization can be high due to unoptimized queries. Opening a new connection for PG is not a complex operation (it does not consume many resources).

Adding connection pooling will not help in this situation, IMHO, because even one unoptimized query is enough to consume all CPU resources on the database layer.

ElastiCache will allow query offloading from the DB layer.

upvoted 1 times

 **TomTom** 1 year, 1 month ago

Selected Answer: A

The first part is a significant increase in Lambda invocation and database connection. So, increasing the Lambda function's memory is the quickest solution.

This will allow the function to handle more concurrent requests and reduce cold start times, immediately improving response times.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

Creating an RDS proxy by using the Lambda console and modifying the Lambda function to use the proxy endpoint can help improve performance during peak usage periods like flash sales. This approach has several advantages:

C is right

Reduced Database Load: By using a connection pool provided by the RDS proxy, you can reduce the number of database connections and queries, which can help decrease CPU utilization and improve overall system performance.

Improved Response Times: With an RDS proxy, your application can respond more quickly to user requests, as it doesn't need to wait for database queries to complete.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: C

"Step 3

1. Open the Functions page in the LAMBDA CONSOLE.

2. In Functions, choose your Lambda function.

3. Choose Configuration, and then choose ADD DATABASE PROXIES.

4. Enter the following variables:

Proxy identifier: The name of the proxy.

RDS DB instance: A supported MySQL or PostgreSQL DB instance or cluster.

Secret: The Secrets Manager that you created.

IAM role: The IAM role that you created.

Authentication: Choose Password to connect with database credentials or choose Execution role to use the function's IAM credentials for authentication.

5. Choose Add."

upvoted 2 times

 **zolthar_z** 1 year, 4 months ago

Selected Answer: D

With the current options for my is D, because you can't create a RDS Proxy from Lambda function console, unless the C is misspelled and the answer is only AWS Console

upvoted 2 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: D

Vote D because answer C is incorrect without mention increasing db server qty increase behind proxy. No improvement by just changing endpoint from db to db proxy.

D can help by reusing the db connection instead of one connection per thread. Lambda by default is parallel run inside the handler.

upvoted 2 times

 **iulian0585** 1 year, 7 months ago

Selected Answer: D

C, is wrong

Creating Proxy: Within the RDS console, find the "Proxies" section and click on "Create proxy".

upvoted 3 times

 **TonytheTiger** 1 year, 8 months ago

Selected Answer: C

Option C: Read AWS Blog - Using Amazon RDS Proxy w/ AWS Lambda

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

Read Section " Create and attach a proxy to a Lambda function "

Next, use the Lambda console to Add a Database proxy to a Lambda function.

Sign into the AWS Lambda console and open the Lambda function you would like to enable RDS Proxy. This Lambda function needs to be configured for access to the same VPC and Subnets as your RDS database.

upvoted 4 times

✉️ **YOUSSEFWAID** 1 year, 8 months ago

C, is wrong

Creating Proxy: Within the RDS console, find the "Proxies" section and click on "Create proxy".

upvoted 2 times

✉️ **teo2157** 1 year, 8 months ago

Selected Answer: D

A) Incorrect because the issue is at database level

B) Partially correct but there's one step missed because you have to modify endpoint for the lambda function

C) This is the tricky one, it's almost correct and the best option except for one comment, it's said "Create an RDS proxy by using the Lambda console" the RDS proxy is not created in the lambda console but in the RDS console....

D) Totally correct, <https://docs.aws.amazon.com/lambda/latest/dg/best-practices.html>

Said that, going for D but I found this question very tricky....

upvoted 1 times

✉️ **teo2157** 1 year, 7 months ago

I've changed my mind as it's possible to create an RDS proxy by using the Lambda console and regarding the D option, this will improve the lambda performance but not the RDS so going for option C definitely.

upvoted 1 times

✉️ **pangchn** 1 year, 9 months ago

Selected Answer: C

BCD all looks good.

I vote for C

upvoted 3 times

✉️ **pangchn** 1 year, 9 months ago

not B, redis is NOSQL so no relevant to this question

upvoted 1 times

✉️ **pangchn** 1 year, 9 months ago

umm, NVM

<https://newsletter.simpleaws.dev/p/elasticache-redis-cache-rds>

upvoted 2 times

✉️ **djangoUnchained** 1 year, 9 months ago

Almost answered C before realizing it was a trap. You don't create RDS Proxies from the LAMBDA console, it is done from the RDS console. D is the best answer.

upvoted 2 times

✉️ **gustori99** 1 year, 9 months ago

It's not a trap. It is possible to create the RDS Proxy from within the lambda console.

upvoted 3 times

Question #474

Topic 1

A retail company wants to improve its application architecture. The company's applications register new orders, handle returns of merchandise, and provide analytics. The applications store retail data in a MySQL database and an Oracle OLAP analytics database. All the applications and databases are hosted on Amazon EC2 instances.

Each application consists of several components that handle different parts of the order process. These components use incoming data from different sources. A separate ETL job runs every week and copies data from each application to the analytics database.

A solutions architect must redesign the architecture into an event-driven solution that uses serverless services. The solution must provide updated analytics in near real time.

Which solution will meet these requirements?

- A. Migrate the individual applications as microservices to Amazon Elastic Container Service (Amazon ECS) containers that use AWS Fargate. Keep the retail MySQL database on Amazon EC2. Move the analytics database to Amazon Neptune. Use Amazon Simple Queue Service (Amazon SQS) to send all the incoming data to the microservices and the analytics database.
- B. Create an Auto Scaling group for each application. Specify the necessary number of EC2 instances in each Auto Scaling group. Migrate the retail MySQL database and the analytics database to Amazon Aurora MySQL. Use Amazon Simple Notification Service (Amazon SNS) to send all the incoming data to the correct EC2 instances and the analytics database.
- C. Migrate the individual applications as microservices to Amazon Elastic Kubernetes Service (Amazon EKS) containers that use AWS Fargate. Migrate the retail MySQL database to Amazon Aurora Serverless MySQL. Migrate the analytics database to Amazon Redshift Serverless. Use Amazon EventBridge to send all the incoming data to the microservices and the analytics database.
- D. Migrate the individual applications as microservices to Amazon AppStream 2.0. Migrate the retail MySQL database to Amazon Aurora MySQL. Migrate the analytics database to Amazon Redshift Serverless. Use AWS IoT Core to send all the incoming data to the microservices and the analytics database.

Correct Answer: C

Community vote distribution

C (100%)

 **CMMC**  1 year, 9 months ago

Selected Answer: C

#A - SQS is not for near real time. MySQL on EC2 is not serverless

#B is not serverless

#D is incorrect - Appstream for desktop app streaming and IoT Core for IoT

upvoted 6 times

 **Malluchan**  3 months, 1 week ago

Selected Answer: C

C - Fully serverless, event-driven architecture with near real-time analytics and decoupled microservices.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

C is right. This solution involves migrating individual applications as microservices to Amazon EKS containers that use Fargate, moving the retail MySQL database to Amazon Aurora Serverless MySQL, and migrating the analytics database to Amazon Redshift Serverless. Using Amazon EventBridge allows you to send all incoming data to the microservices and the analytics database in near real time.

upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: C

C is serverless.

D is rubbish.

upvoted 3 times

 **oayoade** 1 year, 9 months ago

Selected Answer: C

"serverless"

upvoted 2 times

Question #475

Topic 1

A company is planning a migration from an on-premises data center to the AWS Cloud. The company plans to use multiple AWS accounts that are managed in an organization in AWS Organizations. The company will create a small number of accounts initially and will add accounts as needed. A solutions architect must design a solution that turns on AWS CloudTrail in all AWS accounts.

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

- A. Create an AWS Lambda function that creates a new CloudTrail trail in all AWS accounts in the organization. Invoke the Lambda function daily by using a scheduled action in Amazon EventBridge.
- B. Create a new CloudTrail trail in the organization's management account. Configure the trail to log all events for all AWS accounts in the organization.
- C. Create a new CloudTrail trail in all AWS accounts in the organization. Create new trails whenever a new account is created. Define an SCP that prevents deletion or modification of trails. Apply the SCP to the root OU.
- D. Create an AWS Systems Manager Automation runbook that creates a CloudTrail trail in all AWS accounts in the organization. Invoke the automation by using Systems Manager State Manager.

Correct Answer: B*Community vote distribution*

B (100%)

  **juanife** 10 months, 2 weeks ago**Selected Answer: B**

I agree with option B, since the other ones are not operationally efficient. About letter C, I undoubtedly think that it is not needed for you to create every single aws cloudtrail trail on each account to apply it

upvoted 2 times

  **Santoshhhhh** 1 year, 5 months ago

B is correct

upvoted 1 times

  **pangchn** 1 year, 9 months ago**Selected Answer: B**

B

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

upvoted 4 times

  **Dgix** 1 year, 9 months ago**Selected Answer: B**

B is correct.

upvoted 1 times

  **CMMC** 1 year, 9 months ago**Selected Answer: B**

#B is the most operational efficient

upvoted 4 times

Question #476

Topic 1

A software development company has multiple engineers who are working remotely. The company is running Active Directory Domain Services (AD DS) on an Amazon EC2 instance. The company's security policy states that all internal, nonpublic services that are deployed in a VPC must be accessible through a VPN. Multi-factor authentication (MFA) must be used for access to a VPN.

What should a solutions architect do to meet these requirements?

- A. Create an AWS Site-to-Site VPN connection. Configure integration between a VPN and AD DS. Use an Amazon WorkSpaces client with MFA support enabled to establish a VPN connection.
- B. Create an AWS Client VPN endpoint. Create an AD Connector directory for integration with AD DS. Enable MFA for AD Connector. Use AWS Client VPN to establish a VPN connection.
- C. Create multiple AWS Site-to-Site VPN connections by using AWS VPN CloudHub. Configure integration between AWS VPN CloudHub and AD DS. Use AWS Copilot to establish a VPN connection.
- D. Create an Amazon WorkLink endpoint. Configure integration between Amazon WorkLink and AD DS. Enable MFA in Amazon WorkLink. Use AWS Client VPN to establish a VPN connection.

Correct Answer: B*Community vote distribution*

B (100%)

 **Soliner_Bilgi_Teknolojileri** 3 months, 3 weeks ago

Selected Answer: B

B is correct answer
upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

This is no brainer question, B is perfect
upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: B
ACD are wrong.

But for B, it is also not perfect. AD Connector is for connecting between ADDS on premises and AWS. In this case, the ADDS is on AWS's EC2. Do you really need AD Connector?
upvoted 1 times

 **Helpnosense** 1 year, 5 months ago

No doubt that answer B will collect all the events from accounts in the organizations. But the requirement is "A solutions architect must design a solution that turns on AWS CloudTrail in all AWS accounts." Can answer B turn on AWS CloudTrail in all AWS accounts?
upvoted 1 times

 **Fu7ed** 1 year, 8 months ago

Answer is B.

Client VPN provides Active Directory support by integrating with AWS Directory Service. Client VPN supports multi-factor authentication (MFA) when it's enabled for AWS Managed Microsoft AD or AD Connector.
<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/ad.html>

C. WHY Copilot?

D. Worklink is Provide secure mobile access to your internal websites and web apps.
upvoted 1 times

 **Dgix** 1 year, 9 months ago

Selected Answer: B

A: Site-to-Site VPN is for connecting networks, not giving users access.
B is correct.
C is rubbish: AWS Copilot is for deploying containers (and it's bloody good!)
D is also rubbish: WorkLink is for website and webapp access, not VPN access.
upvoted 4 times

 **oayoade** 1 year, 9 months ago

Selected Answer: B

has to be B

upvoted 2 times

 **CMMC** 1 year, 9 months ago

Selected Answer: B

#A - workspaces client for remote desktop access and not for VPN

#C - AWS VPN CloudHub for connecting multiple on-premises or offices, and not for individual VPN connection

#D - WorkLink for secure access from mobile devices and not for VPN connection

upvoted 4 times

Question #477

Topic 1

A company is running a three-tier web application in an on-premises data center. The frontend is served by an Apache web server, the middle tier is a monolithic Java application, and the storage tier is a PostgreSQL database.

During a recent marketing promotion, customers could not place orders through the application because the application crashed. An analysis showed that all three tiers were overloaded. The application became unresponsive, and the database reached its capacity limit because of read operations. The company already has several similar promotions scheduled in the near future.

A solutions architect must develop a plan for migration to AWS to resolve these issues. The solution must maximize scalability and must minimize operational effort

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

- A. Refactor the frontend so that static assets can be hosted on Amazon S3. Use Amazon CloudFront to serve the frontend to customers. Connect the frontend to the Java application.
- B. Rehost the Apache web server of the frontend on Amazon EC2 instances that are in an Auto Scaling group. Use a load balancer in front of the Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) to host the static assets that the Apache web server needs.
- C. Rehost the Java application in an AWS Elastic Beanstalk environment that includes auto scaling.
- D. Refactor the Java application, Develop a Docker container to run the Java application. Use AWS Fargate to host the container.
- E. Use AWS Database Migration Service (AWS DMS) to replatform the PostgreSQL database to an Amazon Aurora PostgreSQL database. Use Aurora Auto Scaling for read replicas.
- F. Rehost the PostgreSQL database on an Amazon EC2 instance that has twice as much memory as the on-premises server.

Correct Answer: ACE*Community vote distribution*

ACE (85%) Other

 **chris_spencer** 1 year, 2 months ago

Selected Answer: ACE

I would prefer container over beanstalk but this are examen questions ACE
upvoted 3 times

 **wbedair** 1 year, 3 months ago

The question says they have incoming campaigns in NEAR future. Doesn't this means Rehost options are better?
upvoted 1 times

 **backbencher2022** 1 year, 4 months ago

Selected Answer: ACE

A, C & E. For A - You can connect S3 with backend Java application. It is a known pattern and also published here -
<https://aws.amazon.com/blogs/storage/extending-java-applications-to-directly-access-files-in-amazon-s3-without-recompiling/>
upvoted 1 times

 **blackname** 1 year, 7 months ago

Selected Answer: ACE

A -> Correct. Frontend could be hosted on s3 so we don't need a EC2
B -> False. That's expensive, and requires operational effort (ex: patches, ...)
C -> Correct. Elastic Beanstalk would reduce operational effort of patches and other stuff and also support native scaling
D -> False. Would be a great answer if it mentioned "Service Autoscaling" for fargate. Since it does not mention, we have to assume that would be only 1 fargate task.
E -> Correct. Aurora RDS would reduce operational effort and would also allow scaling read replicas.
F -> False. Requires very operational effort to allow DB reads scaling
F
upvoted 4 times

 **Dawson75** 1 year, 7 months ago

Selected Answer: ACE

ACE best choices
upvoted 1 times

 **Dawson75** 1 year, 8 months ago

BCF is correct
upvoted 1 times

✉ **Fu7ed** 1 year, 8 months ago

Selected Answer: ACE
I chose ACE, but I don't know why it's not D. If you tried to reduce the development effort, it wouldn't have been D, but if you want to reduce the operation effort, I think D is definitely the answer to some extent. However, I chose C because I thought using app refactoring -> java container development -> EKS Fargate was cumbersome.

upvoted 3 times

✉ **blackname** 1 year, 7 months ago

A single fargate task will not handle peak traffic. In this options it's not mentioned "Service Autoscaling" for fargate, so as is it means that would be a single fargate task

<https://repost.aws/knowledge-center/ecs-fargate-service-auto-scaling>

upvoted 1 times

✉ **4555894** 1 year, 8 months ago

Selected Answer: ACE
1. AWS CloudFront (CDN)
2. AWS Elastic Beanstalk
3. DMS
4. Aurora Auto Scaling
upvoted 1 times

✉ **tushar321** 1 year, 8 months ago

BDE
B for Web Servers ASG with EFS for scale to share Linux apache servers
D for App Servers - Fargate reduces ops efforts
E for DB
upvoted 1 times

✉ **AwsZora** 1 year, 8 months ago

Selected Answer: A
This is what my company does, and there is no mention here of enabling S3 static web hosting
upvoted 1 times

✉ **teo2157** 1 year, 8 months ago

Selected Answer: BCE
A is incorrect because you can't connect a bucket S3 to a Java application so going with Apache Web Servers with autoscaling. Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. It supports Java applications and can automatically handle the details of capacity provisioning, load balancing, scaling, and application health monitoring. The use of Aurora PostgreSQL is pretty obvious. Said that going for BCE.
upvoted 2 times

✉ **backbencher2022** 1 year, 4 months ago

You can connect S3 with backend Java application. It is a known pattern and also published here -
<https://aws.amazon.com/blogs/storage/extending-java-applications-to-directly-access-files-in-amazon-s3-without-recompiling/>
upvoted 1 times

✉ **Zas1** 1 year, 8 months ago

Selected Answer: ACE
In general, Beanstalk is the best option if your priorities are SIMPLICITY and low cost.
Meanwhile, Fargate is better if you want more control over how your application is hosted, your budget is not especially tight, and your application can be containerized.
upvoted 4 times

✉ **devnv** 1 year, 8 months ago

ACE are correct
upvoted 1 times

Question #478

A company is deploying a new application on AWS. The application consists of an Amazon Elastic Kubernetes Service (Amazon EKS) cluster and an Amazon Elastic Container Registry (Amazon ECR) repository. The EKS cluster has an AWS managed node group.

The company's security guidelines state that all resources on AWS must be continuously scanned for security vulnerabilities.

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

- A. Activate AWS Security Hub. Configure Security Hub to scan the EKS nodes and the ECR repository.
- B. Activate Amazon Inspector to scan the EKS nodes and the ECR repository.
- C. Launch a new Amazon EC2 instance and install a vulnerability scanning tool from AWS Marketplace. Configure the EC2 instance to scan the EKS nodes. Configure Amazon ECR to perform a basic scan on push.
- D. Install the Amazon CloudWatch agent on the EKS nodes. Configure the CloudWatch agent to scan continuously. Configure Amazon ECR to perform a basic scan on push.

Correct Answer: B

Community vote distribution

B (90%)	10%
---------	-----

 **AzureDP900** 1 year, 1 month ago

B is most appropriate and no additional overhead.
upvoted 1 times

 **9f02c8d** 1 year, 7 months ago

A is the correct answer, not B is focused primarily on scanning Amazon EC2 instances for vulnerabilities and does not natively support scanning Amazon EKS nodes or Amazon ECR repositories
upvoted 1 times

 **iulian0585** 1 year, 7 months ago

Selected Answer: B

A. Activate AWS Security Hub: While AWS Security Hub aggregates security findings from various AWS services, it is not primarily designed for continuous scanning of EKS nodes or ECR repositories. Security Hub is more suited for compliance checks and aggregation of security alerts from multiple sources.

upvoted 3 times

 **blackname** 1 year, 7 months ago

Selected Answer: B

A -> False. Security Hub is just a Finding aggregator of other services like AWS config, Inspector, Macie, ..., even security hub controls are in the end config rules.

B -> True. Inspector scans EC2, ECR, lambda functions (either layer analysis, either deep scan of the code), ...

C -> False. Has a lot of effort. Plus "perform a basic scan on push" is a deprecated thing, inspector should be used.

D -> False. CW Agent does not report vulns. Inspector uses SSM Agent to perform vulnerability scans. Plus "perform a basic scan on push" is a deprecated thing, inspector should be used.

upvoted 4 times

 **Fu7ed** 1 year, 8 months ago

Selected Answer: B

Configuration and vulnerability analysis in Amazon EKS

- You can use Amazon Inspector to check for unintended network accessibility of your nodes and for vulnerabilities on those Amazon EC2 instances.

<https://docs.aws.amazon.com/eks/latest/userguide/configuration-vulnerability-analysis.html>

Amazon Inspector automatically discovers and scans running Amazon EC2 instances, container images in Amazon Elastic Container Registry (Amazon ECR), and AWS Lambda functions for known software vulnerabilities and unintended network exposure.

<https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html>

So, answer is B.

upvoted 2 times

 **4555894** 1 year, 8 months ago

Selected Answer: B

EKS nodes == EC2 , ECR repository = AWS Inspector

upvoted 1 times

 **tushar321** 1 year, 8 months ago

B. Inspector
upvoted 2 times

 **AwsZora** 1 year, 8 months ago

Selected Answer: A
Inspector not suppot for eks
upvoted 1 times

 **teo2157** 1 year, 8 months ago

Selected Answer: B
Security hub integrates many Security features but the scanning itself is done by Amazon Inspector so going for B.
upvoted 4 times

 **Zas1** 1 year, 8 months ago

Selected Answer: B
You can use Amazon Inspector to check for unintended network accessibility of your nodes and for vulnerabilities on those Amazon EC2 instances.
<https://docs.aws.amazon.com/eks/latest/userguide/configuration-vulnerability-analysis.html>
upvoted 4 times

 **Russ99** 1 year, 8 months ago

Selected Answer: A
A is the correct answer for the given scenario
upvoted 1 times

 **devny** 1 year, 8 months ago

A is correct
upvoted 1 times

Question #479

A company needs to improve the reliability of its ticketing application. The application runs on an Amazon Elastic Container Service (Amazon ECS) cluster. The company uses Amazon CloudFront to serve the application. A single ECS service of the ECS cluster is the CloudFront distribution's origin.

The application allows only a specific number of active users to enter a ticket purchasing flow. These users are identified by an encrypted attribute in their JSON Web Token (JWT). All other users are redirected to a waiting room module until there is available capacity for purchasing.

The application is experiencing high loads. The waiting room module is working as designed, but load on the waiting room is disrupting the applications availability.

This disruption is negatively affecting the application's ticket sale transactions.

Which solution will provide the MOST reliability for ticket sale transactions during periods of high load?

- A. Create a separate service in the ECS cluster for the waiting room. Use a separate scaling configuration. Ensure that the ticketing service uses the JWT information and appropriately forwards requests to the waiting room service.
- B. Move the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Split the waiting room module into a pod that is separate from the ticketing pod. Make the ticketing pod part of a StatefulSet. Ensure that the ticketing pod uses the JWT information and appropriately forwards requests to the waiting room pod.
- C. Create a separate service in the ECS cluster for the waiting room. Use a separate scaling configuration. Create a CloudFront function that inspects the JWT information and appropriately forwards requests to the ticketing service or the waiting room service.
- D. Move the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Split the waiting room module into a pod that is separate from the ticketing pod. Use AWS App Mesh by provisioning the App Mesh controller for Kubernetes. Enable mTLS authentication and service-to-service authentication for communication between the ticketing pod and the waiting room pod. Ensure that the ticketing pod uses the JWT information and appropriately forwards requests to the waiting room pod.

Correct Answer: C

Community vote distribution

C (89%)	5%
---------	----

 **Zas1**  1 year, 8 months ago

Selected Answer: C

CFFunctions: You can validate hashed authorization tokens, such as JSON web tokens (JWT), by inspecting authorization headers or other request metadata.

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

upvoted 11 times

 **EzKkk**  1 month, 1 week ago

Selected Answer: D

I choose D for a few reason:

- Use EKS so that I can have mTLS for S2S authentication which reduce the amount of time that user needs to get authenticated => lower latency
- App Mesh (deprecated but still use for the sake of the question) can use for network management so I can direct the traffic to correct service which is the waiting room before going to ticket module
- Waiting room and ticket module will then create a socket connection to signal if ticket room has capacity to accept user
- Since the user is already authenticated, he/she can be transited seamlessly from S2S with real time stat of waiting line which increase the UX

upvoted 1 times

 **Malluchan** 3 months, 1 week ago

Selected Answer: C

Initial thought was A, but Separating services helps, but without routing at the edge, the ticketing service could still be impacted by traffic that first hits the waiting room. thus picked C

upvoted 1 times

 **AI8282** 5 months ago

Selected Answer: A

I hate to be the only one going with A but CF Functions can't read a database to find out if the queue is full or not, and if we separate out the processes CF would need to call the service or DB to see if the queue is full, then generate the header or send it to the right location. Due to not mentioning how the encrypted header is generated post splitting the microservices Ill have to pick A.

upvoted 1 times

 **874def1** 8 months, 2 weeks ago

Selected Answer: C

"A single ECS service of the ECS cluster is the CloudFront distribution's origin."

This means all requests will hammer this service.

The approach will be to reduce the load on this service by splitting the service and depending on the token contents to send it to the right service...

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: C

By separating the waiting room service, using separate scaling configurations, and leveraging CloudFront functions for efficient routing, Option C provides a reliable and scalable solution while minimizing architectural changes and operational overhead.

The other options have the following drawbacks:

Option A: While it separates the waiting room service, it still relies on the ticketing service to handle the routing logic based on JWT information, which could become a bottleneck during high loads.

Option B: Migrating to Amazon EKS and using StatefulSets may not be necessary for this use case and could introduce additional complexity and operational overhead.

Option D: While using Amazon EKS and App Mesh provides advanced traffic management and security features, it may be an overkill for this specific requirement and could add unnecessary complexity to the architecture.

upvoted 1 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: C

A. No mention of finer control at the CloudFront level

B. When it comes to migrating to EKS, it may bring additional complexity and cost.

C. It combines the flexibility of ECS and the edge computing capability of CloudFront.

D. It involves complex migration, configuration, and authentication mechanisms.

upvoted 1 times

 **trungtd** 1 year, 6 months ago

Selected Answer: C

Option A involves creating a separate service in the ECS cluster for the waiting room but relies on the ticketing service to forward requests to the waiting room service based on JWT information. This approach still puts some load and decision-making logic on the ticketing service, which can affect its performance during high load periods.

upvoted 2 times

 **Win007** 1 year, 7 months ago

A is correct

upvoted 1 times

 **devnv** 1 year, 8 months ago

A is correct

upvoted 1 times

Question #480

A solutions architect is creating an AWS CloudFormation template from an existing manually created non-production AWS environment. The CloudFormation template can be destroyed and recreated as needed. The environment contains an Amazon EC2 instance. The EC2 instance has an instance profile that the EC2 instance uses to assume a role in a parent account.

The solutions architect recreates the role in a CloudFormation template and uses the same role name. When the CloudFormation template is launched in the child account, the EC2 instance can no longer assume the role in the parent account because of insufficient permissions.

What should the solutions architect do to resolve this issue?

- A. In the parent account, edit the trust policy for the role that the EC2 instance needs to assume. Ensure that the target role ARN in the existing statement that allows the sts:AssumeRole action is correct. Save the trust policy.
- B. In the parent account, edit the trust policy for the role that the EC2 instance needs to assume. Add a statement that allows the sts:AssumeRole action for the root principal of the child account. Save the trust policy.
- C. Update the CloudFormation stack again. Specify only the CAPABILITY_NAMED_IAM capability.
- D. Update the CloudFormation stack again. Specify the CAPABILITY_IAM capability and the CAPABILITY_NAMED_IAM capability.

Correct Answer: A*Community vote distribution*

A (68%)	B (27%)	5%
---------	---------	----

 **SKS** Highly Voted 1 year, 8 months ago

Answer is A .

The error occurs because the trust relationship in the parent account that allows the EC2 instance to assume a role may have been broken or misconfigured. This can happen when a role is recreated with a different ARN but the same role name. The trust policy must be updated to reflect the correct ARN.

Option A addresses this by ensuring that the trust policy in the parent account contains the correct ARN for the role in the child account, allowing the sts:AssumeRole action.

Option B, which allows the root principal to assume the role, is risky and should be avoided due to security implications.

upvoted 8 times

 **jzt2003** Highly Voted 1 year, 8 months ago

Selected Answer: A

It is A.

B is incorrect because specifying the root principal opens access up to all principals in the child account that are allowed to use sts.

upvoted 6 times

 **dv1** Most Recent 1 year ago

Selected Answer: B

There is no role ARN in the statement of a trust policy (only principal), so A is not correct.

upvoted 1 times

 **TomTom** 1 year, 1 month ago

Selected Answer: A

A is correct.

There is a statement in the question: "The EC2 instance has an instance profile that the EC2 instance uses to assume a role in a parent account."

Therefore:

Option A is the most accurate solution to address the issue of the EC2 instance not being able to assume the role in the parent account.

upvoted 1 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: A

This option is directly related to the issue mentioned in the explanation. When a character is recreated in a sub account, its ARN will change, but the character name may remain unchanged. If the ARN in the trust policy is not updated to reflect the new ARN, the EC2 instance will not be able to successfully assume that role. Therefore, updating the trust policy to include the correct ARN is the key to solving the problem. The 'correct ARN' here should refer to the ARN currently held by the character recreated in the parent account. That is to say, the corresponding ARN in the parent account policy needs to be updated.

Option B adds a statement that allows the sub account root principal to perform the sts:AssumeRole operation. This is usually not the best practice, as allowing the root account to directly assume roles would pose security risks. The root account is the most powerful identity in AWS accounts and should be strictly protected.

upvoted 2 times

 **asquared16** 1 year, 4 months ago

Selected Answer: B

It's B for sure
upvoted 1 times

 **RotterDam** 1 year, 5 months ago

Selected Answer: A

(A) Because EC2 Instance 's role must be added as a trusted principal so that the parent role can trust it
upvoted 2 times

 **mark_232323** 1 year, 5 months ago

Selected Answer: B

The issue is that the EC2 instance in the child account cannot assume the role in the parent account due to insufficient permissions, even though the role has been recreated in the CloudFormation template with the same name.

Editing the trust policy of the role in the parent account and ensuring the target role ARN is correct does not grant the necessary permissions for the child account to assume the role. The trust policy governs which principals (accounts, users, roles, or services) are allowed to assume the role.

In this case, the correct solution is option B

upvoted 2 times

 **trungtd** 1 year, 6 months ago

Selected Answer: C

it's custom IAM role name so C
upvoted 1 times

 **titi_r** 1 year, 7 months ago

Selected Answer: A

Should be "A".
upvoted 4 times

 **titi_r** 1 year, 8 months ago

In IAM roles, use the Principal element in the role trust policy to specify who can assume the role. For cross-account access, you must specify the 12-digit identifier of the trusted account. [...]

When you allow access to a different account, an administrator in that account must then grant access to an identity (IAM user or role) in that account. When you specify an AWS account, you can use the account ARN (arn:aws:iam::account-ID:root), or a shortened form that consists of the "AWS": prefix followed by the account ID.

upvoted 1 times

 **titi_r** 1 year, 8 months ago

E.g.:

"Principal": { "AWS": "arn:aws:iam::123456789012:root" }
"Principal": { "AWS": "123456789012" }

The account ARN and the shortened account ID behave the same way. Both delegate permissions to the account. Using the account ARN in the Principal element does not limit permissions to only the root user of the account.

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html
<https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles>

A or B?!

upvoted 1 times

 **tushar321** 1 year, 8 months ago

C

https://docs.aws.amazon.com/AWSCloudFormation/latest/APIReference/API_CreateStack.html#:~:text=If%20you%20have%20IAM%20resources%20with%20custom%20names%2C%20you%20must%20specify%20CAPABILITY_NAMED_IAM

upvoted 2 times

 **teo2157** 1 year, 8 months ago

Selected Answer: B

The solutions architect should ensure that the trust relationship of the role in the parent account allows the child account to assume the role. The trust relationship is defined in the role's trust policy. The trust policy should specify the AWS account ID of the child account as a Principal.

upvoted 2 times

 **devnv** 1 year, 8 months ago

B is the correct answer

upvoted 1 times

Question #481

Topic 1

A company's web application has reliability issues. The application serves customers globally. The application runs on a single Amazon EC2 instance and performs read-intensive operations on an Amazon RDS for MySQL database.

During high load, the application becomes unresponsive and requires a manual restart of the EC2 instance. A solutions architect must improve the application's reliability.

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

- A. Create an Amazon CloudFront distribution. Specify the EC2 instance as the distribution's origin. Configure a Multi-AZ deployment for the RDS for MySQL database. Use the standby DB instance for the read-intensive operations.
- B. Run the application on EC2 instances that are in an Auto Scaling group. Place the EC2 instances behind an Elastic Load Balancing (ELB) load balancer. Replace the database service with Amazon Aurora. Use Aurora Replicas for the read-intensive operations.
- C. Deploy AWS Global Accelerator. Configure a Multi-AZ deployment for the RDS for MySQL database. Use the standby DB instance for the read-intensive operations.
- D. Migrate the application to AWS Lambda functions. Create read replicas for the RDS for MySQL database. Use the read replicas for the read-intensive operations.

Correct Answer: B

Community vote distribution

B (79%) 7% 7%

 **0b43291** 1 year, 1 month ago

Selected Answer: B

While the Classic Load Balancer may have limitations compared to the newer Application Load Balancers (ALB) or Network Load Balancers (NLB), it still provides significant benefits over a single EC2 instance architecture.

Therefore, if we consider Option B with the assumption that "ELB" refers to the Classic Load Balancer, it would still be a better solution than Option A, which relies on a single EC2 instance as the origin for the CloudFront distribution.

Combining an ELB (even the Classic Load Balancer) with an Auto Scaling group and a scalable database solution like Amazon Aurora with read replicas would provide a more reliable and scalable architecture than a single EC2 instance and a Multi-AZ RDS for MySQL database.
upvoted 1 times

 **0b43291** 1 year, 1 month ago

B is all great apart from the ELB instead of an ALB

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

B is right answer , A sound right but there is no need of cloud front for this use case.

upvoted 1 times

 **Nandha2021** 1 year, 6 months ago

Answer B

upvoted 1 times

 **blackname** 1 year, 7 months ago

Selected Answer: B

Obviously B

upvoted 2 times

 **Win007** 1 year, 7 months ago

D is the answer

upvoted 1 times

 **titi_r** 1 year, 8 months ago

Selected Answer: B

Answer: B.

upvoted 1 times

 **Fu7ed** 1 year, 8 months ago

Selected Answer: B

The answer is B.

- Automatically restart using health check when not responding ->>ASG
- Global customers and read-intensive >> 'Read Replica' should be available.

- A: EC2 is still alone
C: EC2 is still alone
D: It's not a minimum development effort
upvoted 3 times

 **4555894** 1 year, 8 months ago

Selected Answer: D

D. Migrate the application to AWS Lambda functions. Create read replicas for the RDS for MySQL database. Use the read replicas for the read-intensive operations.

Here's why the other options require more development effort:

- A. CloudFront with Multi-AZ RDS: This requires setting up CloudFront and configuring it to point to the EC2 instance. It also requires switching to a Multi-AZ RDS deployment, which might involve downtime.
B. Auto Scaling with ELB and Aurora: This requires the most effort. You need to migrate the application to run on multiple EC2 instances managed by Auto Scaling, set up an ELB to distribute traffic, migrate the database to Aurora, and configure Aurora Replicas.
C. Global Accelerator with Multi-AZ RDS: Similar to option A, this involves setting up Global Accelerator and requires a Multi-AZ RDS deployment.

upvoted 1 times

 **jtzt2003** 1 year, 8 months ago

You are dangerously stupid. It is B

upvoted 3 times

 **TiredDad** 1 year, 3 months ago

This comment made me laugh! I would also go with B.

upvoted 1 times

 **tushar321** 1 year, 8 months ago

B is correct

upvoted 1 times

 **noisonnoiton** 1 year, 8 months ago

Selected Answer: B

RDS need readable standby instance

upvoted 4 times

 **federikinho** 1 year, 8 months ago

Selected Answer: A

B is obviously correct for LEAST effort

upvoted 1 times

 **Zas1** 1 year, 8 months ago

Selected Answer: C

Customers globally sounds good Global Accelerator

More Work develope migrate app to Lambda

Amazon Relational Database Service (Amazon RDS) for PostgreSQL and for MySQL now support a new Amazon RDS Multi-AZ deployment option with one primary and two readable STANDBY database (DB) instances across three Availability Zones (AZs).

https://pages.awscloud.com/Deep-dive-on-Amazon-RDS-Multi-AZ-with-two-readable-standbys_2022_0408-DAT_OD.html

For a standard accelerator, you can add one or more regional resources, such as load balancers or EC2 instances endpoints,

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-get-started.html>

upvoted 1 times

 **Zas1** 1 year, 7 months ago

B Excuse me...

"Use the standby DB instance for the read-intensive operations" --> NOT

upvoted 1 times

 **devnv** 1 year, 8 months ago

B is correct

upvoted 2 times

Question #482

A company needs to use an AWS Transfer Family SFTP-enabled server with an Amazon S3 bucket to receive updates from a third-party data supplier. The data is encrypted with Pretty Good Privacy (PGP) encryption. The company needs a solution that will automatically decrypt the data after the company receives the data.

A solutions architect will use a Transfer Family managed workflow. The company has created an IAM service role by using an IAM policy that allows access to AWS Secrets Manager and the S3 bucket. The role's trust relationship allows the transfer.amazonaws.com service to assume the role.

What should the solutions architect do next to complete the solution for automatic decryption?

- A. Store the PGP public key in Secrets Manager. Add a nominal step in the Transfer Family managed workflow to decrypt files. Configure PGP encryption parameters in the nominal step. Associate the workflow with the Transfer Family server.
- B. Store the PGP private key in Secrets Manager. Add an exception-handling step in the Transfer Family managed workflow to decrypt files. Configure PGP encryption parameters in the exception handler. Associate the workflow with the SFTP user.
- C. Store the PGP private key in Secrets Manager. Add a nominal step in the Transfer Family managed workflow to decrypt files. Configure PGP decryption parameters in the nominal step. Associate the workflow with the Transfer Family server.
- D. Store the PGP public key in Secrets Manager. Add an exception-handling step in the Transfer Family managed workflow to decrypt files. Configure PGP decryption parameters in the exception handler. Associate the workflow with the SFTP user.

Correct Answer: C

Community vote distribution

C (100%)

 **zapper1234** Highly Voted 1 year, 6 months ago

The answer should be "C" because you store the "private" key in Secrets Manager
upvoted 7 times

 **AzureDP900** Most Recent 1 year, 1 month ago

C and D are pretty similar however D talks about exception handling. C is right answer
upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

store the PGP private key in Secrets Manager. Add a nominal step in the Transfer Family managed workflow to decrypt files.
upvoted 1 times

 **mark_232323** 1 year, 5 months ago

Selected Answer: C

C correct

upvoted 1 times

 **dzhang344** 1 year, 5 months ago

Selected Answer: C

C, for sure.

upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

C, for sure.

In the context of AWS Transfer Family managed workflows, a ""nominal step"" refers to one of the predefined steps that you can include in a managed workflow to automate file transfer and processing tasks.

An ""exception-handling step"" is a specific type of step designed to handle errors or exceptions that occur during the execution of a workflow.

upvoted 3 times

 **grandcanyon** 1 year, 5 months ago

Selected Answer: C

C is correct b/c private key is what is required for decryption

upvoted 2 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: C

Agree with Zapper1234 plus the permission is granted to transfer family server.

upvoted 2 times

Question #483

Topic 1

A company is migrating infrastructure for its massive multiplayer game to AWS. The game's application features a leaderboard where players can see rankings in real time. The leaderboard requires microsecond reads and single-digit-millisecond write latencies. The datasets are single-digit terabytes in size and must be available to accept writes in less than a minute if a primary node failure occurs.

The company needs a solution in which data can persist for further analytical processing through a data pipeline.

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

- B. Create an Amazon RDS database with a read replica. Configure the application to point writes to the writer endpoint. Configure the application to point reads to the reader endpoint.
- C. Create an Amazon MemoryDB for Redis cluster in Multi-AZ mode. Configure the application to interact with the primary node.
- D. Create multiple Redis nodes on Amazon EC2 instances that are spread across multiple Availability Zones. Configure backups to Amazon S3.

Correct Answer: C*Community vote distribution*

C (71%)

B (29%)

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

where is A?

upvoted 8 times

 **zapper1234** Highly Voted 1 year, 6 months ago

memobrydb for ultra-fast Redis performance, so C

upvoted 8 times

 **Sum19** Most Recent 2 months ago

Selected Answer: C

Amazon MemoryDB for Redis is specifically designed for this exact use case:

1. Ultra-low latency: Provides microsecond read latency required for real-time leaderboards
2. Fast writes: Single-digit millisecond write performance
3. Durability: Unlike ElastiCache, MemoryDB provides data persistence with transaction logs
4. Multi-AZ failover: Automatic failover in under 1 minute
5. Fully managed: Minimal operational overhead compared to self-managed solutions
6. Analytics ready: Persistent data can be accessed by data pipelines for further processing

MemoryDB combines the performance of Redis with the durability and reliability needed for this gaming application while being fully managed by AWS.

upvoted 1 times

 **Murtuza** 2 months, 3 weeks ago

Selected Answer: B

Here is your choice A.

A. (Amazon DynamoDB with Global Secondary Index): DynamoDB delivers single-digit millisecond latency for both reads and writes, but the requirement is microsecond reads. While DynamoDB is fully managed and supports leaderboards, MemoryDB is the only one that meets the strict microsecond read latency.

upvoted 1 times

 **eesa** 8 months, 4 weeks ago

Selected Answer: C

where is A?

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

C is right. Amazon MemoryDB for Redis is a fully managed, Redis-compatible, in-memory database service that delivers ultra-fast performance with microsecond read and single-digit millisecond write latencies. It supports Multi-AZ replication for high availability and durability. If the primary node fails, MemoryDB automatically fails over to a replica node in less than a minute.

upvoted 2 times

 **TomTom** 1 year, 1 month ago

Selected Answer: B

To meet the requirements of low latency and high availability for a gaming leaderboard, Amazon MemoryDB for Redis is the best solution. It provides microsecond read latencies and single-digit millisecond write latencies, ensuring fast data access and updates, which is critical for real-time applications like leaderboards.

This setup minimizes operational overhead compared to managing multiple EC2 instances or configuring a traditional RDS database

upvoted 1 times

 **TomTom** 1 year, 1 month ago

Wrongly tick, should be C

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: C

MEM DB for gaming leaderboard with related latency requirement

upvoted 3 times

 **rohan0411** 1 year, 5 months ago

It is C for sure

upvoted 2 times

Question #484

A company is running several applications in the AWS Cloud. The applications are specific to separate business units in the company. The company is running the components of the applications in several AWS accounts that are in an organization in AWS Organizations.

Every cloud resource in the company's organization has a tag that is named BusinessUnit. Every tag already has the appropriate value of the business unit name.

The company needs to allocate its cloud costs to different business units. The company also needs to visualize the cloud costs for each business unit.

Which solution will meet these requirements?

- A. In the organization's management account, create a cost allocation tag that is named BusinessUnit. Also in the management account, create an Amazon S3 bucket and an AWS Cost and Usage Report (AWS CUR). Configure the S3 bucket as the destination for the AWS CUR. From the management account, query the AWS CUR data by using Amazon Athena. Use Amazon QuickSight for visualization.
- B. In each member account, create a cost allocation tag that is named BusinessUnit. In the organization's management account, create an Amazon S3 bucket and an AWS Cost and Usage Report (AWS CUR). Configure the S3 bucket as the destination for the AWS CUR. Create an Amazon CloudWatch dashboard for visualization.
- C. In the organization's management account, create a cost allocation tag that is named BusinessUnit. In each member account, create an Amazon S3 bucket and an AWS Cost and Usage Report (AWS CUR). Configure each S3 bucket as the destination for its respective AWS CUR. In the management account, create an Amazon CloudWatch dashboard for visualization.
- D. In each member account, create a cost allocation tag that is named BusinessUnit. Also in each member account, create an Amazon S3 bucket and an AWS Cost and Usage Report (AWS CUR). Configure each S3 bucket as the destination for its respective AWS CUR. From the management account, query the AWS CUR data by using Amazon Athena. Use Amazon QuickSight for visualization.

Correct Answer: A

Community vote distribution

A (100%)

 **zapper1234** Highly Voted 1 year, 6 months ago

You need Athena and Quicksight so I say A
upvoted 6 times

 **altonh** Most Recent 10 months, 1 week ago

Selected Answer: A

Although I believe the correct answer is A, the statement "create a cost allocation tag" seemed to be incorrect. You need to Activate the tag, not create it.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

A right

The cost allocation tag is attached to all resources in the organization's management account, which allows for easy identification of costs associated with each business unit.

The S3 bucket and AWS CUR are created in the management account, which simplifies the process of storing and querying cost data. Amazon Athena can be used from the management account to query the AWS CUR data, allowing for easy visualization and analysis of costs across different business units.

Amazon QuickSight is also available in the management account, providing a user-friendly interface for visualizing the cost data.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: A

By centralizing the cost allocation tag, AWS CUR, and data analysis in the management account, this solution ensures consistent tagging and cost allocation across the organization. It also provides a single source of truth for cost and usage data, enabling efficient querying and visualization using Athena and QuickSight.

upvoted 1 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: A

Create tag in management account

Use Athena + QuickSight

upvoted 2 times

 **gfhbox0083** 1 year, 5 months ago

A, for sure

upvoted 1 times

 **NoInNothing** 1 year, 5 months ago

Selected Answer: A

Answer is "A"

upvoted 1 times

 **grandcanyon** 1 year, 5 months ago

Selected Answer: A

A is the best answer

upvoted 1 times

 **d7ccbf6** 1 year, 6 months ago

Selected Answer: A

You need Athena and Quicksight to visualize CUR

upvoted 1 times

Question #485

A utility company wants to collect usage data every 5 minutes from its smart meters to facilitate time-of-use metering. When a meter sends data to AWS, the data is sent to Amazon API Gateway, processed by an AWS Lambda function, and stored in an Amazon DynamoDB table. During the pilot phase, the Lambda functions took from 3 to 5 seconds to complete.

As more smart meters are deployed, the engineers notice the Lambda functions are taking from 1 to 2 minutes to complete. The functions are also increasing in duration as new types of metrics are collected from the devices. There are many ProvisionedThroughputExceededException errors while performing PUT operations on DynamoDB, and there are also many TooManyRequestsException errors from Lambda.

Which combination of changes will resolve these issues? (Choose two.)

- A. Increase the write capacity units to the DynamoDB table.
- B. Increase the memory available to the Lambda functions.
- C. Increase the payload size from the smart meters to send more data.
- D. Stream the data into an Amazon Kinesis data stream from API Gateway and process the data in batches.
- E. Collect data in an Amazon SQS FIFO queue, which triggers a Lambda function to process each message

Correct Answer: AD

Community vote distribution

AD (100%)

 **mifune** Highly Voted 1 year, 6 months ago

Selected Answer: AD

I would go with Increasing the write capacity units to the DynamoDB table and Stream the data into an Amazon Kinesis data stream from API Gateway and process the data in batches. I think that processing the data in batches is much better than increasing the lambda functions memory.

upvoted 6 times

 **zapper1234** Highly Voted 1 year, 6 months ago

AB because the more memory a Lambda function has the faster it reacts

upvoted 6 times

 **0b43291** Most Recent 1 year, 1 month ago

Selected Answer: AD

By increasing the DynamoDB write capacity units and streaming the data into a Kinesis data stream for batch processing, you can address the throughput limitations, reduce Lambda invocation overhead, and improve the overall performance and scalability of the smart meter data processing pipeline.

The other options are either not applicable or may not resolve the issues effectively:

B. Increasing the memory available to the Lambda functions may not resolve the issues caused by the high volume of concurrent requests and the need for batching.

C. Increasing the payload size from the smart meters is not necessary and may even exacerbate the issues by increasing the processing overhead for each data point.

E. Collecting data in an Amazon SQS FIFO queue and triggering a Lambda function for each message would still result in a high number of Lambda invocations and may not provide significant performance improvements compared to processing data in batches from a Kinesis data stream.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: AD

Kinesis allows to process data in batches, which can help reduce the number of requests and the load on your Lambda functions and DynamoDB.

upvoted 4 times

 **wbedair** 1 year, 6 months ago

Selected Answer: AD

A and D

upvoted 3 times

 **ujizane** 1 year, 6 months ago

need batch execution so i think AD is correct

upvoted 2 times

Question #486

A company recently completed a successful proof of concept of Amazon WorkSpaces. A solutions architect needs to make the solution highly available across two AWS Regions. Amazon WorkSpaces is deployed in a failover Region, and a hosted zone is deployed in Amazon Route 53.

What should the solutions architect do to configure high availability for the solution?

- A. Create a connection alias in the primary Region and in the failover Region. Associate the connection aliases with a directory in each Region. Create a Route 53 failover routing policy. Set Evaluate Target Health to Yes.
- B. Create a connection alias in the primary Region and in the failover Region. Associate the connection aliases with a directory in the primary Region. Create a Route 53 multivalue answer routing policy.
- C. Create a connection alias in the primary Region. Associate the connection alias with a directory in the primary Region. Create a Route 53 weighted routing policy.
- D. Create a connection alias in the primary Region. Associate the connection alias with a directory in the failover Region. Create a Route 53 failover routing policy. Set Evaluate Target Health to Yes.

Correct Answer: A*Community vote distribution*

A (75%)

D (25%)

✉  **ujizane**  1 year, 6 months ago

Selected Answer: A

A

https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/cross-region-redirection.html
upvoted 7 times

✉  **d7ccbf6**  1 year, 6 months ago

Selected Answer: D

<https://docs.aws.amazon.com/workspaces/latest/adminguide/cross-region-redirection.html#cross-region-redirection-associate-connection-aliases>
upvoted 6 times

✉  **toma** 1 year, 6 months ago

you are right.
upvoted 3 times

✉  **vip2** 1 year, 5 months ago

I think you mean A with link that you provided
upvoted 2 times

✉  **bhanus**  1 year ago

Selected Answer: A

<https://docs.aws.amazon.com/workspaces/latest/adminguide/cross-region-redirection.html#cross-region-redirection-create-connection-aliases>

Using the same AWS account, create connection aliases in each primary and failover Region where you want to set up cross-Region redirection.

upvoted 1 times

✉  **AzureDP900** 1 year, 1 month ago

A is right
Creating connection aliases in both Regions ensures that users can access the WorkSpaces instance from either region.

Associating the connection aliases with directories in each Region allows for load balancing and redirection of traffic between the two Regions.

Creating a Route 53 failover routing policy enables Amazon Route 53 to direct users from the primary Region to the failover Region if there's an issue with the primary Region.

Setting Evaluate Target Health to Yes ensures that Route 53 continuously monitors the health of the WorkSpaces instance in both Regions and directs traffic accordingly.

upvoted 3 times

✉  **0b43291** 1 year, 1 month ago

Selected Answer: A

By following Option A, you can achieve high availability for your Amazon WorkSpaces solution across two AWS Regions, with automatic failover and health monitoring provided by the Route 53 failover routing policy and connection aliases associated with WorkSpaces directories in each Region.

The other options are either incomplete or incorrect:

Option B (multivalue answer routing policy) is not suitable for failover scenarios, as it distributes traffic across multiple resources simultaneously, rather than failing over to a secondary resource when the primary becomes unavailable.

Option C (weighted routing policy) is used for distributing traffic based on predefined weights, but it does not provide automatic failover capabilities based on health checks.

Option D is incorrect because it associates the connection alias with the failover Region's directory, which would make the failover Region the primary deployment, defeating the purpose of having a failover configuration.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: A

"You can associate a connection alias with ONLY ONE directory per AWS Region."

So, it can't be D.

upvoted 1 times

 **PSPaul** 1 year, 4 months ago

For A: Potential latency increase due to cross-region access

For B: Potential data consistency issues if failover occurs

I choose A

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: A

A is correct

upvoted 2 times

 **Moghite** 1 year, 5 months ago

Selected Answer: A

I will go with option A

upvoted 2 times

 **mark_232323** 1 year, 5 months ago

Selected Answer: A

A for sure

upvoted 4 times

 **NoInNothing** 1 year, 5 months ago

Answer is A -

A. Create a connection alias in the primary Region and in the failover Region. Associate the connection aliases with a directory in each Region. Create a Route 53 failover routing policy. Set Evaluate Target Health to Yes.

upvoted 3 times

 **ujizane** 1 year, 6 months ago

A

https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/cross-region-redirection.html

upvoted 3 times

 **zapper1234** 1 year, 6 months ago

Believe the answer is A because the two distinct Workspaces directories would give you two IP's for true failover

upvoted 4 times

Question #487

A company plans to migrate many VMs from an on-premises environment to AWS. The company requires an initial assessment of the on-premises environment before the migration, a visualization of the dependencies between applications that run on the VMs, and a report that provides an assessment of the on-premises environment.

To get this information, the company has initiated a Migration Evaluator assessment request. The company has the ability to install collector software in its on-premises environment without any constraints

Which solution will provide the company with the required information with the LEAST operational overhead?

- A. Install the AWS Application Discovery Agent on each on-premises VM. After the data collection period ends, use AWS Migration Hub to view the application dependencies. Download the Quick insights assessment report from Migration Hub.
- B. Install the Migration Evaluator Collector on each on-premises VM. After the data collection period ends, use Migration Evaluator to view the application dependencies. Download and export the discovered server list from Migration Evaluator. Upload the list to Amazon QuickSight. When the QuickSight report is generated, download the Quick Insights assessment report.
- C. Setup the AWS Application Discovery Service Agentless Collector in the on-premises environment. After the data collection period ends, use AWS Migration Hub to view the application dependencies. Export the discovered server list from Application Discovery Service. Upload the list to Migration Evaluator. When the Migration Evaluator report is generated, download the Quick Insights assessment.
- D. Set up the Migration Evaluator Collector in the on-premises environment. Install the AWS Application Discovery Agent on each VM. After the data collection period ends, use AWS Migration Hub to view the application dependencies. Download the Quick Insights assessment report from Migration Evaluator.

Correct Answer: A

Community vote distribution

A (62%)	C (27%)	5%
---------	---------	----

 **5ehjry6sktukliyliulykutjhy** Highly Voted 1 year, 5 months ago

Selected Answer: C

For VMs use agentless unless you need to track network
upvoted 8 times

 **Spike2020** 1 year, 2 months ago

requirement is to discover application dependency. So that needs to track network. So it should be A.
upvoted 2 times

 **Russ99** Highly Voted 1 year, 5 months ago

Selected Answer: A

Option C is not the least operation overhead. it requires Application Discovery agentless Collector + Export & Upload of the report. also, Discovery agentless will not gather data for all dependencies.
upvoted 8 times

 **DANMUSO** Most Recent 7 months ago

Selected Answer: D

D. Set up the Migration Evaluator Collector in the on-premises environment. Install the AWS Application Discovery Agent on each VM. After the data collection period ends, use AWS Migration Hub to view the application dependencies. Download the Quick Insights assessment report from Migration Evaluator.

- Fulfils the Migration Evaluator requirement (assessment and Quick Insights).
- Fulfils the dependency mapping requirement (via Application Discovery Agent).
- Uses Migration Hub to visualize dependencies.
- Provides a Quick Insights assessment report, as the question requires.
- Minimal operational overhead, since you're allowed to install software freely
upvoted 2 times

 **zhen234** 11 months, 1 week ago

Selected Answer: B

The Migration Evaluator Collector is better for high-level assessment and cost planning, while the Application Discovery Agentless Collector is suited for detailed dependency analysis between applications and VMs.

upvoted 1 times

 **BeyondCoder** 11 months, 2 weeks ago

Selected Answer: C

Option C is correct.

https://aws.amazon.com/about-aws/whats-new/2024/11/network-connections-aws-application-discovery-service-agentless-collector/?nc1=h_ls

upvoted 1 times

 **TomTom** 1 year, 1 month ago

Selected Answer: B

The solution that provides the company with the required information with the least operational overhead is B: Install the Migration Evaluator Collector on each on-premises VM.

This method allows for efficient data collection, enabling the use of Migration Evaluator to visualize application dependencies and download the Quick Insights assessment report easily. This approach minimizes complexity compared to options that require multiple software installations or data transfers between services, thus reducing operational overhead significantly

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

This solution requires minimal operational overhead as it only involves installing a small agent (AWS Application Discovery Agent) on each VM, which can be done without disrupting the environment.

The AWS Application Discovery Service is an agentless collector that can discover resources in your organization without requiring any configuration or agent installation. However, in this case, the company has already initiated a Migration Evaluator assessment request and can use the built-in capabilities of Migration Hub to collect information about their on-premises environment.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

A is correct

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: A

Option A is the answer with the least operational overhead because it leverages the AWS Application Discovery Agent, which can be installed on each on-premises VM to collect configuration data, performance metrics, and application dependencies. AWS Migration Hub integrates with Application Discovery Service, providing a centralized view of discovered servers, dependencies, and migration status. Migration Hub allows visualizing application dependencies and provides the Quick Insights assessment report, fulfilling all requirements. By using a single agent and Migration Hub's built-in capabilities, Option A minimizes operational overhead and provides a streamlined solution for the required information.

upvoted 2 times

 **Danm86** 1 year, 2 months ago

I think option A is correct

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: A

"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."

upvoted 3 times

 **Syre** 1 year, 2 months ago

Selected Answer: A

The question clearly states, "The company has the ability to install collector software in its on-premises environment without any constraints"

upvoted 3 times

 **Chungies** 1 year, 3 months ago

They have the capability of accepting installs on their VM so I will go with A. It can not be the agent less because there is no mention that they can not allow installs on their VMs

upvoted 1 times

 **asquared16** 1 year, 4 months ago

Selected Answer: C

the key word here is "many" VMs, hence C.

upvoted 1 times

 **toma** 1 year, 5 months ago

it should be A, as you can see on this link: <https://aws.amazon.com/migration-evaluator/> agentless collector should be used, it is simple.

upvoted 2 times

 **toma** 1 year, 5 months ago

sorry i wanted to say C

upvoted 1 times

 **5ehjry6sktukliyliulykutjhy** 1 year, 5 months ago

Option C: Use Agentless for VMs

upvoted 1 times

 **mifune** 1 year, 6 months ago

Selected Answer: A

"To get this information, the company has initiated a Migration Evaluator assessment request. The company has the ability to install collector software in its on-premises environment without any constraints", so I understand from the question that the next step would be installing the AWS Application Discovery Agent on each on-premises VM, so for me the answer is A.

upvoted 7 times

 **zapper1234** 1 year, 6 months ago

B is the correct answer because you would use migration evaluator

upvoted 4 times

Question #488

Topic 1

A company hosts its primary API on AWS by using an Amazon API Gateway API and AWS Lambda functions that contain the logic for the API methods. The company's internal applications use the API for core functionality and business logic. The company's customers use the API to access data from their accounts. Several customers also have access to a legacy API that is running on a single standalone Amazon EC2 instance.

The company wants to increase the security for these APIs to better prevent denial of service (DoS) attacks, check for vulnerabilities, and guard against common exploits.

What should a solutions architect do to meet these requirements?

- A. Use AWS WAF to protect both APIs. Configure Amazon Inspector to analyze the legacy API. Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs.
- B. Use AWS WAF to protect the API Gateway API. Configure Amazon Inspector to analyze both APIs. Configure Amazon GuardDuty to block malicious attempts to access the APIs.
- C. Use AWS WAF to protect the API Gateway API. Configure Amazon Inspector to analyze the legacy API. Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs.
- D. Use AWS WAF to protect the API Gateway API! Configure Amazon Inspector to protect the legacy API. Configure Amazon GuardDuty to block malicious attempts to access the APIs.

Correct Answer: C

Community vote distribution

C (91%) 9%

 **ebbf63** Highly Voted 1 year, 6 months ago

Selected Answer: C

GuardDuty only monitors but doesn't block malicious attempts. So answer is C
upvoted 12 times

 **Helpnosense** Highly Voted 1 year, 6 months ago

Selected Answer: C

Not A because the question only say "Several customers also have access to a legacy API that is running on a single standalone Amazon EC2 instance." There is no ALB or cloudfront mentioned so WAF can't be attached to EC2 directly.
upvoted 7 times

 **0b43291** Most Recent 1 year, 1 month ago

Selected Answer: C

The correct answer is Option C: Use AWS WAF to protect the API Gateway API. Configure Amazon Inspector to analyze the legacy API. Configure Amazon GuardDuty to monitor for malicious attempts to access the APIs.

Option C is the right choice because it directly addresses the requirement of increasing security for the API Gateway API by using AWS WAF to protect it from DoS attacks, vulnerabilities, and exploits. It also correctly suggests using Amazon Inspector to assess the security posture of the EC2 instance hosting the legacy API, and configures Amazon GuardDuty to monitor for malicious attempts across both APIs.

In contrast, Option A does not explicitly mention protecting the API Gateway API and incorrectly suggests using Inspector to analyze the legacy API application itself.

upvoted 1 times

 **Danm86** 1 year, 2 months ago

Option C seems to be correct. In Option B, it's mentioned AWS inspector to analyze both the gateway API and EC2 API. AWS inspector cannot directly monitor gateway API, it requires additional WAF configuration for it.

upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

C, for sure.

AWS GuardDuty is a monitoring and threat detection service and does not directly block malicious activities. GuardDuty is designed to continuously monitor and analyze your AWS accounts and workloads for potential threats using machine learning, anomaly detection, and integrated threat intelligence.

upvoted 1 times

 **mifune** 1 year, 6 months ago

Selected Answer: A

"The company wants to increase the security for these APIs to better prevent denial of service (DoS) attacks, check for vulnerabilities, and guard against common exploits.", so I understand that we have to protect BOTH, and GuardDuty does not block anything... The answer for me is A

upvoted 2 times

✉️  **toma** 1 year, 6 months ago

how are you going to attache WAF to ec2? :)

upvoted 4 times

✉️  **zapper1234** 1 year, 6 months ago

B because this protects both API's

upvoted 1 times

Question #489

Topic 1

A company is running a serverless ecommerce application on AWS. The application uses Amazon API Gateway to invoke AWS Lambda Java functions. The Lambda functions connect to an Amazon RDS for MySQL database to store data.

During a recent sale event, a sudden increase in web traffic resulted in poor API performance and database connection failures. The company needs to implement a solution to minimize the latency for the Lambda functions and to support bursts in traffic.

Which solution will meet these requirements with the LEAST amount of change to the application?

- A. Update the code of the Lambda functions so that the Lambda functions open the database connection outside of the function handler. Increase the provisioned concurrency for the Lambda functions.
- B. Create an RDS Proxy endpoint for the database. Store database secrets in AWS Secrets Manager. Set up the required IAM permissions. Update the Lambda functions to connect to the RDS Proxy endpoint. Increase the provisioned concurrency for the Lambda functions.
- C. Create a custom parameter group. Increase the value of the max_connections parameter. Associate the custom parameter group with the RDS DB instance and schedule a reboot. Increase the reserved concurrency for the Lambda functions.
- D. Create an RDS Proxy endpoint for the database. Store database secrets in AWS Secrets Manager. Set up the required IAM permissions. Update the Lambda functions to connect to the RDS Proxy endpoint. Increase the reserved concurrency for the Lambda functions.

Correct Answer: B

Community vote distribution

B (67%)	D (19%)	14%
---------	---------	-----

 **ebbf63** Highly Voted 1 year, 6 months ago

Provisioned Concurrency - makes sure Lambda functions could handle traffic bursts
 RDS proxy endpoint - intelligently manages connections to a relational database (Amazon RDS here) So, the answer - B
 upvoted 6 times

 **mifune** 1 year, 6 months ago

yes, I would go with "Provisioned concurrency" too.
 upvoted 3 times

 **mifune** Highly Voted 1 year, 6 months ago

Selected Answer: B

If cost is a primary concern, Reserved Concurrency could be a more economical choice. Provisioned Concurrency is designed to provide more control over your Lambda function's performance and scalability. Answer is B.
 upvoted 5 times

 **TomTom** Most Recent 1 year ago

Selected Answer: A

Option A is likely the best choice.
 It involves a straightforward adjustment to how database connections are handled without introducing new services or significantly altering existing infrastructure. While it still requires some code changes, these are limited compared to Options B, C, and D.

In summary, while using AWS Secrets Manager (as in Options B and D) provides security benefits, it also introduces more complexity and significant changes to your existing setup. Therefore, if minimizing changes is your primary goal, Option A (updating the Lambda function code for connection handling) is the most suitable choice.
 upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

B is correct

This solution requires minimal changes to the application:

- Creating an RDS Proxy endpoint and updating the Lambda functions to use it is a relatively minor modification.
- Store database secrets in AWS Secrets Manager adds some complexity, but it is still a manageable change.
- Increasing provisioned concurrency for the Lambda functions can help handle bursts in traffic without requiring significant changes to the application.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: B

By leveraging RDS Proxy, AWS Secrets Manager, and increasing provisioned concurrency, Option B provides a scalable and secure solution with minimal changes to the application code, making it the most appropriate choice for meeting the requirements.

The other options have drawbacks or require more significant changes to the application:

Option A: While it suggests increasing provisioned concurrency, opening database connections outside the function handler may not be a best practice and could lead to connection leaks or other issues.

Option C: Increasing the max_connections parameter on the RDS instance may not be sufficient to handle bursts in traffic and could potentially impact performance. Additionally, it requires scheduling a reboot, which could cause downtime.

Option D: While it correctly suggests using RDS Proxy, AWS Secrets Manager, and increasing reserved concurrency, it does not mention provisioned concurrency, which is more suitable for handling bursts in traffic.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: B

Connection Pooling: RDS Proxy helps manage database connections efficiently by pooling and reusing connections. Reduced Latency: By reducing the overhead of establishing new connections for each Lambda invocation, RDS Proxy improves the overall performance, minimizing the latency experienced by your application during traffic bursts. Provisioned Concurrency: Increasing the provisioned concurrency for the Lambda functions ensures they are always ready to handle spikes in traffic, reducing cold start times. Seamless Integration: The integration with AWS Lambda and Secrets Manager ensures that the database credentials are securely managed. IAM Permissions: The use of AWS Identity and Access Management (IAM) permissions to control access to the proxy ensures security and compliance, making this solution secure and scalable.

upvoted 3 times

 **vip2** 1 year, 5 months ago

Selected Answer: B

B is correct for least operation(not cost effectively) in question

upvoted 4 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: A

A is right answer. D is wrong because the provisioned Concurrency is the term to keep pre-allocated warm instances of lambda not reserved concurrency. B missing auto scaling the db.

upvoted 2 times

 **tgv** 1 year, 4 months ago

"LEAST amount of change to the application"

B doesn't need auto-scaling if you're using RDS Proxy

upvoted 1 times

 **ebbf63** 1 year, 6 months ago

Selected Answer: B

Answer B

upvoted 1 times

 **Alagong** 1 year, 6 months ago

Selected Answer: D

Option D with "reserved concurrency" can be more cost-effective and flexible for handling sudden traffic bursts, as it ensures a minimum number of instances without the potential over-provisioning of provisioned concurrency.

upvoted 4 times

 **zapper1234** 1 year, 6 months ago

Sorry, meant A

upvoted 1 times

Question #490

Topic 1

A company requires that all internal application connectivity use private IP addresses. To facilitate this policy, a solutions architect has created interface endpoints to connect to AWS Public services. Upon testing, the solutions architect notices that the service names are resolving to public IP addresses, and that internal services cannot connect to the interface endpoints.

Which step should the solutions architect take to resolve this issue?

- A. Update the subnet route table with a route to the interface endpoint.
- B. Enable the private DNS option on the VPC attributes.
- C. Configure the security group on the interface endpoint to allow connectivity to the AWS services.
- D. Configure an Amazon Route 53 private hosted zone with a conditional forwarder for the internal application.

Correct Answer: B

Community vote distribution

B (92%)	8%
---------	----

✉  **ebbf63** Highly Voted 1 year, 6 months ago

Selected Answer: B

ensures proper DNS resolution for VPC endpoints.
upvoted 6 times

✉  **AzureDP900** Most Recent 1 year, 1 month ago

By choosing option B, the solutions architect can enable private DNS on the VPC attributes, which will resolve service names to private IP addresses, allowing internal applications to connect to interface endpoints without issues.
upvoted 1 times

✉  **0b43291** 1 year, 1 month ago

Selected Answer: B

The correct step the solutions architect should take to resolve the issue of service names resolving to public IP addresses and internal services not being able to connect to the interface endpoints is Option B: Enable the private DNS option on the VPC attributes.

When you create an interface endpoint, AWS automatically creates a private DNS name for the service that resolves to the private IP addresses of the interface endpoint. However, by default, the private DNS option is disabled on the VPC, which means that DNS queries for the service name will be resolved using the public DNS instead of the private DNS provided by the interface endpoint.

By enabling the private DNS option on the VPC attributes, you instruct the VPC to use the private DNS names provided by the interface endpoints for the specified AWS services. This ensures that the service names resolve to the private IP addresses of the interface endpoints, allowing internal services within the VPC to connect to the AWS services using private IP addresses, as per the company's policy.

upvoted 3 times

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

Selected Answer: B

B .. .because we had exact this problem once. C would be right if name would be resolved to a private IP, but as described it is not, it resolves to the public ip, so B
upvoted 1 times

✉  **backbencher2022** 1 year, 4 months ago

Selected Answer: B

Sorry, Ignore my previous comment. private DNS would solve the issue. Option B is correct
upvoted 1 times

✉  **backbencher2022** 1 year, 4 months ago

Selected Answer: C

C (security group) is correct. Private DNS resolution is neither a mandatory pre-requisite to use interface endpoints nor a requirement in this question. If you read the question again, resolving to a public IP is a distractor which makes us think that private DNS (option B) is the correct option. The real problem is the 2nd issue of the question - not able to connect which is a security group configuration issue. Even if you don't want to use private DNS, your interface endpoint will still work however, without security group rule configured, you can't use interface endpoint at all. Check this document for a list of pre-requisites - <https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html> and 2nd point says "To use private DNS..." which implies you may or may not want to use Private DNS however, 4th pre-requisite "Create a security group...." is mandatory.

upvoted 1 times

✉  **altonh** 10 months, 1 week ago

Agree. Besides, it seems the option to "Enable private DNS only for inbound endpoint" is to optimize networking costs.

upvoted 1 times

 **dzidis** 1 year, 5 months ago

Here in prerequisites for interface endpoint:

To use private DNS, you must enable DNS hostnames and DNS resolution for your VPC. For more information, see View and update DNS attributes in the Amazon VPC User Guide.

<https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html>

upvoted 1 times

 **mifune** 1 year, 6 months ago

Selected Answer: B

Private DNS for Interface Endpoints. Answer B.

upvoted 1 times

Question #491

Topic 1

A company is developing a latency-sensitive application. Part of the application includes several AWS Lambda functions that need to initialize as quickly as possible. The Lambda functions are written in Java and contain initialization code outside the handlers to load libraries, initialize classes, and generate unique IDs.

Which solution will meet the startup performance requirement MOST cost-effectively?

- A. Move all the initialization code to the handlers for each Lambda function. Activate Lambda SnapStart for each Lambda function. Configure SnapStart to reference the \$LATEST version of each Lambda function.
- B. Publish a version of each Lambda function. Create an alias for each Lambda function. Configure each alias to point to its corresponding version. Set up a provisioned concurrency configuration for each Lambda function to point to the corresponding alias.
- C. Publish a version of each Lambda function. Set up a provisioned concurrency configuration for each Lambda function to point to the corresponding version. Activate Lambda SnapStart for the published versions of the Lambda functions.
- D. Update the Lambda functions to add a pre-snapshot hook. Move the code that generates unique IDs into the handlers. Publish a version of each Lambda function. Activate Lambda SnapStart for the published versions of the Lambda functions.

Correct Answer: D

Community vote distribution

D (80%)

C (20%)

 Russ99 Highly Voted 1 year, 6 months ago

Selected Answer: D

While option B improves startup performance, it is generally more expensive than SnapStart because it keeps environments warm continuously.

upvoted 5 times

 AzureDP900 Most Recent 1 year, 1 month ago

Option D is right

This solution provides a good balance between performance and code organization. By moving the code that generates unique IDs into the handlers, you keep the initialization code out of the way, but still make it accessible when needed.

The pre-snapshot hook allows you to run some initialization code before the Lambda function is executed, which can be useful for tasks like generating unique IDs.

Publishing a version of each Lambda function and activating SnapStart ensures that the functions are running with the latest code and optimizations.

upvoted 1 times

 JoeTromundo 1 year, 2 months ago

Selected Answer: D

For those who think option C is correct: as dzidis commented, "SnapStart does NOT support PROVISIONED CONCURRENCY"
<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

upvoted 2 times

 zolthar_z 1 year, 4 months ago

Selected Answer: D

<https://aws.amazon.com/blogs/compute/reducing-java-cold-starts-on-aws-lambda-functions-with-snapstart/>

upvoted 2 times

 backbencher2022 1 year, 4 months ago

Selected Answer: D

D is correct and as dzidis referred to AWS document, you can't use both provisioned concurrency and SnapStart for the same function version. Therefore, C can't be a correct option. Refer to this section of document for more details:
<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html#snapstart-concurrency>

upvoted 1 times

 dzidis 1 year, 4 months ago

Selected Answer: D

You can't use both SnapStart and provisioned concurrency on the same function version.

Therefore cannot be C.

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

upvoted 3 times

 **vip2** 1 year, 5 months ago

Selected Answer: D

D

Combining provisioned concurrency with SnapStart is redundant

While provisioned concurrency reduces cold start latency, it is more costly compared to SnapStart because it keeps a set number of instances warm and ready to handle requests, even when not in use.

upvoted 3 times

 **5ehjry6sktukliyliulykutjhy** 1 year, 5 months ago

Selected Answer: C

It is C

upvoted 1 times

 **mifune** 1 year, 6 months ago

Selected Answer: C

"Lambda SnapStart for Java can improve startup performance for latency-sensitive applications by up to 10x at no extra cost". Answer C.

upvoted 2 times

 **ebbf63** 1 year, 6 months ago

Selected Answer: C

Leverages both versioning and provisioned concurrency. Also Lambda SnapStart for improved startup performance.

upvoted 1 times

Question #492

Topic 1

A solutions architect is importing a VM from an on-premises environment by using the Amazon EC2 VM Import feature of AWS Import/Export. The solutions architect has created an AMI and has provisioned an Amazon EC2 instance that is based on that AMI. The EC2 instance runs inside a public subnet in a VPC and has a public IP address assigned.

The EC2 instance does not appear as a managed instance in the AWS Systems Manager console.

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

- A. Verify that Systems Manager Agent is installed on the instance and is running.
- B. Verify that the instance is assigned an appropriate IAM role for Systems Manager.
- C. Verify the existence of a VPC endpoint on the VPC.
- D. Verify that the AWS Application Discovery Agent is configured.
- E. Verify the correct configuration of service-linked roles for Systems Manager.

Correct Answer: AB

Community vote distribution

AB (100%)

 **ebbfff63** Highly Voted 1 year, 6 months ago

Answer:AB

SSM Agent - must for communication between EC2 instances and Systems Manager
Appropriate IAM role allows the instance to interact with Systems Manager services
upvoted 9 times

 **toma** 1 year, 6 months ago

correct.

upvoted 2 times

 **AzureDP900** Most Recent 1 year, 1 month ago

A & B are right options.

The EC2 instance not appearing as a managed instance in the AWS Systems Manager console suggests that the Systems Manager Agent is not running or is not properly configured.

By verifying that the Systems Manager Agent is installed and running on the instance, the solutions architect can ensure that the agent is collecting metrics and data from the instance.

Assigning an appropriate IAM role to the instance for Systems Manager ensures that the agent has the necessary permissions to collect data and perform management tasks.

upvoted 1 times

 **Chungies** 1 year, 3 months ago

I will go with A and B because with SSM agent it has to be installed on the VM and there has to be a role for it that allows it to interact with systems manager

upvoted 1 times

 **Daniel76** 1 year, 3 months ago

Selected Answer: AB

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

upvoted 2 times

 **G4Exams** 1 year, 5 months ago

Selected Answer: AB

I also go for A and B. A, the agent for sure and I think B because without the role it would definitely have no access to that instance. I don't know why D should be related to the scenario.

upvoted 1 times

Question #493

Topic 1

A company is using AWS CloudFormation as its deployment tool for all applications. It stages all application binaries and templates within Amazon S3 buckets with versioning enabled. Developers have access to an Amazon EC2 instance that hosts the integrated development environment (IDE). The developers download the application binaries from Amazon S3 to the EC2 instance, make changes, and upload the binaries to an S3 bucket after running the unit tests locally. The developers want to improve the existing deployment mechanism and implement CI/CD using AWS CodePipeline.

The developers have the following requirements:

- Use AWS CodeCommit for source control.
- Automate unit testing and security scanning.
- Alert the developers when unit tests fail.
- Turn application features on and off, and customize deployment dynamically as part of CI/CD.
- Have the lead developer provide approval before deploying an application.

Which solution will meet these requirements?

- A. Use AWS CodeBuild to run unit tests and security scans. Use an Amazon EventBridge rule to send Amazon SNS alerts to the developers when unit tests fail. Write AWS Cloud Development Kit (AWS CDK) constructs for different solution features, and use a manifest file to turn features on and off in the AWS CDK application. Use a manual approval stage in the pipeline to allow the lead developer to approve applications.
- B. Use AWS Lambda to run unit tests and security scans. Use Lambda in a subsequent stage in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Write AWS Amplify plugins for different solution features and utilize user prompts to turn features on and off. Use Amazon SES in the pipeline to allow the lead developer to approve applications.
- C. Use Jenkins to run unit tests and security scans. Use an Amazon EventBridge rule in the pipeline to send Amazon SES alerts to the developers when unit tests fail. Use AWS CloudFormation nested stacks for different solution features and parameters to turn features on and off. Use AWS Lambda in the pipeline to allow the lead developer to approve applications.
- D. Use AWS CodeDeploy to run unit tests and security scans. Use an Amazon CloudWatch alarm in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Use Docker images for different solution features and the AWS CLI to turn features on and off. Use a manual approval stage in the pipeline to allow the lead developer to approve applications.

Correct Answer: A*Community vote distribution*

A (100%)

 **ebbf63** Highly Voted  1 year, 6 months ago

- A- Yes
B - No - Lambda not optimal for unit testing
c- No - Jenkins needs separate management not part of the AWS native services
D - No - CodeDeploy is for deployment, not to run unit tests and security scans

upvoted 10 times

 **AzureDP900** Most Recent 1 year, 1 month ago

By choosing option A, the developers can meet all of their requirements and implement a robust CI/CD pipeline that integrates with AWS services.
Using AWS CodeBuild to run unit tests and security scans meets the requirement of automating these tasks.
The use of Amazon EventBridge rules to send SNS alerts when unit tests fail meets the requirement of alerting developers when tests fail.
Writing AWS CDK constructs for different solution features allows for dynamic customization of deployment, meeting the requirement of turning features on and off.
Using a manifest file to control feature toggling in the AWS CDK application provides a centralized way to manage these changes, making it easier to customize deployment dynamically.
The manual approval stage using AWS CodePipeline allows the lead developer to provide approval before deploying an application, meeting this requirement.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: A

By leveraging AWS CodeBuild, EventBridge, SNS, AWS CDK, and manual approval stages in CodePipeline, Option A provides a comprehensive solution that meets all the requirements for implementing CI/CD using AWS CodePipeline.

Option B: AWS Lambda is not suitable for running unit tests and security scans. Additionally, using Amplify plugins and user prompts for

feature toggling may not be as flexible as using AWS CDK constructs and a manifest file.

Option C: Using Jenkins for unit testing and security scanning introduces an additional tool to manage and maintain. Additionally, using nested stacks and parameters for feature toggling may not be as flexible as using AWS CDK constructs and a manifest file.

Option D: AWS CodeDeploy is primarily used for application deployment, not for running unit tests and security scans. Additionally, using Docker images and the AWS CLI for feature toggling may not be as flexible as using AWS CDK constructs and a manifest file.

upvoted 1 times

 **backbencher2022** 1 year, 4 months ago

Selected Answer: A

A is correct option - <https://docs.aws.amazon.com/codebuild/latest/userguide/test-reporting.html>

upvoted 1 times

 **ryuhei** 1 year, 4 months ago

Selected Answer: A

I think A is the correct answer because I will be testing with codebuild.

upvoted 1 times

 **5ehjry6sktukliyliulykutjhy** 1 year, 5 months ago

Selected Answer: A

Codebuild looks good

upvoted 2 times

Question #494

Topic 1

A global ecommerce company has many data centers around the world. With the growth of its stored data, the company needs to set up a solution to provide scalable storage for legacy on-premises file applications. The company must be able to take point-in-time copies of volumes by using AWS Backup and must retain low-latency access to frequently accessed data. The company also needs to have storage volumes that can be mounted as Internet Small Computer System Interface (iSCSI) devices from the company's on-premises application servers.

Which solution will meet these requirements?

- A. Provision an AWS Storage Gateway tape gateway. Configure the tape gateway to store data in an Amazon S3 bucket. Deploy AWS Backup to take point-in-time copies of the volumes.
- B. Provision an Amazon FSx File Gateway and an Amazon S3 File Gateway. Deploy AWS Backup to take point-in-time copies of the data.
- C. Provision an AWS Storage Gateway volume gateway in cache mode. Back up the on-premises Storage Gateway volumes with AWS Backup.
- D. Provision an AWS Storage Gateway file gateway in cache mode. Deploy AWS Backup to take point-in-time copies of the volumes.

Correct Answer: C

Community vote distribution

C (100%)

 **ebbf63** Highly Voted 1 year, 6 months ago

Selected Answer: C

Answer C - a comprehensive solution for all the requirements for scalable storage, low-latency access, point-in-time backups, and iSCSI device support

upvoted 8 times

 **AzureDP900** Most Recent 1 year, 1 month ago

Selected Answer: C

C meets security and compliance requirements by storing sensitive data within the company's own storage infrastructure (on-premises) while still leveraging the scalability, durability, and flexibility of the cloud.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

C correct because

Amazon FSx File Gateway is not required for this scenario, as the storage volumes can be backed up and restored using AWS Storage Gateway.

The "cache" mode of the Storage Gateway volume gateway does provide low-latency access to frequently accessed data, meeting one of the company's requirements.

The Storage Gateway file gateway can be used to mount storage volumes as iSCSI devices from on-premises application servers, meeting another requirement.

AWS Backup is a widely supported backup solution that can take point-in-time copies of data, meeting the company's requirement for backup and recovery.

upvoted 2 times

 **backbencher2022** 1 year, 4 months ago

Selected Answer: C

C is correct - <https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html>

upvoted 1 times

 **AhmedSalem** 1 year, 5 months ago

Selected Answer: C

Answer C

upvoted 1 times

 **paderni** 1 year, 5 months ago

B with Amazon FSx File Gateway and S3 File Gateway, along with AWS Backup for data protection, best aligns with the company's requirements for scalable storage, low-latency access, point-in-time backups, and integration with on-premises applications.

upvoted 1 times

 **mifune** 1 year, 6 months ago

Selected Answer: C

iSCSI ---> AWS Storage Gateway volume gateway

upvoted 3 times

✉️  **zapper1234** 1 year, 6 months ago

B because you need iSCSI interface
upvoted 2 times

✉️  **marchelok** 1 year, 6 months ago

C..."and must retain low-latency access to frequently accessed data"
upvoted 4 times

Question #495

Topic 1

A company has an application that uses AWS Key Management Service (AWS KMS) to encrypt and decrypt data. The application stores data in an Amazon S3 bucket in an AWS Region. Company security policies require the data to be encrypted before the data is placed into the S3 bucket. The application must decrypt the data when the application reads files from the S3 bucket.

The company replicates the S3 bucket to other Regions. A solutions architect must design a solution so that the application can encrypt and decrypt data across Regions. The application must use the same key to decrypt the data in each Region.

Which solution will meet these requirements?

- A. Create a KMS multi-Region primary key. Use the KMS multi-Region primary key to create a KMS multi-Region replica key in each additional Region where the application is running. Update the application code to use the specific replica key in each Region.
- B. Create a new customer managed KMS key in each additional Region where the application is running. Update the application code to use the specific KMS key in each Region.
- C. Use AWS Private Certificate Authority to create a new certificate authority (CA) in the primary Region. Issue a new private certificate from the CA for the application's website URL. Share the CA with the additional Regions by using AWS Resource Access Manager (AWS RAM). Update the application code to use the shared CA certificates in each Region.
- D. Use AWS Systems Manager Parameter Store to create a parameter in each additional Region where the application is running. Export the key material from the KMS key in the primary Region. Store the key material in the parameter in each Region. Update the application code to use the key data from the parameter in each Region.

Correct Answer: A

Community vote distribution

A (100%)

 **ebbf63** Highly Voted 1 year, 6 months ago

Selected Answer: A

A- straightforward - encryption and decryption across regions using multi-region key
upvoted 11 times

 **AzureDP900** Most Recent 1 year, 1 month ago

A) Create a KMS multi-Region primary key. Use the KMS multi-Region primary key to create a KMS multi-Region replica key in each additional Region where the application is running. Update the application code to use the specific replica key in each Region. To meet the requirements, you need to use the same key to decrypt data across Regions, while also using AWS Key Management Service (KMS) to manage encryption and decryption.

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option A

Creating a KMS multi-region primary key allows you to manage encryption keys across multiple Regions.

A KMS multi-region primary key can be used to create a KMS multi-region replica key, which can then be used to encrypt and decrypt data in other Regions.

The application code can be updated to use the specific replica key in each Region, ensuring that the same key is used for encryption and decryption across all Regions.

The other options do not meet all of the requirements:

upvoted 1 times

 **backbencher2022** 1 year, 4 months ago

Selected Answer: A

A is the correct answer as per this AWS documentation - <https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html#:~:text=A%20multi%2DRegion%20primary%20key%20is%20a%20KMS%20key%20that,primary%20key%20can%20be%20replicated.>

upvoted 1 times

 **AhmedSalem** 1 year, 5 months ago

Selected Answer: A

Answer A. AWS KMS multi-Region keys allow you to replicate keys across multiple Regions, ensuring that the same key material is available in each Region.

upvoted 1 times

Question #496

Topic 1

A company hosts an application that uses several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). During the initial startup of the EC2 instances, the EC2 instances run user data scripts to download critical content for the application from an Amazon S3 bucket.

The EC2 instances are launching correctly. However, after a period of time, the EC2 instances are terminated with the following error message: "An instance was taken out of service in response to an ELB system health check failure." EC2 instances continue to launch and be terminated because of Auto Scaling events in an endless loop.

The only recent change to the deployment is that the company added a large amount of critical content to the S3 bucket. The company does not want to alter the user data scripts in production.

What should a solutions architect do so that the production environment can deploy successfully?

- A. Increase the size of the EC2 instances.
- B. Increase the health check timeout for the ALB.
- C. Change the health check path for the ALB.
- D. Increase the health check grace period for the Auto Scaling group.

Correct Answer: D

Community vote distribution

D (90%)	10%
---------	-----

 **ebbf63** Highly Voted 1 year, 6 months ago

Selected Answer: D

D. Increase the health check grace period
upvoted 9 times

 **AhmedSalem** Highly Voted 1 year, 5 months ago

Selected Answer: D

Answer D.
Extending the grace period allows the instances more time to complete their startup tasks, including downloading the additional content from S3, before health checks start. This solution does not require altering the user data scripts in production, which aligns with the company's requirements.
upvoted 7 times

 **nimbus_00** Most Recent 1 year ago

Selected Answer: D

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/health-check-grace-period.html#:~:text=In%20the%20console%2C%20by%20default,the%20health%20check%20grace%20period.>
upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

D is right.
Since the EC2 instances are being terminated due to an ELB system health check failure, it's likely that the health checks are timing out while the user data scripts are still running and downloading content from S3. This causes the ALB to think the instance is unhealthy, leading to termination.

By increasing the health check grace period for the Auto Scaling group, you give the instances more time to complete their startup process, including the execution of the user data scripts, before considering them healthy or unhealthy. This should prevent the endless loop of launching and terminating EC2 instances due to health check failures.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: D

Correct answer: D - The grace period in Auto Scaling allows new instances time to finish initialization (like downloading data or running user scripts) before health checks start. By increasing this grace period, you provide more time for the EC2 instances to complete the startup process and avoid premature termination.

Incorrect answer: B - This only extends the time the ALB waits for a response on a health check, but if the EC2 instance isn't ready to serve requests due to its long initialization time, it will still fail the health check.

upvoted 1 times

liuliangzhou 1 year, 3 months ago

Selected Answer: B

I prefer B over D:

The problem is that EC2 instances need to download content from S3 during the startup process, which may take some time. If ALB's health check is performed during this period and the EC2 instance is unable to respond to the health check request due to incomplete downloads, ALB may consider the instance unhealthy and remove it from the service. This may trigger the auto scaling group to start new instances, creating an endless loop.

upvoted 2 times

AzureDP900 1 year, 1 month ago

D is right

Increasing the health check timeout might allow more time for the user data scripts to run, but it doesn't give the instance a chance to recover and become healthy before termination.

upvoted 1 times

Question #497

Topic 1

A company needs to move some on-premises Oracle databases to AWS. The company has chosen to keep some of the databases on premises for business compliance reasons.

The on-premises databases contain spatial data and run cron jobs for maintenance. The company needs to connect to the on-premises systems directly from AWS to query data as a foreign table.

Which solution will meet these requirements?

- A. Create Amazon DynamoDB global tables with auto scaling enabled. Use the AWS Schema Conversion Tool (AWS SCT) and AWS Database Migration Service (AWS DMS) to move the data from on premises to DynamoDB. Create an AWS Lambda function to move the spatial data to Amazon S3. Query the data by using Amazon Athena. Use Amazon EventBridge to schedule jobs in DynamoDB for maintenance. Use Amazon API Gateway for foreign table support.
- B. Create an Amazon RDS for Microsoft SQL Server DB instance. Use native replication to move the data from on premises to the DB instance. Use the AWS Schema Conversion Tool (AWS SCT) to modify the SQL Server schema as needed after replication. Move the spatial data to Amazon Redshift. Use stored procedures for system maintenance. Create AWS Glue crawlers to connect to the on-premises Oracle databases for foreign table support.
- C. Launch Amazon EC2 instances to host the Oracle databases. Place the EC2 instances in an Auto Scaling group. Use AWS Application Migration Service to move the data from on premises to the EC2 instances and for real-time bidirectional change data capture (CDC) synchronization. Use Oracle native spatial data support. Create an AWS Lambda function to run maintenance jobs as part of an AWS Step Functions workflow. Create an internet gateway for foreign table support.
- D. Create an Amazon RDS for PostgreSQL DB instance. Use the AWS Schema Conversion Tool (AWS SCT) and AWS Database Migration Service (AWS DMS) to move the data from on premises to the DB instance. Use PostgreSQL native spatial data support. Run cron jobs on the DB instance for maintenance. Use AWS Direct Connect to connect the DB instance to the on-premises environment for foreign table support.

Correct Answer: D*Community vote distribution*

D (100%)

  **JoeTromundo** 1 year, 2 months ago**Selected Answer: D**

PostgreSQL natively supports spatial data through the PostGIS extension. This makes it well-suited for handling spatial data from the Oracle databases. AWS Schema Conversion Tool (SCT) and AWS Database Migration Service (DMS) are both effective tools for migrating schema and data from Oracle to Amazon RDS for PostgreSQL, ensuring minimal disruption during the migration process. Amazon RDS for PostgreSQL allows the use of cron jobs directly on the instance through extensions like pg_cron for scheduling maintenance tasks. AWS Direct Connect provides a dedicated, secure connection between the on-premises systems and the AWS environment. This low-latency link will allow querying data from on-premises Oracle databases as foreign tables in the PostgreSQL instance without going through the internet, which supports compliance and performance needs.

upvoted 4 times

  **neta1o** 1 year, 4 months ago**Selected Answer: D**

I didn't realize SCT could convert from Oracle to things like Aurora MySQL and PostgreSQL. But since that is true and a direct connect also makes sense, I'd go D. <https://aws.amazon.com/dms/schema-conversion-tool/>

upvoted 2 times

  **Helpnosense** 1 year, 6 months ago**Selected Answer: D**

It's Data Migration Service that provides real-time bidirectional change data capture (CDC) synchronization

upvoted 2 times

  **goldeneye** 1 year, 6 months ago**Selected Answer: D**

Option D is the most appropriate because it leverages AWS services effectively to migrate and manage the databases while ensuring compatibility with spatial data types and maintaining connectivity for querying on-premises data.

upvoted 3 times

  **goldeneye** 1 year, 6 months ago

Option D is the most appropriate because it leverages AWS services effectively to migrate and manage the databases while ensuring compatibility with spatial data types and maintaining connectivity for querying on-premises data.

upvoted 2 times

 **mifune** 1 year, 6 months ago

Selected Answer: D

PostgreSQL has native support for spatial data, which is required by the company, so answer for me is D

upvoted 3 times

Question #498

Accompany runs an application on Amazon EC2 and AWS Lambda. The application stores temporary data in Amazon S3. The S3 objects are deleted after 24 hours.

The company deploys new versions of the application by launching AWS CloudFormation stacks. The stacks create the required resources. After validating a new version, the company deletes the old stack. The deletion of an old development stack recently failed. A solutions architect needs to resolve this issue without major architecture changes.

Which solution will meet these requirements?

- A. Create a Lambda function to delete objects from an S3 bucket. Add the Lambda function as a custom resource in the CloudFormation stack with a DependsOn attribute that points to the S3 bucket resource.
- B. Modify the CloudFormation stack to attach a DeletionPolicy attribute with a value of Delete to the S3 bucket.
- C. Update the CloudFormation stack to add a DeletionPolicy attribute with a value of Snapshot for the S3 bucket resource
- D. Update the CloudFormation template to create an Amazon Elastic File System (Amazon EFS) file system to store temporary files instead of Amazon S3. Configure the Lambda functions to run in the same VPC as the EFS file system.

Correct Answer: A*Community vote distribution*

A (88%) 8%

 **gfhbox0083** Highly Voted  1 year, 5 months ago

Selected Answer: A

A, for sure.

DeletionPolicy: Delete: The DeletionPolicy attribute in CloudFormation is used to specify what should happen to a resource when the stack is deleted. The value Delete indicates that CloudFormation should delete the resource (in this case, the S3 bucket) when the stack is deleted.

Non-Empty Buckets: The problem with this approach is that CloudFormation cannot delete an S3 bucket if it contains any objects. The DeletionPolicy: Delete does not change this behavior; it only specifies that the bucket should be deleted, which will still fail if the bucket is not empty.

upvoted 6 times

 **SIJUTHOMASP** Most Recent  1 year ago

Selected Answer: A

Repeated question.

upvoted 2 times

 **nimbus_00** 1 year ago

Selected Answer: A

common scenario.

<https://repost.aws/questions/QUvAaCd6J7To-Fs-eReXMgNg/to-add-an-aws-custom-resource-to-cloudformation-template-and-provide-an-aws-lambda-function>

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

A is right

By creating a Lambda function that deletes objects from the S3 bucket, you can ensure that the old CloudFormation stack is deleted even if the deletion process fails.

Attaching this Lambda function as a custom resource in the CloudFormation stack allows CloudFormation to wait for the delete operation to complete before proceeding with the deletion of the old stack.

The DependsOn attribute ensures that the Lambda function runs after the S3 bucket has been deleted, preventing any potential issues with deleting objects that may not be removed yet.

Attaching this custom resource solves the issue without requiring major architecture changes.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: A

By using a Lambda function as a custom resource, you can ensure that the Lambda function deletes the objects in the S3 bucket before CloudFormation attempts to delete the bucket itself. Adding the DependsOn attribute ensures that the S3 bucket resource will not be deleted until the Lambda function has completed its task of clearing out all objects from the bucket, thus avoiding any errors caused by attempting to delete a non-empty S3 bucket. Options B and C: These options will not work because the DeletionPolicy attribute does NOT trigger the deletion of the OBJECTS INSIDE THE BUCKET. It ONLY determines what happens to the BUCKET RESOURCE ITSELF, not its contents. The stack deletion will still fail if objects remain in the bucket. Option D introduces significant architectural changes, which are unnecessary for solving the stack deletion issue.

upvoted 2 times

 **gfhbox0083** 1 year, 5 months ago

A, for sure.

DeletionPolicy: Delete: The DeletionPolicy attribute in CloudFormation is used to specify what should happen to a resource when the stack is deleted. The value Delete indicates that CloudFormation should delete the resource (in this case, the S3 bucket) when the stack is deleted.

Non-Empty Buckets: The problem with this approach is that CloudFormation cannot delete an S3 bucket if it contains any objects. The DeletionPolicy: Delete does not change this behavior; it only specifies that the bucket should be deleted, which will still fail if the bucket is not empty.

upvoted 2 times

 **ahrentom** 1 year, 5 months ago

Selected Answer: A

you can't delete a S3 bucket with objects in it. So A is correct

upvoted 3 times

 **Russs99** 1 year, 5 months ago

Selected Answer: B

By setting the Deletion Policy attribute to Delete in the stack, you ensure that the S3 bucket and its contents are deleted when the CloudFormation stack is deleted. This best option for the scenario and aligns with the desired behavior of removing old resources when the stack is deleted.

upvoted 1 times

 **Alagong** 1 year, 5 months ago

Selected Answer: A

IT SHOULD BE A

upvoted 3 times

 **AhmedSalem** 1 year, 5 months ago

Selected Answer: A

I will go for A.

Using Lambda function as a custom resource ensures that the S3 bucket is emptied before the stack is deleted. DependsOn Attribute ensures the Lambda function runs and completes before attempting to delete the S3 bucket, thus preventing deletion failure.

upvoted 4 times

 **grandcanyon** 1 year, 5 months ago

Selected Answer: B

When you specify a DeletionPolicy attribute with a value of Delete for an S3 bucket in a CloudFormation template, CloudFormation will delete the bucket and all its contents during stack deletion. This approach addresses the issue of the stack deletion failing due to the bucket not being empty.

upvoted 1 times

 **Helpnosense** 1 year, 6 months ago

Selected Answer: C

Votes C. After s3 snapshot, cloud formation will proceed s3 bucket deletion. A is right but compare to c it doesn't match the requirement in the question. "resolve this issue without major architecture changes."

Also the data become useless only after 24 hours. A delete everything regardless. C is better.

upvoted 1 times

 **toma** 1 year, 6 months ago

it should be A

upvoted 4 times

 **mifune** 1 year, 6 months ago

Selected Answer: A

"DependsOn" attribute ensures that the Lambda function will always be invoked before the S3 bucket is deleted in a CloudFormation. Answer A.

upvoted 1 times

Question #499

A company has an application that stores user-uploaded videos in an Amazon S3 bucket that uses S3 Standard storage. Users access the videos frequently in the first 180 days after the videos are uploaded. Access after 180 days is rare. Named users and anonymous users access the videos.

Most of the videos are more than 100 MB in size. Users often have poor internet connectivity when they upload videos, resulting in failed uploads. The company uses multipart uploads for the videos.

A solutions architect needs to optimize the S3 costs of the application.

Which combination of actions will meet these requirements? (Choose two.)

- A. Configure the S3 bucket to be a Requester Pays bucket.
- B. Use S3 Transfer Acceleration to upload the videos to the S3 bucket.
- C. Create an S3 Lifecycle configuration to expire incomplete multipart uploads 7 days after initiation.
- D. Create an S3 Lifecycle configuration to transition objects to S3 Glacier Instant Retrieval after 1 day.
- E. Create an S3 Lifecycle configuration to transition objects to S3 Standard-Infrequent Access (S3 Standard- IA) after 180 days.

Correct Answer: CE*Community vote distribution*

CE (88%)

13%

 **d401c0d** 10 months, 2 weeks ago

Selected Answer: CE

Couldn't have said it better than JoeTromundo
upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: CE

C: Incomplete multipart uploads consume unnecessary storage and increase costs, especially with large files like videos. Setting a lifecycle policy to automatically delete incomplete uploads after 7 days helps reduce unnecessary storage costs without manual intervention.
E: The videos are frequently accessed in the first 180 days and rarely accessed after that. Transitioning the videos to S3 Standard-IA after 180 days reduces costs while still providing immediate retrieval when needed. S3 Standard-IA is designed for infrequently accessed data and offers lower storage costs than S3 Standard while maintaining fast access times.
Why not B? S3 Transfer Acceleration improves upload speeds for users with poor internet connectivity, but it INCURS ADDITIONAL COSTS. While this can help with uploads, it does NOT directly optimize STORAGE COSTS, which is the main goal here.
upvoted 3 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: CE

CE for sure.

Why not B?

The root cause for failed upload is due to that fact that user has poor internet connectivity. That's not something transfer accelerator can help with, maybe the user need to find a better internet provider, or use Elon's star link

upvoted 1 times

 **Russ99** 1 year, 5 months ago

Selected Answer: CE

CE are the best options. In option C, incomplete upload should be deleted to save costs.
upvoted 1 times

 **AhmedSalem** 1 year, 5 months ago

Selected Answer: CE

From the cost management perspective, the answer should be CE
upvoted 1 times

 **ujizane** 1 year, 6 months ago

Selected Answer: CE

Cost Optimization so CE
upvoted 3 times

 **ujizane** 1 year, 6 months ago

Cost Optimization so CE

upvoted 2 times

 **mifune** 1 year, 6 months ago

Selected Answer: BE

B - for transfers of files over long distances between your client and an S3 bucket | E - for reducing cost for data that is accessed less frequently.

upvoted 2 times

 **ebbf63** 1 year, 6 months ago

Selected Answer: CE

C - optimizes the S3 storage costs effectively

E - address frequent access in the first 180 days and infrequent access afterward

upvoted 4 times

 **zapper1234** 1 year, 6 months ago

B and E are the only ones that make sense to me

upvoted 3 times

 **toma** 1 year, 6 months ago

B is not related to cost optimization.

upvoted 1 times

Question #500

Topic 1

A company runs an ecommerce web application on AWS. The web application is hosted as a static website on Amazon S3 with Amazon CloudFront for content delivery. An Amazon API Gateway API invokes AWS Lambda functions to handle user requests and order processing for the web application. The Lambda functions store data in an Amazon RDS for MySQL DB cluster that uses On-Demand instances. The DB cluster usage has been consistent in the past 12 months.

Recently, the website has experienced SQL injection and web exploit attempts. Customers also report that order processing time has increased during periods of peak usage. During these periods, the Lambda functions often have cold starts. As the company grows, the company needs to ensure scalability and low-latency access during traffic peaks. The company also must optimize the database costs and add protection against the SQL injection and web exploit attempts.

Which solution will meet these requirements?

- A. Configure the Lambda functions to have an increased timeout value during peak periods. Use RDS Reserved Instances for the database. Use CloudFront and subscribe to AWS Shield Advanced to protect against the SQL injection and web exploit attempts.
- B. Increase the memory of the Lambda functions, Transition to Amazon Redshift for the database. Integrate Amazon Inspector with CloudFront to protect against the SQL injection and web exploit attempts.
- C. Use Lambda functions with provisioned concurrency for compute during peak periods, Transition to Amazon Aurora Serverless for the database. Use CloudFront and subscribe to AWS Shield Advanced to protect against the SQL injection and web exploit attempts.
- D. Use Lambda functions with provisioned concurrency for compute during peak periods. Use RDS Reserved Instances for the database. Integrate AWS WAF with CloudFront to protect against the SQL injection and web exploit attempts.

Correct Answer: D

Community vote distribution

D (79%)

C (21%)

 **ebbf63** Highly Voted 1 year, 6 months ago

Selected Answer: D

D - AWS WAF for SQL injection and web exploit protection
upvoted 10 times

 **Blair77** Most Recent 2 months, 3 weeks ago

Selected Answer: D

Option C (Aurora Serverless) is a great solution for the highly variable traffic and automatic scaling needs. It directly addresses the cost optimization and scalability requirements. However, as you noted, it does not provide the application-level security against SQL injection that the question explicitly requires. This makes it an incomplete solution.

Option D provides the most comprehensive and balanced approach by addressing all four key requirement
upvoted 1 times

 **0dc6cac** 6 months, 1 week ago

Selected Answer: D

C is wrong because AWS shield advanced doesn't help against SQL injections. But the bigger concern IMO is the serverless DB, considering that the question mentions consistent load with several bursts. You'd have a heart attack when you get the bill at the end of the month.
upvoted 2 times

 **nimbus_00** 1 year ago

Selected Answer: D

"DB cluster that uses On-Demand instances. The DB cluster usage has been consistent in the past 12 months." suggests RDS Reserved Instances for the database.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithReservedDBInstances.html
upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: D

By leveraging Lambda functions with provisioned concurrency, RDS Reserved Instances, and AWS WAF with CloudFront, Option D provides a comprehensive solution addressing low-latency access during traffic peaks, optimizing database costs, and adding protection against SQL injection and web exploit attempts, meeting all stated requirements.

Option C: While Aurora Serverless addresses database scalability and cost, AWS Shield Advanced may be unnecessary if SQL injection and web exploits are the primary concern, which AWS WAF can mitigate.

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: D

It's D: Provisioned Concurrency ensures that Lambda functions are pre-warmed and ready to handle requests instantly, which reduces the "cold start" problem. RDS Reserved Instances for Amazon RDS will help reduce the database cost. Since the workload has been consistent over the past 12 months, Reserved Instances provide a cost-effective solution by offering significant discounts compared to On-Demand pricing. AWS WAF protects the application from web exploits such as SQL injection and cross-site scripting (XSS).

upvoted 2 times

 **wbedair** 1 year, 3 months ago

Selected Answer: D

waf for sql injection and web exploits

upvoted 2 times

 **wbedair** 1 year, 3 months ago

Selected Answer: C

expanding business needs serverless database so Aurora in option C is the best

upvoted 1 times

 **wbedair** 1 year, 3 months ago

It looks like I was looking at different question as no mention in the question to use serverless database. I will go with D

upvoted 1 times

 **Isaac_lin** 1 year, 4 months ago

using shield advanced will enable the basic features of WAF for free as well, so C

upvoted 1 times

 **Daniel76** 1 year, 3 months ago

Shield Advanced is not free, and it's used against DDoS, not SQL injection.

upvoted 1 times

 **asquared16** 1 year, 4 months ago

Selected Answer: C

Regardless of the diabolical wording of the question. Forget about whether it's WAF or Shield Advance, it's 'C' because it drills down to saying "the company is now expecting growth and needs to ensure scalability", this pushes us to Aurora Serverless. DB usage was consistent last year, it no longer is.

upvoted 3 times

 **vip2** 1 year, 5 months ago

Selected Answer: D

AWS WAF instead of AWS Shield

upvoted 3 times

 **gfhbox0083** 1 year, 5 months ago

D, for sure.

To protect against SQL injection attacks, AWS WAF (Web Application Firewall) is the appropriate service to use, not AWS Shield Advanced.

upvoted 2 times

 **mifune** 1 year, 6 months ago

Selected Answer: C

Lambda functions with provisioned concurrency for compute during peak periods + Aurora Serverless + AWS Shield Advanced, I don't see any better choice. Answer C.

upvoted 2 times

 **zapper1234** 1 year, 6 months ago

C - using Lambda concurrency with Aurora Serverless solves a bunch of the issues

upvoted 1 times

 **toma** 1 year, 6 months ago

it is D, no need for AWS Shield Advanced, WAF is sufficient.

upvoted 2 times

 **kupo777** 1 year, 6 months ago

it is D, AWS Shield Advanced is not required; AWS WAF can be used to protect against common web exploits such as SQL injection and cross-site scripting (XSS) attacks.

upvoted 2 times

Question #501

A company runs a web application on a single Amazon EC2 instance. End users experience slow application performance during times of peak usage, when CPU utilization is consistently more than 95%.

A user data script installs required custom packages on the EC2 instance. The process of launching the instance takes several minutes.

The company is creating an Auto Scaling group that has mixed instance groups, varied CPUs, and a maximum capacity limit. The Auto Scaling group will use a launch template for various configuration options. The company needs to decrease application latency when new instances are launched during auto scaling.

Which solution will meet these requirements?

- A. Use a predictive scaling policy. Use an instance maintenance policy to run the user data script. Set the default instance warmup time to 0 seconds.
- B. Use a dynamic scaling policy. Use lifecycle hooks to run the user data script. Set the default instance warmup time to 0 seconds.
- C. Use a predictive scaling policy. Enable warm pools for the Auto Scaling group. Use an instance maintenance policy to run the user data script.
- D. Use a dynamic scaling policy. Enable warm pools for the Auto Scaling group. Use lifecycle hooks to run the user data script.

Correct Answer: D*Community vote distribution*

D (50%)	B (25%)	13%	13%
---------	---------	-----	-----

 **aka1177** 3 weeks, 3 days ago

Selected Answer: D

Starting Nov 4, 2025 you can enable warm pools for an Auto Scaling group (ASG) with mixed instance types.
<https://aws.amazon.com/about-aws/whats-new/2025/11/ec2-auto-scaling-warm-pool-mixed-instances-policies/>.

So D is the right answer
 upvoted 1 times

 **jimee11** 7 months, 1 week ago

Selected Answer: B

You can't add a warm pool to an ASG that has mixed instances policy. Predictive is based on historic data and is too rigid for this scenario.
 upvoted 1 times

 **sergza888** 7 months, 3 weeks ago

Selected Answer: A

It is poorly asked question but I lean towards A "In general, if you have regular patterns of traffic increases and applications that take a long time to initialize, you should consider using predictive scaling. Predictive scaling can help you scale faster by launching capacity in advance of forecasted load, compared to using only dynamic scaling, which is reactive in nature." And you can not use C and D for Mixed Instance types. Life Hooks will run before instance becomes InService so warm timeout could be set to 0 and Predictive can improve Latencies <https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html> as I don't see how B can do it
 upvoted 2 times

 **zhen234** 11 months, 1 week ago

Selected Answer: C

An instance maintenance policy in the context of AWS Auto Scaling governs how instances are handled before they are fully launched and available for use. It defines the actions that need to occur (such as running a user data script, applying patches, or installing software) to ensure the instance is ready. When combined with features like warm pools, maintenance policies can ensure instances are prepared in advance and reduce delays during scaling events. These policies help ensure instances are fully initialized before serving traffic.

upvoted 2 times

 **altonh** 10 months, 1 week ago

Nope. An instance maintenance policy affects Amazon EC2 Auto Scaling events that cause instances to be replaced.
 upvoted 1 times

 **henrikhmkharyan59** 1 year ago

Selected Answer: B

@songilly provided an exhaustive comment explaining why B is the only viable answer
 upvoted 2 times

✉  **alexbraila** 1 year ago

Selected Answer: B

Due to the link in songilly's comment, which clearly states D is out. I am almost sure they were looking for knowledge of "warm pools", but here is another poorly written AWS question

upvoted 1 times

✉  **horiuchi** 1 year ago

Selected Answer: D

No mention of any peak period so there's no way to use predictive scaling

The problem occurs cause the VMs take too long to boot up and be ready to accept requests, the only thing to do is to have them already "warm".

And I've never heard of a "maintenance mode" and I know that lifecycle hooks are a common practice with ASGs

Warm pools

Lifecycle hooks are how

upvoted 1 times

✉  **songilly** 1 year, 1 month ago

You can't use a warm pool in an Auto Scaling group with mixed instances policy or has spot instances:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-warm-pools.html>

So not sure how D can be write. Although B doesn't seem great it might be the only viable option.

upvoted 3 times

✉  **Daniel76** 1 year, 3 months ago

Selected Answer: D

Agree with D

There is no mention of predictable peak period. Since there's a known metric where user experience skippiness, dynamic scaling should be used.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html#:~:text=A%20dynamic%20scaling%20policy%20instructs,CloudWatch%20alarm%20is%20in%20ALARM.>

Use warm pool to reduce latency and cost of unnecessary standby instance.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-warm-pools.html>

Use lifecycle hook due to the need to install custom packages

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

More reference:

<https://aws.amazon.com/blogs/compute/introducing-instance-maintenance-policy-for-amazon-ec2-auto-scaling/>

upvoted 3 times

✉  **altonh** 10 months, 1 week ago

But why do you need a lifecycle hook just to run a script? It is already a user data script, so there is no need for this.

upvoted 1 times

✉  **vip2** 1 year, 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

✉  **Alagong** 1 year, 5 months ago

Selected Answer: D

Answer : D

upvoted 1 times

✉  **AhmedSalem** 1 year, 5 months ago

Selected Answer: D

Answer D

upvoted 1 times

✉  **kupo777** 1 year, 6 months ago

B

AWS Database Migration Service can convert Oracle and SQL Server to Amazon RDS for MySQL and Amazon RDS for PostgreSQL stored procedures.

D

AWS Database Migration Service (AWS DMS) performs data migration.

The answer is DB.

upvoted 1 times

✉  **wbedair** 1 year, 6 months ago

looks like this is an answer for different question

upvoted 3 times

Question #502

A company needs to migrate its on-premises database fleet to Amazon RDS. The company is currently using a mixture of Microsoft SQL Server, MySQL, and Oracle databases. Some of the databases have custom schemas and stored procedures.

Which combination of steps should the company take for the migration? (Choose two.)

- A. Use Migration Evaluator Quick Insights to analyze the source databases and to identify the stored procedures that need to be migrated.
- B. Use AWS Application Migration Service to analyze the source databases and to identify the stored procedures that need to be migrated.
- C. Use the AWS Schema Conversion Tool (AWS SCT) to analyze the source databases for changes that are required
- D. Use AWS Database Migration Service (AWS DMS) to migrate the source databases to Amazon RDS.
- E. Use AWS DataSync to migrate the data from the source databases to Amazon RDS.

Correct Answer: CD*Community vote distribution*

CD (100%)

 **ebbf63** Highly Voted 1 year, 6 months ago

Selected Answer: CD

Answer CD

upvoted 7 times

 **AzureDP900** Most Recent 1 year, 1 month ago

CD

Using both AWS SCT and AWS DMS will provide the necessary tools for a successful database migration. AWS SCT helps with identifying the changes needed during migration, while AWS DMS provides a managed service for executing the migration.

upvoted 1 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: CD

A. AWS does not have a service directly named 'Migration Evaluator Quick Insights'.

B. AWS Application Migration Service is primarily used for migrating virtual machines rather than analyzing them.

C. AWS SCT can analyze the source database and identify potential architecture changes needed for successful migration to Amazon RDS.
D. AWS DMS is a data migration service.

E. AWS DataSync is a service used for quickly migrating large amounts of data between local storage and AWS storage services, with a focus on file level data migration. But database migration requires maintaining data integrity, relationships, constraints, and so on.

upvoted 1 times

 **Moghite** 1 year, 5 months ago

Selected Answer: CD

answer CD

upvoted 1 times

 **AhmedSalem** 1 year, 5 months ago

Selected Answer: CD

Answer CD

upvoted 1 times

 **kupo777** 1 year, 6 months ago

B

AWS Database Migration Service can convert Oracle and SQL Server to Amazon RDS for MySQL and Amazon RDS for PostgreSQL stored procedures.

D

AWS Database Migration Service (AWS DMS) performs data migration.

The answer is DB.

upvoted 1 times

 **awsaz** 1 year, 6 months ago

Selected Answer: CD

C and D

upvoted 4 times

Question #503

Topic 1

A company is migrating its blog platform to AWS. The company's on-premises servers connect to AWS through an AWS Site-to-Site VPN connection. The blog content is updated several times a day by multiple authors and is served from a file share on a network-attached storage (NAS) server.

The company needs to migrate the blog platform without delaying the content updates. The company has deployed Amazon EC2 instances across multiple Availability Zones to run the blog platform behind an Application Load Balancer. The company also needs to move 200 TB of archival data from its on-premises servers to Amazon S3 as soon as possible.

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

- A. Create a weekly cron job in Amazon EventBridge. Use the cron job to invoke an AWS Lambda function to update the EC2 instances from the NAS server.
- B. Configure an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume for the EC2 instances to share for content access. Write code to synchronize the EBS volume with the NAS server weekly.
- C. Mount an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers to act as the NAS server. Copy the blog data to the EFS file system. Mount the EFS file system to the C2 instances to serve the content.
- D. Order an AWS Snowball Edge Storage Optimized device. Copy the static data artifacts to the device. Ship the device to AWS.
- E. Order an AWS Snowcone SSD device. Copy the static data artifacts to the device. Ship the device to AWS.

Correct Answer: CD

Community vote distribution

CD (100%)

 **AI8282** 5 months, 2 weeks ago

Selected Answer: CD

C & D. Also, 200 TB is A LOT of blog content.
upvoted 1 times

 **altonh** 10 months, 1 week ago

Selected Answer: CD

Snowcone is discontinued.
upvoted 1 times

 **ITguy_10** 1 year, 5 months ago

C & D

<https://aws.amazon.com/about-aws/whats-new/2023/05/aws-snow-family-multi-pb-data-migration-210tb-device/>
upvoted 1 times

 **AhmedSalem** 1 year, 5 months ago

Selected Answer: CD

Answer is CD
C. EFS provides a scalable, shared file storage that can be accessed by both on-premises servers and EC2 instances. This ensures that updates to the content are immediately available to the blog platform without the need for synchronization.
D. Snowball Edge is designed for large-scale data transfers, providing an efficient way to move 200 TB of data to Amazon S3 quickly and securely.
upvoted 3 times

 **kupo777** 1 year, 6 months ago

A, B
The NAS server has not been migrated.

E

AWS Snowcone does not have enough capacity.
Snowball Edge Storage Optimized can handle up to 210 TB of NVMe capacity.

The answers are C and D.

upvoted 1 times

 **awsaz** 1 year, 6 months ago

Selected Answer: CD

C And D

upvoted 4 times

 **ebbf63** 1 year, 6 months ago

Selected Answer: CD

Answer CD

upvoted 4 times

Question #504

Topic 1

A company plans to migrate a legacy on-premises application to AWS. The application is a Java web application that runs on Apache Tomcat with a PostgreSQL database.

The company does not have access to the source code but can deploy the application Java Archive (JAR) files. The application has increased traffic at the end of each month.

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

- A. Launch Amazon EC2 instances in multiple Availability Zones. Deploy Tomcat and PostgreSQL to all the instances by using Amazon Elastic File System (Amazon EFS) mount points. Use AWS Step Functions to deploy additional EC2 instances to scale for increased traffic.
- B. Provision Amazon Elastic Kubernetes Service (Amazon EKS) in an Auto Scaling group across multiple AWS Regions. Deploy Tomcat and PostgreSQL in the container images. Use a Network Load Balancer to scale for increased traffic.
- C. Refactor the Java application into Python-based containers. Use AWS Lambda functions for the application logic. Store application data in Amazon DynamoDB global tables. Use AWS Storage Gateway and Lambda concurrency to scale for increased traffic.
- D. Use AWS Elastic Beanstalk to deploy the Tomcat servers with auto scaling in multiple Availability Zones. Store application data in an Amazon RDS for PostgreSQL database. Deploy Amazon CloudFront and an Application Load Balancer to scale for increased traffic.

Correct Answer: D

Community vote distribution

D (100%)

✉  **nimbus_00** 1 year ago

Selected Answer: D

<https://stackoverflow.com/questions/70184420/can-jars-be-uploaded-successfully-to-aws-elastic-beanstalk-from-the-aws-web-ui>
upvoted 1 times

✉  **AzureDP900** 1 year, 1 month ago

D is right

Elastic Beanstalk: AWS Elastic Beanstalk is a managed service that automates the deployment, scaling, and management of web applications on EC2 instances. It provides auto-scaling capabilities, which can handle increased traffic without manual intervention.
Multi-AZ deployment: Deploying Tomcat servers in multiple Availability Zones (AZs) ensures high availability and reduces downtime in case of failures or outages.

RDS database instance: Using an RDS PostgreSQL database instance allows for easy scaling and management of your application's data, making it well-suited for increased traffic.

CloudFront and ALB: Deploying Amazon CloudFront (CDN) and Application Load Balancer (ALB) helps distribute traffic across multiple regions and instances, ensuring a scalable and high-performance architecture.

upvoted 1 times

✉  **AhmedSalem** 1 year, 5 months ago

Selected Answer: D

Answer D

Elastic Beanstalk: Provides an easy and managed way to deploy and scale web applications. It handles the deployment, capacity provisioning, load balancing, and auto-scaling automatically.

Amazon RDS for PostgreSQL: Manages the database operations, providing automated backups, patching, and scaling, which reduces operational overhead.

CloudFront and Application Load Balancer: Ensure that the application can handle increased traffic efficiently, distributing the load across multiple Availability Zones and providing low latency.

upvoted 4 times

✉  **kupo777** 1 year, 6 months ago

D

The option with the least overhead is the use of AWS Elastic Beanstalk Tomcat.

upvoted 1 times

✉  **mifune** 1 year, 6 months ago

Selected Answer: D

Upload the .jar straightforward to AWS Elastic Beanstalk. Answer D

upvoted 3 times

Question #505

Topic 1

A company is migrating its on-premises IoT platform to AWS. The platform consists of the following components:

- A MongoDB cluster as a data store for all collected and processed IoT data.
- An application that uses Message Queuing Telemetry Transport (MQTT) to connect to IoT devices every 5 minutes to collect data.
- An application that runs jobs periodically to generate reports from the IoT data. The jobs take 120-600 seconds to finish running.
- A web application that runs on a web server. End users use the web application to generate reports that are accessible to the general public.

The company needs to migrate the platform to AWS to reduce operational overhead while maintaining performance.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

- A. Create AWS Step Functions state machines with AWS Lambda tasks to prepare the reports and to write the reports to Amazon S3. Configure an Amazon CloudFront distribution that has an S3 origin to serve the reports
- B. Create an AWS Lambda function. Program the Lambda function to connect to the IoT devices, process the data, and write the data to the data store. Configure a Lambda layer to temporarily store messages for processing.
- C. Configure an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with Amazon EC2 instances to prepare the reports. Create an ingress controller on the EKS cluster to serve the reports.
- D. Connect the IoT devices to AWS IoT Core to publish messages. Create an AWS IoT rule that runs when a message is received. Configure the rule to call an AWS Lambda function. Program the Lambda function to parse, transform, and store device message data to the data store.
- E. Migrate the MongoDB cluster to Amazon DocumentDB (with MongoDB compatibility).
- F. Migrate the MongoDB cluster to Amazon EC2 instances.

Correct Answer: ADE

Community vote distribution

ADE (100%)

 **awsaz** Highly Voted 1 year, 6 months ago

Selected Answer: ADE

Step Functions and Lambda for Report Generation (A):

AWS Step Functions and Lambda can manage the periodic jobs to generate reports with minimal operational overhead. By using Amazon S3 for storage and Amazon CloudFront for distribution, the solution provides scalability and reliability with minimal management.

AWS IoT Core for MQTT Messaging (D):

AWS IoT Core is a managed service that simplifies the connection and management of IoT devices. Using IoT rules and Lambda functions ensures efficient message processing and data storage with minimal overhead.

Amazon DocumentDB for MongoDB Compatibility (E):

Amazon DocumentDB is a managed database service compatible with MongoDB, which reduces the operational burden of managing a MongoDB cluster while maintaining performance and scalability.

upvoted 7 times

 **vip2** Most Recent 1 year, 5 months ago

Selected Answer: ADE

A, D and E meet all requirements clearly

upvoted 1 times

 **mifune** 1 year, 6 months ago

Selected Answer: ADE

A - for preparing the reports and writing them to Amazon S3 | D - for handling connections from IoT devices | E - supporting MongoDB workloads.

upvoted 2 times

Question #506

A company creates an Amazon API Gateway API and shares the API with an external development team. The API uses AWS Lambda functions and is deployed to a stage that is named Production.

The external development team is the sole consumer of the API. The API experiences sudden increases of usage at specific times, leading to concerns about increased costs. The company needs to limit cost and usage without reworking the Lambda functions.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure the API to send requests to Amazon Simple Queue Service (Amazon SQS) queues instead of directly to the Lambda functions. Update the Lambda functions to consume messages from the queues and to process the requests. Set up the queues to invoke the Lambda functions when new messages arrive.
- B. Configure provisioned concurrency for each Lambda function. Use AWS Application Auto Scaling to register the Lambda functions as targets. Set up scaling schedules to increase and decrease capacity to match changes in API usage.
- C. Create an API Gateway API key and an AWS WAF Regional web ACL. Associate the web ACL with the Production stage. Add a rate-based rule to the web ACL. In the rule, specify the rate limit and a custom request aggregation that uses the X-API-Key header. Share the API key with the external development team.
- D. Create an API Gateway API Key and usage plan. Define throttling limits and quotas in the usage plan. Associate the usage plan with the Production stage and the API key. Share the API key with the external development team.

Correct Answer: D

Community vote distribution

D (100%)

 **Chakanetsa**  1 year, 5 months ago

Selected Answer: D

The most cost-effective solution to limit cost and usage for the API Gateway API with minimal code changes is:

D. Create an API Gateway API Key and usage plan. Define throttling limits and quotas in the usage plan. Associate the usage plan with the Production stage and the API key. Share the API key with the external development team.

Here's why this approach is most cost-effective:

API Key and Usage Plan: This restricts access to the API only for the development team using the provided API key. The usage plan allows defining throttling limits (maximum requests per unit time) and quotas (total requests allowed) for the API key. This controls resource utilization and costs.

Minimal Code Changes: No modifications are required to the existing Lambda functions, reducing development effort.
upvoted 5 times

 **nimbus_00**  1 year ago

Selected Answer: D

effective way to control API consumption = API KEY + Usage Plan

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

 **gfhbox0083** 1 year, 5 months ago

Selected Answer: D

D, for sure.

API Gateway Usage Plans allow you to set throttling limits and quotas on API keys. This directly controls the number of requests per second and per day that the external development team can make. It helps in managing costs by limiting the amount of Lambda invocations triggered by API requests.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: D

User plan is to define who and how much for API usage
upvoted 1 times

 **awsaz** 1 year, 6 months ago

Selected Answer: D

Creating an API key and a usage plan allows you to control and limit the usage of the API. The usage plan lets you define throttling limits (requests per second) and quotas (total requests per day or month).

By associating the usage plan with the Production stage and the API key, you can enforce these limits on the external development team, ensuring that the API usage stays within the desired boundaries.

This approach directly addresses the concern of sudden increases in usage and helps control costs without requiring any changes to the existing Lambda functions or the overall architecture

upvoted 4 times

 **mifune** 1 year, 6 months ago

Selected Answer: D

The "usage plan" is the key here for me to access the API within the defined limits.

upvoted 1 times

Question #507

Topic 1

An entertainment company hosts a ticketing service on a fleet of Linux Amazon EC2 instances that are in an Auto Scaling group. The ticketing service uses a pricing file. The pricing file is stored in an Amazon S3 bucket that has S3 Standard storage. A central pricing solution that is hosted by a third party updates the pricing file.

The pricing file is updated every 1-15 minutes and has several thousand line items. The pricing file is downloaded to each EC2 instance when the instance launches.

The EC2 instances occasionally use outdated pricing information that can result in incorrect charges for customers.

Which solution will resolve this problem MOST cost-effectively?

- A. Create an AWS Lambda function to update an Amazon DynamoDB table with new prices each time the pricing file is updated. Update the ticketing service to use DynamoDB to look up pricing
- B. Create an AWS Lambda function to update an Amazon Elastic File System (Amazon EFS) file share with the pricing file each time the file is updated. Update the ticketing service to use Amazon EFS to access the pricing file.
- C. Load Mountpoint for Amazon S3 onto the AMI of the EC2 instances. Configure Mountpoint for Amazon S3 to mount the S3 bucket that contains the pricing file. Update the ticketing service to point to the mount point and path to access the \$3 object,
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume. Use EBS Multi-Attach to attach the volume to every EC2 instance. When a new EC2 instance launches, configure the new instance to update the pricing file on the EBS volume. Update the ticketing service to point to the new local source.

Correct Answer: C

Community vote distribution

C (62%)

A (38%)

 **awsaz** Highly Voted 1 year, 6 months ago

Selected Answer: C

Mountpoint for Amazon S3: This solution allows the EC2 instances to directly access the S3 bucket as if it were a local file system. This ensures that the instances always access the latest version of the pricing file without having to download it each time.

Cost-Effective: This approach avoids the need to constantly download and store the file on each instance, which can save on both S3 GET requests and local storage costs.

Simplicity: By mounting the S3 bucket, you ensure that all instances are using the most current file without additional logic or processes to manage file updates.

upvoted 9 times

 **mifune** Highly Voted 1 year, 6 months ago

Selected Answer: A

DynamoDB in this scenario looks cheaper than EFS. Answer A

upvoted 5 times

 **aka1177** Most Recent 3 weeks, 3 days ago

Selected Answer: A

Only A; S3 service is not a file share system by design. In reality it won't work as good as other solutions. You all were misled.

upvoted 1 times

 **eesa** 8 months, 3 weeks ago

Selected Answer: C

Option C (Mountpoint for S3) (best solution):

Mountpoint for Amazon S3 allows the EC2 instances to directly access the latest version of the pricing file stored in S3 without repeatedly downloading it. Each EC2 instance will always read the most up-to-date file directly from S3, eliminating the risk of outdated information. This solution is cost-effective as it involves minimal overhead, does not incur unnecessary data transfer or operational complexity, and requires minimal application modification.

upvoted 2 times

 **nimbus_00** 1 year ago

Selected Answer: C

"Mountpoint for Amazon S3 is available only for Linux operating systems. You can use Mountpoint to access S3 objects in all storage classes except S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Intelligent-Tiering Archive Access Tier, and S3 Intelligent-Tiering Deep Archive Access Tier."

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

upvoted 3 times

✉ **0b43291** 1 year, 1 month ago

Selected Answer: C

By leveraging the strong consistency guarantees, cost-effectiveness, and simplicity of Mountpoint for Amazon S3, Option C provides the most appropriate and cost-effective solution for ensuring the EC2 instances in the Auto Scaling group always have access to the latest pricing information, resolving the outdated pricing data problem.

The other options have drawbacks or are less cost-effective:

Option A: Using DynamoDB may not be cost-effective for storing and accessing a large, frequently updated pricing file with several thousand line items.

Option B: While Amazon EFS is viable, it introduces additional infrastructure and potential costs compared to directly accessing the pricing file from the S3 bucket using Mountpoint for Amazon S3.

Option D: Using an Amazon EBS volume with Multi-Attach would require updating the pricing file on the volume whenever a new instance launches, which is less efficient and more prone to errors than directly accessing the file from the S3 bucket.

upvoted 2 times

✉ **Danm86** 1 year, 2 months ago

Option C is most cost effective, but the question has ambiguity where it tells customer could be wrongly charged, more details should be provided on the same to understand if wrong charging is critical or not. If wrong charging is critical and needs low latency and more reliability on the queried data then its option A

upvoted 1 times

✉ **pk0619** 1 year, 2 months ago

Selected Answer: C

most cost effective

upvoted 1 times

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

none of them makes sense... if an S3 object is uploaded it is strongly consist since end 2020, eventual consistency is a matter of the past. So it doesn't matter if the lambda function get the trigger after upload and transfer the information to dynamodb (A) or EFS(b), or the ec2 instance get the object via blocklevel file access (C) or EBS (D). The consistency is being provided by the source system which is S3, so nothing helps here. From the cost perspective is C the cheapest

upvoted 1 times

✉ **alexbraila** 1 year ago

The way I understand it, the question is not about S3 consistency. The problem is that an EC2 instance downloads the file from S3 upon launch and never updates it during its lifetime. Hence A, B and C would all solve this problem (but not D, as the file in EBS would only be updated when a new instance is launched), but the most cost-effective is C

upvoted 1 times

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

Selected Answer: C

Mountpoint for Amazon S3 allows EC2 instances to treat an S3 bucket like a file system. This solution ensures that the EC2 instances always have access to the latest version of the pricing file, as the file is directly accessed from S3. You avoid downloading the file every time and reduce the risk of using outdated pricing data.

S3 Consistency: Amazon S3 provides strong read-after-write consistency, so any update to the pricing file in S3 will be immediately visible to all EC2 instances accessing the file via the mount point.

Cost Efficiency: By using Mountpoint for Amazon S3, you leverage S3's cost-effective storage and avoid additional infrastructure like DynamoDB or Elastic File System (EFS). This solution does not require copying data to another storage system, minimizing overhead.

upvoted 2 times

✉ **wbedair** 1 year, 3 months ago

Selected Answer: C

the question is asking about cost effectiveness so why choose A to add additional service like Dynamodb . I will go for option C

upvoted 2 times

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

Selected Answer: A

A. DynamoDB provides fast data access and query capabilities, suitable for frequently read but infrequently updated data.

B. EFS may not be suitable for frequent small file updates, and its cost may be higher than using DynamoDB.

C. This solution can directly read pricing files from S3, but it does not solve the problem of outdated pricing data being used by old instances even after the pricing files are updated.

D. EBS is not good at Multi Attach to multiple EC2 instances, and it can increase complexity and cost.

upvoted 3 times

✉ **alexbraila** 1 year ago

I would argue that option C does solve the problem of outdated pricing data. If the ticketing service looks up the price in the local file upon every request and since the local file links to the up to date file in S3, it looks right to me

upvoted 1 times

✉ **DS2023** 1 year, 4 months ago

Selected Answer: A

Option A is the correct answer.

upvoted 4 times

 **mns0173** 1 year, 5 months ago

There is no need to move away from S3

upvoted 2 times

Question #508

Topic 1

A company has an application that uses Amazon EC2 instances in an Auto Scaling group. The quality assurance (QA) department needs to launch a large number of short-lived environments to test the application. The application environments are currently launched by the manager of the department using an AWS CloudFormation template. To launch the stack, the manager uses a role with permission to use CloudFormation, EC2, and Auto Scaling APIs. The manager wants to allow testers to launch their own environments, but does not want to grant broad permissions to each user.

Which set up would achieve these goals?

- A. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to assume the manager's role and add a policy that restricts the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console.
- B. Create an AWS Service Catalog product from the environment template. Add a launch constraint to the product with the existing role. Give users in the QA department permission to use AWS Service Catalog APIs only. Train users to launch the template from the AWS Service Catalog console.
- C. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to use CloudFormation and S3 APIs, with conditions that restrict the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console.
- D. Create an AWS Elastic Beanstalk application from the environment template. Give users in the QA department permission to use Elastic Beanstalk permissions only. Train users to launch Elastic Beanstalk environments with the Elastic Beanstalk CLI, passing the existing role to the environment as a service role.

Correct Answer: B

Community vote distribution

B (100%)

 **awsaz**  1 year, 6 months ago

Selected Answer: B

B is the answer
upvoted 6 times

 **0b43291**  1 year, 1 month ago

Selected Answer: B

By using AWS Service Catalog, you can leverage its built-in features for self-service, launch constraints, and restricted permissions, making it the most appropriate solution for allowing testers to launch their own environments while limiting their access to only the necessary resources and actions.

The other options have drawbacks or do not fully address the requirements:

Option A: Granting users permission to assume the manager's role and restricting permissions through policies can be complex to manage and may still grant broader permissions than desired.

Option C: Granting users direct permission to use CloudFormation and S3 APIs, even with conditions, may still provide more access than necessary and increase the risk of unintended actions.

Option D: While Elastic Beanstalk can be used to launch environments, it may not provide the same level of control and customization as a CloudFormation template. Additionally, granting Elastic Beanstalk permissions may still provide more access than necessary.

upvoted 1 times

 **mifune** 1 year, 6 months ago

Selected Answer: B

Service Catalog, answer B
upvoted 1 times

Question #509

A company is using a single AWS Region for its ecommerce website. The website includes a web application that runs on several Amazon EC2 instances behind an Application Load Balancer (ALB). The website also includes an Amazon DynamoDB table. A custom domain name in Amazon Route 53 is linked to the ALB. The company created an SSL/TLS certificate in AWS Certificate Manager (ACM) and attached the certificate to the ALB. The company is not using a content delivery network as part of its design.

The company wants to replicate its entire application stack in a second Region to provide disaster recovery, plan for future growth, and provide improved access time to users. A solutions architect needs to implement a solution that achieves these goals and minimizes administrative overhead.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Create an AWS CloudFormation template for the current infrastructure design. Use parameters for important system values, including Region. Use the CloudFormation template to create the new infrastructure in the second Region.
- B. Use the AWS Management Console to document the existing infrastructure design in the first Region and to create the new infrastructure in the second Region.
- C. Update the Route 53 hosted zone record for the application to use weighted routing. Send 50% of the traffic to the ALB in each Region.
- D. Update the Route 53 hosted zone record for the application to use latency-based routing. Send traffic to the ALB in each Region.
- E. Update the configuration of the existing DynamoDB table by enabling DynamoDB Streams. Add the second Region to create a global table.
- F. Create a new DynamoDB table. Enable DynamoDB Streams for the new table. Add the second Region to create a global table. Copy the data from the existing DynamoDB table to the new table as a one-time operation.

Correct Answer: ADE

Community vote distribution

ADE (89%) 11%

 **horiuchi** 6 months ago

Selected Answer: ABD

It doesn't say Global Table. It says Global Streams. And it asks us to "replicate the entire stack", not modify the existing stack. So...
upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: ADE

By combining CloudFormation for infrastructure deployment, latency-based routing in Route 53, and creating a global DynamoDB table, the solutions architect can achieve the goals of disaster recovery, future growth, and improved access time while minimizing administrative overhead and ensuring data consistency across both Regions.

The other options are either not necessary or do not fully meet the requirements:

- B. Using the AWS Management Console to document and create the infrastructure manually would be time-consuming and prone to human error, increasing administrative overhead.
- C. Using weighted routing in Route 53 would distribute traffic based on predefined weights, which may not provide the best user experience or account for future growth or changes in traffic patterns.
- F. Creating a new DynamoDB table and copying data as a one-time operation would not provide continuous replication and could lead to data inconsistencies or data loss in case of a Regional outage.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

ADE is best option for given scenario.

upvoted 1 times

 **NoInNothing** 1 year, 5 months ago

Selected Answer: ADE

A, D , E is correct

upvoted 2 times

 **awsaz** 1 year, 6 months ago

Selected Answer: ADE

A and D And E

upvoted 3 times

 **mifune** 1 year, 6 months ago

Selected Answer: ADE

A-D-E makes more sense to me here
upvoted 1 times

Question #510

Topic 1

A company wants to create a single Amazon S3 bucket for its data scientists to store work-related documents. The company uses AWS IAM Identity Center to authenticate all users. A group for the data scientists was created.

The company wants to give the data scientists access to only their own work. The company also wants to create monthly reports that show which documents each user accessed.

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

- A. Create a custom IAM Identity Center permission set to grant the data scientists access to an S3 bucket prefix that matches their username tag. Use a policy to limit access to paths with the \${aws:PrincipalTag/userName}/* condition.
- B. Create an IAM Identity Center role for the data scientists group that has Amazon S3 read access and write access. Add an S3 bucket policy that allows access to the IAM Identity Center role.
- C. Configure AWS CloudTrail to log S3 data events and deliver the logs to an S3 bucket. Use Amazon Athena to run queries on the CloudTrail logs in Amazon S3 and generate reports.
- D. Configure AWS CloudTrail to log S3 management events to CloudWatch. Use Amazon Athena's CloudWatch connector to query the logs and generate reports.
- E. Enable S3 access logging to EMR File System (EMRFS). Use Amazon S3 Select to query logs and generate reports.

Correct Answer: AC*Community vote distribution*

AC (100%)

 **Soliner_Bilgi_Teknolojileri** 3 months, 3 weeks ago

Selected Answer: AC

A: Grants each user access only to their own S3 folder using \${aws:PrincipalTag/userName}/*, ensuring data isolation.

C: CloudTrail S3 data events track which objects each user accessed, and Athena can query these logs to generate monthly usage reports.
upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: AC

By combining a custom IAM Identity Center permission set with path-based access control and CloudTrail logging with Athena querying, the company can achieve the desired access control and reporting requirements for the data scientists' work-related documents stored in the S3 bucket.

The other options are either incorrect or do not fully meet the requirements:

- B. Creating an IAM Identity Center role with S3 read and write access and adding an S3 bucket policy would not provide the granular access control required to restrict each user to their own work.
- D. Configuring CloudTrail to log S3 management events to CloudWatch and using Athena's CloudWatch connector would not capture the necessary data events for generating reports on which documents each user accessed.
- E. Enabling S3 access logging to EMRFS and using S3 Select would not provide the necessary logging and reporting capabilities for this use case.

upvoted 2 times

 **awsaz** 1 year, 6 months ago

Selected Answer: AC

A and C

upvoted 4 times

 **mifune** 1 year, 6 months ago

Selected Answer: AC

IAM Identity Center permission + Amazon Athena to run queries on the CloudTrail logs in Amazon S3 and generate reports, answer A-C
upvoted 1 times

Question #511

Topic 1

A company hosts a data-processing application on Amazon EC2 instances. The application polls an Amazon Elastic File System (Amazon EFS) file system for newly uploaded files. When a new file is detected, the application extracts data from the file and runs logic to select a Docker container image to process the file. The application starts the appropriate container image and passes the file location as a parameter.

The data processing that the container performs can take up to 2 hours. When the processing is complete, the code that runs inside the container writes the file back to Amazon EFS and exits.

The company needs to refactor the application to eliminate the EC2 instances that are running the containers.

Which solution will meet these requirements?

- A. Create an Amazon Elastic Container Service (Amazon ECS) cluster. Configure the processing to run as AWS Fargate tasks. Extract the container selection logic to run as an Amazon EventBridge rule that starts the appropriate Fargate task. Configure the EventBridge rule to run when files are added to the EFS file system.
- B. Create an Amazon Elastic Container Service (Amazon ECS) cluster. Configure the processing to run as AWS Fargate tasks. Update and containerize the container selection logic to run as a Fargate service that starts the appropriate Fargate task. Configure an EFS event notification to invoke the Fargate service when files are added to the EFS file system.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster. Configure the processing to run as AWS Fargate tasks. Extract the container selection logic to run as an AWS Lambda function that starts the appropriate Fargate task. Migrate the storage of file uploads to an Amazon S3 bucket. Update the processing code to use Amazon S3. Configure an S3 event notification to invoke the Lambda function when objects are created.
- D. Create AWS Lambda container images for the processing. Configure Lambda functions to use the container images. Extract the container selection logic to run as a decision Lambda function that invokes the appropriate Lambda processing function. Migrate the storage of file uploads to an Amazon S3 bucket. Update the processing code to use Amazon S3. Configure an S3 event notification to invoke the decision Lambda function when objects are created.

Correct Answer: C

Community vote distribution

C (100%)

 **AI8282** 5 months, 2 weeks ago

Selected Answer: C

There is no event trigger for EFS like there is for S3 for A.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: C

By combining Amazon ECS with Fargate tasks, AWS Lambda for the container selection logic, and Amazon S3 for event-driven processing, Option C provides a serverless and scalable solution that meets the requirements while minimizing the need for EC2 instances and leveraging the strengths of each AWS service.

While this solution requires migrating the file storage from Amazon EFS to Amazon S3, it addresses the requirement of eliminating EC2 instances by leveraging AWS Fargate for the processing tasks and AWS Lambda for the container selection logic. Additionally, it utilizes the event notification capabilities of Amazon S3 to trigger the Lambda function when new files are uploaded.

The other options are either not feasible due to the limitations of Amazon EFS (Options A and B) or introduce additional constraints by using AWS Lambda for the long-running data processing tasks (Option D).

upvoted 3 times

 **mkgiz** 1 year, 3 months ago

Selected Answer: C

EFS event notification to invoke the Fargate

upvoted 1 times

 **mark_232323** 1 year, 5 months ago

Selected Answer: C

EFS event notification to invoke the Fargate --> EFS don't have event notification like s3

upvoted 3 times

 **vip2** 1 year, 5 months ago

Selected Answer: C

C

EventBridge can not monitor EFS event directly, not A

upvoted 3 times

 **kupo777** 1 year, 6 months ago

C

EFS cannot notify events and Lambda cannot do container execution for 2 hours.

upvoted 3 times

Question #512

Topic 1

A media company has a 30-T8 repository of digital news videos. These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management (MAM) system. The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature. The company must be able to search based on information in the video, such as objects, scenery items, or people's faces. A catalog is available that contains faces of people who have appeared in the videos that include an image of each person. The company would like to migrate these videos to AWS.

The company has a high-speed AWS Direct Connect connection with AWS and would like to move the MAM solution video content directly from its current file system.

How can these requirements be met by using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system?

- A. Set up an AWS Storage Gateway, file gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the file gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata, and push the metadata into the MAM solution.
- B. Set up an AWS Storage Gateway, tape gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the tape gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Amazon Rekognition process the video in the tape gateway, retrieve the required metadata, and push the metadata into the MAM solution.
- C. Configure a video ingestion stream by using Amazon Kinesis Video Streams. Use the catalog of faces to build a collection in Amazon Rekognition. Stream the videos from the MAM solution into Kinesis Video Streams. Configure Amazon Rekognition to process the streamed videos. Then, use a stream consumer to retrieve the required metadata, and push the metadata into the MAM solution. Configure the stream to store the videos in Amazon S3.
- D. Set up an Amazon EC2 instance that runs the OpenCV libraries. Copy the videos, images, and face catalog from the on-premises library into an Amazon EBS volume mounted on this EC2 instance. Process the videos to retrieve the required metadata, and push the metadata into the MAM solution, while also copying the video files to an Amazon S3 bucket.

Correct Answer: A

Community vote distribution

A (63%)

B (37%)

 **mifune** Highly Voted 1 year, 6 months ago

Selected Answer: B

B - Tape Gateway
upvoted 5 times

 **Hizumi** Highly Voted 1 year, 5 months ago

Selected Answer: B

Answer is B - Use Tape Gateway, then Lambda and Rekognition can be used to process and index the data for the MAM system.

<https://aws.amazon.com/storagegateway/vtl/>
<https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/>
 upvoted 5 times

 **bdloko** Most Recent 9 months, 1 week ago

Selected Answer: A

How do people come-up with such scenarios?
upvoted 2 times

 **albert_kuo** 9 months, 2 weeks ago

Selected Answer: A

Because of the company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature, so exclude B
upvoted 1 times

 **SIJUTHOMASP** 1 year ago

Selected Answer: A

Since the need is "move the MAM solution video content directly from its current file system.", they want the files from tape to another storage which can be S3. Hence the solution would be A.

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Selected Answer: A

Option A leverages fully managed AWS services (AWS Storage Gateway, Amazon Rekognition, AWS Lambda, and Amazon S3) while minimizing disruption to the existing MAM solution and its workflow for extracting videos from the tape library. This approach strikes a balance between leveraging AWS services for metadata enrichment, face recognition, and durable video storage while causing minimal disruption to the existing system and minimizing ongoing management overhead.

extract videos from onprem tapes - push through file gateway to S3

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

A

Using an on-premises file gateway appliance with AWS Storage Gateway has several advantages over using a tape gateway:

Less administrative burden: Managing the file gateway appliance is still handled by AWS, reducing your administrative tasks.

Easier to scale: With a file gateway, you can scale more easily to handle increasing amounts of video content.

More flexible storage options: You can store videos in Amazon S3, which provides more flexibility and scalability compared to tape storage.

upvoted 1 times

 **AloraCloud** 1 year, 1 month ago

You can use Tape Gateway to archive data you need to preserve at another offsite location for disaster recovery or regulatory compliance needs. Tape Gateway enables you to replace magnetic tape libraries and physical tapes with AWS Cloud storage for long-term storage retention needs.

upvoted 1 times

 **Danm86** 1 year, 2 months ago

I believe A should be the write answer of using file gateway, since there is processing of data required before storing. and Tape Gateway cannot be directly used, it involves complexity

upvoted 2 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: A

AWS Rekognition is capable of processing both images and videos from the following sources: Amazon S3, directly passed images, Kinesis Video Streams. Although option C mentions Kinesis Video Streams, it would be an overkill for a scenario where videos are not being streamed in real time, and it introduces unnecessary complexity. So the solution using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system is A.

upvoted 2 times

 **mkgiz** 1 year, 3 months ago

Selected Answer: A

Use the MAM solution to extract the videos from the current archive

upvoted 2 times

 **felon124** 1 year, 4 months ago

Selected Answer: A

It is not possible to directly invoke Amazon Rekognition to process videos that are stored on an AWS Storage Gateway (whether it's a file gateway or tape gateway). Amazon Rekognition processes videos that are stored in Amazon S3.

upvoted 3 times

 **asquared16** 1 year, 4 months ago

Selected Answer: A

Yes the videos were stored on tape on premise, but the solution requires active processing later on, this can't be done on Tape GW; won't make sense.

upvoted 2 times

 **asquared16** 1 year, 4 months ago

Okay, it's B. You cannot directly migrate videos from a tape library to an AWS Storage Gateway file gateway appliance.

upvoted 2 times

 **c22ddd8** 1 year, 4 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/>

upvoted 1 times

 **toma** 1 year, 5 months ago

Answer is B: "These videos are stored on tape in an on-premises tape library...."

upvoted 2 times

 **Russss99** 1 year, 5 months ago

Selected Answer: A

ape Gateway is designed for offline data transfer, not ideal for actively accessed videos.

upvoted 2 times

✉ **kupo777** 1 year, 6 months ago

A

A tape gateway appliance is required.

AWS Storage Gateway also requires S3 or other storage.

upvoted 2 times

✉ **wbedair** 1 year, 6 months ago

so you mean B ???

upvoted 1 times

✉ **kupo777** 1 year, 5 months ago

A - Amazon Rekognition and Tape Gateway cannot communicate directly; S3 is required.

upvoted 2 times

✉ **Hizumi** 1 year, 5 months ago

Storage Gateway stores the tape library in S3.

upvoted 2 times

Question #513

Topic 1

A company needs to optimize the cost of an AWS environment that contains multiple accounts in an organization in AWS Organizations. The company conducted cost optimization activities 3 years ago and purchased Amazon EC2 Standard Reserved Instances that recently expired.

The company needs EC2 instances for 3 more years. Additionally, the company has deployed a new serverless workload.

Which strategy will provide the company with the MOST cost savings?

- A. Purchase the same Reserved Instances for an additional 3-year term with All Upfront payment. Purchase a 3-year Compute Savings Plan with All Upfront payment in the management account to cover any additional compute costs
- B. Purchase a 1-year Compute Savings Plan with No Upfront payment in each member account. Use the Savings Plans recommendations in the AWS Cost Management console to choose the Compute Savings Plan.
- C. Purchase a 3-year EC2 Instance Savings Plan with No Upfront payment in the management account to cover EC2 costs in each AWS Region. Purchase a 3-year Compute Savings Plan with No Upfront payment in the management account to cover any additional compute costs.
- D. Purchase a 3-year EC2 Instance Savings Plan with All Upfront payment in each member account. Use the Savings Plans recommendations in the AWS Cost Management console to choose the EC2 Instance Savings Plan.

Correct Answer: A

Community vote distribution

A (100%)

053081f Highly Voted 1 year, 5 months ago

Selected Answer: A

Since there are no special requirements in the problem statement other than cost (e.g., workload consistency, specific instance size, future changes), simply select the least expensive plan.

Compared to on-demand instances, Reserved Instances (RI) offer discounts of up to 75%, Compute Savings Plans up to 66%, and EC2 Instance Savings Plans up to 72%. In each case, the higher the upfront payment, the greater the discount.

upvoted 9 times

Daniel76 Most Recent 1 year, 3 months ago

Selected Answer: A

The mention of serverless workload is just distraction. It can be for a new system and meanwhile it may not be commercially or operationally viable to move the current ec2 workload to serverless, so it's normal to continue to run it with cost effectiveness for the next 3 years.

upvoted 1 times

TiredDad 1 year, 3 months ago

Option C seems better. Because with Option A, provides comprehensive coverage but involves upfront payment and potentially redundant cost coverage if Compute Savings Plans are also being purchased. The combination might be less cost-efficient due to the overlap in coverage.

upvoted 1 times

mark_232323 1 year, 5 months ago

Selected Answer: A

It's clear, RI for EC2 and compute saving for serverless

upvoted 3 times

G4Exams 1 year, 5 months ago

A because it is said that 3 years ago they optimized costs and came to that conclusion... so just renew reserved instances and for compute use compute plan because that is the best add for serverless...

upvoted 3 times

kupo777 1 year, 6 months ago

A

Need a Compute Savings Plan for serverless workloads

The least expensive way to run EC2 instances for 3 years would be either a Reserved Instance or EC2 Instance Savings Plan.

upvoted 4 times

alex_heavy 1 year, 5 months ago

+1 for 3Y All Upfront RI, which will give best discount ever

upvoted 1 times

Question #514

Topic 1

A company operates a static content distribution platform that serves customers globally. The customers consume content from their own AWS accounts.

The company serves its content from an Amazon S3 bucket. The company uploads the content from its on-premises environment to the S3 bucket by using an S3 File Gateway.

The company wants to improve the platform's performance and reliability by serving content from the AWS Region that is geographically closest to customers. The company must route the on-premises data to Amazon S3 with minimal latency and without public internet exposure.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Implement S3 Multi-Region Access Points
- B. Use S3 Cross-Region Replication (CRR) to copy content to different Regions
- C. Create an AWS Lambda function that tracks the routing of clients to Regions
- D. Use an AWS Site-to-Site VPN connection to connect to a Multi-Region Access Point.
- E. Use AWS PrivateLink and AWS Direct Connect to connect to a Multi-Region Access Point.

Correct Answer: AE

Community vote distribution

AE (65%) AB (18%) BE (18%)

 **awsaz** Highly Voted 1 year, 6 months ago

Selected Answer: AE

A and E

upvoted 5 times

 **kupo777** 1 year, 5 months ago

A,E is correct.

On-premise data needed to be routed to Amazon S3 with minimal latency and without exposing it to the public Internet.

upvoted 1 times

 **nimbus_00** Most Recent 1 year ago

Selected Answer: BE

B and E. S3 Multi-Region Access Points Most Voted is mentioned in E anyway.

upvoted 1 times

 **dv1** 1 year ago

Selected Answer: BE

A+B+E is better for me tbh, but since we have to select 2 I go with B+E

upvoted 1 times

 **0b43291** 1 year, 1 month ago

Difficult one. Need E to protect traffic from onprem to AWS. Need A to access. However you would also need B to Sync the buckets across regions.

upvoted 1 times

 **chris_spencer** 1 year, 2 months ago

Selected Answer: AB

A. Implement S3 Multi-Region Access Points and B. Use S3 Cross-Region Replication (CRR) to copy content to different Regions.

The combination of (A) and (B) allows the company to serve content from the closest region to the end-user and ensures that the data is replicated across multiple regions to support this.

Multi-Region Access Points simplify the access and management of the data while CRR ensures that the content is available across these regions.

This setup provides a straightforward and managed solution to meet the requirement of geographical content routing with minimal operational overhead.

For all that voting for E... how does AWS DirectConnect and "LEAST operational overhead" fit together.

upvoted 3 times

 **dv1** 1 year ago

While I agree with you that B is required, answer E covers the "minimal latency and without public internet exposure" part of the requirement.

upvoted 3 times

 **vmia159** 10 months ago

Is AB to me.

There are 2 objectives.

- The company wants to improve the platform's performance and reliability by serving content from the AWS Region that is geographically closest to customers. -> multi region access point and cross-region replication required
- The company must route the on-premises data to Amazon S3 with minimal latency and without public internet exposure -> S3 File Gateway(already mentioned)

Upload -> S3 File Gateway (already setup)

Download -> S3 multi region access point and cross region replication

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: AE

A: S3 Multi-Region Access Points allow customers to access Amazon S3 data from multiple AWS Regions with the lowest latency. These access points automatically route requests to the closest region based on the user's location. This helps optimize performance and increases reliability by dynamically routing traffic to the most optimal region.

E: AWS PrivateLink ensures private connectivity between AWS services and on-premises resources without traversing the public internet.

B: Although CRR replicates data across Regions, it does NOT optimize performance by routing users to the closest Region dynamically.

C: While Lambda can handle some routing logic, this option adds more operational overhead compared to using built-in features like S3 Multi-Region Access Points.

D: It can't be because one of the requirements is "without public internet exposure."

upvoted 2 times

 **Daniel76** 1 year, 3 months ago

Selected Answer: AE

The company wants to improve the platform's performance and reliability by serving content from the AWS Region that is geographically closest to customers: s3 multi region access point. (A)

The company must route the on-premises data to Amazon S3 with minimal latency and without public internet exposure: PrivateLink and Direct Connect to the MRAP. (E)

upvoted 2 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: BE

Option A: Multi regional access points are mainly used to access S3 data across multiple regions, rather than solving data transmission problems.

Option B: Allows companies to automatically asynchronously replicate data from S3 buckets to S3 buckets in other AWS regions.

Option E: AWS PrivateLink provides a secure and private way to access AWS services without using the public Internet.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: AE

A and E is correct to meet latency and private network

upvoted 2 times

 **gfhbox0083** 1 year, 5 months ago

A, E, for sure

upvoted 2 times

 **kupo777** 1 year, 6 months ago

A and B

Multi-region access configuration allows content to be served from each region closest to the customer's AWS access using a cross-region replica of the AWS global network.

upvoted 3 times

Question #515

A company is migrating its data center to the AWS Cloud and needs to complete the migration as quickly as possible. The company has many applications that are running on hundreds of VMware VMs in the data center. Each VM is configured with a shared Windows folder that contains common shared files. The file share is larger than 100 GB in size.

The company's compliance team requires a change request to be filed and approved for every software installation and modification to each VM. The company has an AWS Direct Connect connection with 10 GB of bandwidth between AWS and the data center.

Which set of steps should the company take to complete the migration in the LEAST amount of time?

- A. Use VM ImportExport to create images of each VM. Use AWS Application Migration Service to manage and view the images. Copy the Windows file share data to an Amazon Elastic File System (Amazon EFS) file system. After migration, remap the file share to the EFS file system.
- B. Deploy the AWS Application Discovery Service agentless appliance to VMware vCenter. Review the portfolio of discovered VMs in AWS Migration Hub.
- C. Deploy the AWS Application Migration Service agentless appliance to VMware vCenter. Copy the Windows file share data to a new Amazon FSx for Windows File Server file system. After migration, remap the file share on each VM to the FSx for Windows File Server file system.
- C. Create and review a portfolio in AWS Migration Hub. Order an AWS Snowcone device. Deploy AWS Application Migration Service to VMware vCenter and export all the VMs to the Snowcone device. Copy all Windows file share data to the Snowcone device. Ship the Snowcone device to AWS. Use Application Migration Service to deploy all the migrated instances.
- D. Deploy the AWS Application Discovery Service Agent and the AWS Application Migration Service Agent onto each VMware hypervisor directly. Review the portfolio in AWS Migration Hub. Copy each VM's file share data to a new Amazon FSx for Windows File Server file system. After migration, remap the file share on each VM to the FSx for Windows File Server file system.

Correct Answer: C*Community vote distribution*

C (100%)

 **vip2** Highly Voted 1 year, 5 months ago

Selected Answer: C

C1 (not C2) is correct because Application Migration Agentless on vMCenter.

upvoted 7 times

 **JoeTromundo** Most Recent 1 year, 2 months ago

Selected Answer: C

C1 is correct. The AWS Application Migration Service (AMS) agentless appliance can quickly be deployed into the VMware environment via VMware vCenter. It simplifies migration by eliminating the need for installing agents on each individual VM, reducing time and complexity. Because AMS is agentless, you don't need to install additional software on the VMs themselves, which aligns with the company's requirement to file and approve change requests for any software installation or modifications on VMs. By copying the shared Windows folder to Amazon FSx for Windows File Server, the company can maintain a native Windows environment for file sharing. After migration, it will be easy to remap the file share from the VMs to the new FSx file system, which minimizes disruptions and downtime.

upvoted 3 times

 **053081f** 1 year, 5 months ago

A combination of A and B is one option.

In AWS, if there are five choices, the answer is usually two.

In the case of multiple choice, there is only one answer from ABCD.

I have never seen a pattern where there is only one answer from ABCDE.

upvoted 1 times

 **Alagong** 1 year, 5 months ago

Selected Answer: C

IT should be C

upvoted 2 times

 **kupo777** 1 year, 6 months ago

B

Migration can be completed in the shortest possible time using an agentless appliance

upvoted 1 times

 **wbedair** 1 year, 6 months ago

B focuses on discovery and does not address the migration process, correct answer is C
upvoted 4 times

 **awsaz** 1 year, 6 months ago

Selected Answer: C

ç1 is the answer

upvoted 4 times

Question #516

Topic 1

A company has multiple AWS accounts that are in an organization in AWS Organizations. The company needs to store AWS account activity and query the data from a central location by using SQL.

Which solution will meet these requirements?

- A. Create an AWS CloudTrail trail in each account. Specify CloudTrail management events for the trail. Configure CloudTrail to send the events to Amazon CloudWatch Logs. Configure CloudWatch cross-account observability. Query the data in CloudWatch Logs Insights.
- B. Use a delegated administrator account to create an AWS CloudTrail Lake data store. Specify CloudTrail management events for the data store. Enable the data store for all accounts in the organization. Query the data in CloudTrail Lake.
- C. Use a delegated administrator account to create an AWS CloudTrail trail. Specify CloudTrail management events for the trail. Enable the trail for all accounts in the organization. Keep all other settings as default. Query the CloudTrail data from the CloudTrail event history page.
- D. Use AWS CloudFormation StackSets to deploy AWS CloudTrail Lake data stores in each account. Specify CloudTrail management events for the data stores. Keep all other settings as default, Query the data in CloudTrail Lake.

Correct Answer: B

Community vote distribution

B (100%)

 **0b43291** 1 year, 1 month ago

By leveraging AWS CloudTrail Lake and a delegated administrator account in AWS Organizations, Option B provides a centralized and managed solution for ingesting, storing, and querying AWS account activity using SQL, meeting the company's requirements efficiently.

The other options have drawbacks or do not fully meet the requirements:

Option A: While it uses CloudWatch Logs and CloudWatch Logs Insights, it requires creating and managing CloudTrail trails in each account, which can be more complex and less centralized than using CloudTrail Lake.

Option C: This option suggests using the CloudTrail event history page for querying, which does not provide the SQL querying capabilities required by the company. Additionally, it may not offer the same level of centralization and advanced analytics as CloudTrail Lake.

Option D: While it uses CloudTrail Lake, deploying data stores in each account using CloudFormation StackSets can be more complex and less centralized than using a delegated administrator account to manage the data store for all accounts.

upvoted 2 times

 **Daniel76** 1 year, 3 months ago

Selected Answer: B

To enable CloudTrail Lake, you need to log in with admin access to CloudTrail.

<https://aws.amazon.com/blogs/mt/announcing-aws-cloudtrail-lake-a-managed-audit-and-security-lake/>

upvoted 3 times

 **c22ddd8** 1 year, 5 months ago

Selected Answer: B

AWS CloudTrail Lake lets you run SQL-based queries on your events.

upvoted 2 times

 **kupo777** 1 year, 6 months ago

B

You can aggregate events within an Organization by enabling it for all accounts in the Organization with AWS CloudTrail Lake.

upvoted 3 times

Question #517

A company is using AWS to develop and manage its production web application. The application includes an Amazon API Gateway HTTP API that invokes an AWS Lambda function. The Lambda function processes and then stores data in a database.

The company wants to implement user authorization for the web application in an integrated way. The company already uses a third-party identity provider that issues OAuth tokens for the company's other applications.

Which solution will meet these requirements?

- A. Integrate the company's third-party identity provider with API Gateway. Configure an API Gateway Lambda authorizer to validate tokens from the identity provider. Require the Lambda authorizer on all API routes. Update the web application to get tokens from the identity provider and include the tokens in the Authorization header when calling the API Gateway HTTP API.
- B. Integrate the company's third-party identity provider with AWS Directory Service. Configure Directory Service as an API Gateway authorizer to validate tokens from the identity provider. Require the Directory Service authorizer on all API routes. Configure AWS IAM Identity Center as a SAML 2.0 identity Provider. Configure the web application as a custom SAML 2.0 application.
- C. Integrate the company's third-party identity provider with AWS IAM Identity Center. Configure API Gateway to use IAM Identity Center for zero-configuration authentication and authorization. Update the web application to retrieve AWS Security Token Service (AWS STS) tokens from IAM Identity Center and include the tokens in the Authorization header when calling the API Gateway HTTP API.
- D. Integrate the company's third-party identity provider with AWS IAM Identity Center. Configure IAM users with permissions to call the API Gateway HTTP API. Update the web application to extract request parameters from the IAM users and include the parameters in the Authorization header when calling the API Gateway HTTP API.

Correct Answer: A

Community vote distribution

A (100%)

 **AzureDP900** 1 year, 1 month ago

Selected Answer: A

A is right, to implement user authorization for the web application, you can integrate the company's third-party identity provider with API Gateway using an API Gateway Lambda authorizer to validate tokens from the identity provider. By requiring this authorizer on all API routes, you ensure that only authenticated and authorized users can access the application. Finally, update the web application to retrieve tokens from the identity provider and include them in the Authorization header when making requests to the API Gateway HTTP API. This ensures a seamless and integrated user experience across all applications using the same third-party identity provider.

upvoted 3 times

 **0b43291** 1 year, 1 month ago

Selected Answer: A

By integrating the third-party identity provider with API Gateway and using a Lambda authorizer to validate OAuth tokens, Option A provides a seamless and integrated solution for user authorization in the web application, while leveraging the company's existing identity management infrastructure.

The other options have drawbacks or do not fully meet the requirements:

Option B: Integrating with AWS Directory Service and configuring it as an API Gateway authorizer may be unnecessary since the company already has a third-party identity provider.

Option C: Requiring the web application to retrieve AWS STS tokens may be unnecessary since the company already has OAuth tokens issued by the third-party identity provider.

Option D: Creating IAM users and extracting request parameters can be more complex and may not leverage the existing third-party identity provider and OAuth token issuance process.

upvoted 3 times

 **Daniel76** 1 year, 3 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/security/use-aws-lambda-authorizers-with-a-third-party-identity-provider-to-secure-amazon-api-gateway-rest-apis/>

upvoted 4 times

 **Daniel76** 1 year, 3 months ago

Selected Answer: A

Building a Lambda authorizer allows users to access API Gateway resources by using their third-party credentials without having to configure additional services, such as Amazon Cognito. This can be particularly useful if your organization is using the third-party identity provider for single sign-on (SSO).

<https://aws.amazon.com/blogs/security/use-aws-lambda-authorizers-with-a-third-party-identity-provider-to-secure-amazon-api-gateway-rest-apis/>

upvoted 1 times

 **gfhbox0083** 1 year, 5 months ago

Selected Answer: A

A, for sure.

Lambda authorizers can integrate with external identity providers, including OAuth2, OpenID Connect, and others, to validate tokens or credentials.

upvoted 1 times

 **vip2** 1 year, 5 months ago

Selected Answer: A

A

API GW + integrated Lambda Authorizer for Authen. and Author.

upvoted 2 times

 **kupo777** 1 year, 6 months ago

A

It is reasonable to configure the API Gateway Lambda authorizer to validate tokens from identity providers.

upvoted 2 times

Question #518

Topic 1

A company has deployed applications to thousands of Amazon EC2 instances in an AWS account. A security audit discovers that several unencrypted Amazon Elastic Block Store (Amazon EBS) volumes are attached to the EC2 instances. The company's security policy requires the EBS volumes to be encrypted.

The company needs to implement an automated solution to encrypt the EBS volumes. The solution also must prevent development teams from creating unencrypted EBS volumes.

Which solution will meet these requirements?

- A. Configure the AWS Config managed rule that identifies unencrypted EBS volumes. Configure an automatic remediation action. Associate an AWS Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Create an AWS Key Management Service (AWS KMS) customer managed key. In the key policy, include a statement to deny the creation of unencrypted EBS volumes.
- B. Use AWS Systems Manager Fleet Manager to create a list of unencrypted EBS volumes. Create a Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Create an SCP to deny the creation of unencrypted EBS volumes.
- C. Use AWS Systems Manager Fleet Manager to create a list of unencrypted EBS volumes. Create a Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Modify the AWS account setting for EBS encryption to always encrypt new EBS volumes.
- D. Configure the AWS Config managed rule that identifies unencrypted EBS volumes. Configure an automatic remediation action. Associate an AWS Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Modify the AWS account setting for EBS encryption to always encrypt new EBS volumes.

Correct Answer: D

Community vote distribution

D (90%)	10%
---------	-----

 **AzureDP900** 1 year, 1 month ago

Option D meet the requirements of automatically encrypting existing unencrypted EBS volumes and preventing development teams from creating unencrypted EBS volumes, you can configure an AWS Config managed rule that identifies unencrypted EBS volumes. The automatic remediation action should be to create a new encrypted EBS volume and replace the old one. Additionally, modifying the AWS account setting for EBS encryption to always encrypt new EBS volumes ensures that no more unencrypted EBS volumes are created in the future.

upvoted 3 times

 **sammyhaj** 1 year, 1 month ago

Selected Answer: B

Issue is that NONE prevent new EBS volumes to be launched without encryption, albeit systems manager can remediate it isn't ideal. regardless you need a solution to PREVENT 100% unencrypted drives, and this is only done via SCP. other items can be circumvented by CLI

upvoted 1 times

 **alexbraila** 1 year ago

SCPs are not available in this case, as the question is about a standalone AWS account, not an organization

upvoted 2 times

 **Daniel76** 1 year, 1 month ago

Selected Answer: D

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>
1. Use AWS Config to detect an unencrypted EBS volume. Not fleet manager. B and C out.

2. System manager runbook is the automation that creates an encrypted copy of the EBS snapshot and replaces the unencrypted EBS with the encrypted copy. The KMS is used for the encryption and it cannot be used to deny creation of unencrypted EBS volume (A is out).

upvoted 2 times

 **PSPaul** 1 year, 2 months ago

My answer is D

Proactive Remediation: The AWS Config rule and Automation runbook identify and remediate existing unencrypted volumes automatically. Preventive Measure: The modified AWS account setting ensures that all new EBS volumes created in the account are automatically encrypted.

This approach provides a comprehensive solution that addresses both existing unencrypted volumes and future volume creation.

Why not Option A: While it addresses the issue of existing unencrypted volumes, it doesn't prevent future unencrypted volume creation.

upvoted 2 times

 **vip2** 1 year, 5 months ago

Selected Answer: D

D is correct instead of A because AWS support change account setting for EBS encryption

upvoted 3 times

 **Helpnosense** 1 year, 5 months ago

Selected Answer: D

Use config to find unencrypted EBS. Change the default setting.

upvoted 2 times

 **kupo777** 1 year, 6 months ago

D

Enabling default encryption for EBSs prevents the creation of unencrypted EBSs.

upvoted 2 times

 **awsaz** 1 year, 6 months ago

Selected Answer: D

the answer is D

upvoted 2 times

Question #519

Topic 1

A company is running a large containerized workload in the AWS Cloud. The workload consists of approximately 100 different services. The company uses Amazon Elastic Container Service (Amazon ECS) to orchestrate the workload.

Recently the company's development team started using AWS Fargate instead of Amazon EC2 instances in the ECS cluster. In the past, the workload has come close to running the maximum number of EC2 instances that are available in the account.

The company is worried that the workload could reach the maximum number of ECS tasks that are allowed. A solutions architect must implement a solution that will notify the development team when Fargate reaches 80% of the maximum number of tasks.

What should the solutions architect do to meet this requirement?

- A. Use Amazon CloudWatch to monitor the Sample Count statistic for each service in the ECS cluster. Set an alarm for when the math expression sample count/SERVICE_QUOTA(service)*100 is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- B. Use Amazon CloudWatch to monitor service quotas that are published under the AWS/Usage metric namespace. Set an alarm for when the math expression metric/SERVICE_QUOTA(metric)*100 is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- C. Create an AWS Lambda function to poll detailed metrics from the ECS cluster. When the number of running Fargate tasks is greater than 80, invoke Amazon Simple Email Service (Amazon SES) to notify the development team.
- D. Create an AWS Config rule to evaluate whether the Fargate SERVICE_QUOTA is greater than 80. Use Amazon Simple Email Service (Amazon SES) to notify the development team when the AWS Config rule is not compliant.

Correct Answer: B

Community vote distribution

B (100%)

 **kupo777** Highly Voted 1 year, 5 months ago

B

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Quotas-Visualize-Alarms.html>
upvoted 5 times

 **Daniel76** Most Recent 1 year, 1 month ago

Selected Answer: B

C and D are out due to using SES and not SNS for simple notification.

Among A and B, A is out because CloudWatch alarm was set with SERVICE_QUOTA but the option choose to monitor sample count stats instead of service quota published.

upvoted 1 times

 **Chakanetsa** 1 year, 3 months ago

Selected Answer: B

Why this is the correct choice:

AWS/Usage metric namespace: This namespace provides detailed metrics for service usage and quotas, including the number of running ECS Fargate tasks. You can use this data to monitor how close you are to the service quotas.

Service quota monitoring: The math expression metric/SERVICE_QUOTA(metric)*100 allows you to calculate the percentage of the quota being used, making it easy to set an alarm when usage reaches 80%.

CloudWatch Alarm: This is a native and efficient way to monitor service usage, and you can easily configure notifications via Amazon SNS to alert the development team when the threshold is crossed.

upvoted 3 times

 **c22ddd8** 1 year, 5 months ago

Selected Answer: B

Service Quota

upvoted 2 times

Question #520

Topic 1

A company has several AWS Lambda functions written in Python. The functions are deployed with the .zip package deployment type. The functions use a Lambda layer that contains common libraries and packages in a .zip file. The Lambda .zip packages and Lambda layer .zip file are stored in an Amazon S3 bucket.

The company must implement automatic scanning of the Lambda functions and the Lambda layer to identify CVEs. A subset of the Lambda functions must receive automated code scans to detect potential data leaks and other vulnerabilities. The code scans must occur only for selected Lambda functions, not all the Lambda functions.

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

- A. Activate Amazon Inspector. Start automated CVE scans.
- B. Activate Lambda standard scanning and Lambda code scanning in Amazon Inspector.
- C. Enable Amazon GuardDuty. Enable the Lambda Protection feature in GuardDuty.
- D. Enable scanning in the Monitor settings of the Lambda functions that need code scans.
- E. Tag Lambda functions that do not need code scans. In the tag, include a key of InspectorCodeExclusion and a value of LambdaCodeScanning.
- F. Use Amazon Inspector to scan the S3 bucket that contains the Lambda .zip packages and the Lambda layer .zip file for code scans.

Correct Answer: ABE

Community vote distribution

ABE (100%)

 **vip2** Highly Voted 1 year, 5 months ago

Selected Answer: ABE

A, B and E
Inspector for Lambda std scanning and code scanning
Lambda Function with monitor setting to code scan
Tag for conditional function, not for all functions
upvoted 5 times

 **JoeTromundo** Most Recent 1 year, 2 months ago

Selected Answer: ABE

A: Amazon Inspector can automatically scan your Lambda functions for known vulnerabilities (CVEs) in the dependencies of the functions. This action will initiate the security scanning of Lambda functions and Lambda layers to detect vulnerabilities.
B: Amazon Inspector provides enhanced scanning features for Lambda functions. This includes both standard scanning (for CVEs in dependencies and layers) and code scanning (for potential vulnerabilities, like data leaks, directly in the code).
E: <https://docs.aws.amazon.com/lambda/latest/dg/governance-code-scanning.html#:~:text>To%20exclude%20a%20Lambda%20function,Value%3ALambdaStandardScanning>.
"To exclude a Lambda function from code scans, tag the function with the following key-value pair:
Key:InspectorCodeExclusion
Value:LambdaCodeScanning"
upvoted 2 times

 **kgpoj** 1 year, 3 months ago

Selected Answer: ABE

A: Need to Activate Amazon Inspector first
B: For **CVE**, need to use **Lambda standard scanning**
B: For **data leaks**, need to use Lambda code scanning
E: Tag Lambda functions that do not need code scans
upvoted 2 times

 **guruguru** 1 year, 3 months ago

ABE,
<https://docs.aws.amazon.com/inspector/latest/user/scanning-lambda.html>
To exclude a Lambda function from Lambda standard scanning, tag the function with the following key-value pair:
Key:InspectorExclusion
Value:LambdaStandardScanning
upvoted 1 times

Question #521

A company is changing the way that it handles patching of Amazon EC2 instances in its application account. The company currently patches instances over the internet by using a NAT gateway in a VPC in the application account.

The company has EC2 instances set up as a patch source repository in a dedicated private VPC in a core account. The company wants to use AWS Systems Manager Patch Manager and the patch source repository in the core account to patch the EC2 instances in the application account. The company must prevent all EC2 instances in the application account from accessing the internet.

The EC2 instances in the application account need to access Amazon S3, where the application data is stored. These EC2 instances need connectivity to Systems Manager and to the patch source repository in the private VPC in the core account.

Which solution will meet these requirements?

- A. Create a network ACL that blocks outbound traffic on port 80. Associate the network ACL with all subnets in the application account. In the application account and the core account, deploy one EC2 instance that runs a custom VPN server. Create a VPN tunnel to access the private VPC. Update the route table in the application account.
- B. Create private VIFs for Systems Manager and Amazon S3. Delete the NAT gateway from the VPC in the application account. Create a transit gateway to access the patch source repository EC2 instances in the core account. Update the route table in the core account.
- C. Create VPC endpoints for Systems Manager and Amazon S3. Delete the NAT gateway from the VPC in the application account. Create a VPC peering connection to access the patch source repository EC2 instances in the core account. Update the route tables in both accounts.
- D. Create a network ACL that blocks inbound traffic on port 80. Associate the network ACL with all subnets in the application account. Create a transit gateway to access the patch source repository EC2 instances in the core account. Update the route tables in both accounts.

Correct Answer: C

Community vote distribution

C (100%)

 **SIJUTHOMASP** 1 year ago

Selected Answer: C

Why not B?

upvoted 1 times

 **Daniel76** 1 year, 3 months ago

Selected Answer: C

Aftee delete NAT gateway theres no need to block outbound port 80. Use vpc interface endpoint to keep traffic private.
<https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-create-vpc.html>

upvoted 2 times

 **AzureDP900** 1 year, 3 months ago

C is right

Here's why:

The company needs to prevent all EC2 instances in the application account from accessing the internet, which means they can't use a NAT gateway.

They need to access Amazon S3 and Systems Manager, so creating VPC endpoints for these services is the way to go.

A VPC peering connection between the two accounts will allow the EC2 instances in the application account to access the patch source repository in the core account.

Updating the route tables in both accounts is necessary to ensure that traffic is properly routed.

upvoted 1 times

 **Alagong** 1 year, 5 months ago

Selected Answer: C

answer : C

upvoted 3 times

 **kupo777** 1 year, 5 months ago

A, D

A block of Port.80 is not enough.

B

private VIFs is inadequate.

The correct answer is C.

upvoted 3 times

Question #522

Topic 1

A company in the United States (US) has acquired a company in Europe. Both companies use the AWS Cloud. The US company has built a new application with a microservices architecture. The US company is hosting the application across five VPCs in the us-east-2 Region. The application must be able to access resources in one VPC in the eu-west-1 Region. However, the application must not be able to access any other VPCs.

The VPCs in both Regions have no overlapping CIDR ranges. All accounts are already consolidated in one organization in AWS Organizations.

Which solution will meet these requirements MOST cost-effectively?

- A. Create one transit gateway in eu-west-1. Attach the VPCs in us-east-2 and the VPC in eu-west-1 to the transit gateway. Create the necessary route entries in each VPC so that the traffic is routed through the transit gateway.
- B. Create one transit gateway in each Region. Attach the involved subnets to the regional transit gateway. Create the necessary route entries in the associated route tables for each subnet so that the traffic is routed through the regional transit gateway. Peer the two transit gateways.
- C. Create a full mesh VPC peering connection configuration between all the VPCs. Create the necessary route entries in each VPC so that the traffic is routed through the VPC peering connection.
- D. Create one VPC peering connection for each VPC in us-east-2 to the VPC in eu-west-1. Create the necessary route entries in each VPC so that the traffic is routed through the VPC peering connection.

Correct Answer: D

Community vote distribution

D (89%)

11%

 **aahrentom** Highly Voted 1 year, 5 months ago

Selected Answer: D

is most cost-effectively
upvoted 5 times

 **AzureDP900** Most Recent 1 year, 1 month ago

D meets the requirements most cost-effectively because:
Minimum infrastructure: Creating a single VPC peering connection between each of the five VPCs in us-east-2 and the VPC in eu-west-1 requires minimal infrastructure changes.
Simple management: This solution requires only one VPC peering connection, making it easier to manage and monitor network connectivity.
No need for transit gateway: Since you already have a dedicated VPC in eu-west-1 that needs to be accessed, creating a VPC peering connection is the most straightforward approach.
upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

D is best in the scenario.
upvoted 1 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: D

VPC peer-to-peer connection is a free service in AWS used for communication between VPCs.
AWS's Transit Gateway is mainly used for connecting across multiple VPCs or accounts and does not directly support cross regional VPC connections.
upvoted 3 times

 **GDuque** 1 year, 4 months ago

Selected Answer: A

Taking into account what solutions are possible, only A or B can do it, because we need a transit gateway to connect VPCs that are in different regions. You cannot peer both vpcs directly. And as for costing, A is more economic.
upvoted 1 times

 **GDuque** 1 year, 4 months ago

After reconsidering, the answer is D.
With Inter-region VPC peering you can peer 2 VPCs in different regions. So, the most economic solution is D.
upvoted 3 times

Question #523

A travel company built a web application that uses Amazon Simple Email Service (Amazon SES) to send email notifications to users. The company needs to enable logging to help troubleshoot email delivery issues. The company also needs the ability to do searches that are based on recipient, subject, and time sent.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Create an Amazon SES configuration set with Amazon Data Firehose as the destination. Choose to send logs to an Amazon S3 bucket.
- B. Enable AWS CloudTrail logging. Specify an Amazon S3 bucket as the destination for the logs.
- C. Use Amazon Athena to query the logs in the Amazon S3 bucket for recipient, subject, and time sent.
- D. Create an Amazon CloudWatch log group. Configure Amazon SES to send logs to the log group.
- E. Use Amazon Athena to query the logs in Amazon CloudWatch for recipient, subject, and time sent.

Correct Answer: AC*Community vote distribution*

AC (75%) DE (17%) 8%

 **AzureDP900** 1 year, 1 month ago

A,C

By creating a configuration set with Data Firehose as the destination (A), the SES logs will be stored in an S3 bucket. Then, using Athena (C) allows you to query those logs for specific information, such as recipient, subject, and time sent

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: AC

- A: An Amazon SES configuration set allows you to capture event data related to email sending, such as delivery status, bounces, and complaints. By setting Amazon Kinesis Data Firehose as the destination, you can stream these logs to an Amazon S3 bucket.
- C: Once the logs are in the S3 bucket, Amazon Athena allows you to run SQL queries directly on the data stored in S3. This enables easy searching and filtering by recipient, subject, and time sent, without having to move or load the data into a database.
- B: CloudTrail logs API calls to Amazon SES but does NOT provide detailed information about email delivery, bounces, or complaints.
- D: While you can monitor metrics in CloudWatch, it's not a good fit for storing or searching detailed SES email logs.
- E: CloudWatch logs are not natively queryable using Athena.

upvoted 2 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: AC

- A. Amazon Data Firehose is configured as the target of SES configuration set, which can capture and transfer SES log data in real-time to Amazon S3 storage buckets.
- B. CloudTrail is primarily used to track AWS management operations, rather than service level operation logs.
- C. Amazon Athena allows you to directly analyze data stored in Amazon S3 using SQL queries.
- D. Amazon SES does not directly support sending logs to CloudWatch.
- E. Athena does not support directly querying logs in CloudWatch.

upvoted 4 times

 **starcub** 1 year, 2 months ago

Yes it does with the connector -> <https://docs.aws.amazon.com/athena/latest/ug/connectors-cloudwatch.html>

upvoted 1 times

 **jopaca1216** 1 year, 3 months ago

Selected Answer: AC

Just It.

<https://docs.aws.amazon.com/ses/latest/dg/event-publishing-add-event-destination-firehose.html>

upvoted 1 times

 **neta1o** 1 year, 4 months ago

Selected Answer: AC

The answers seem pretty split on this. Based on this <https://docs.aws.amazon.com/athena/latest/ug/querying-ses-logs.html> I'd go A/C

upvoted 2 times

 **jopaca1216** 1 year, 3 months ago

I'd go A/C too.

upvoted 1 times

 **Russ99** 1 year, 5 months ago

A & C is the correct answer.

upvoted 4 times

 **vip2** 1 year, 5 months ago

Selected Answer: CE

Athena can not direct query Cloudwatch log, so C is correct instead of E.

upvoted 1 times

 **G4Exams** 1 year, 5 months ago

A & C. Cloudtrail does not track the emails.

upvoted 3 times

 **[Removed]** 1 year, 5 months ago

Selected Answer: DE

<https://aws.amazon.com/blogs/messaging-and-targeting/how-to-log-amazon-ses-details-using-amazon-cloudwatch/>

upvoted 2 times

 **Hizumi** 1 year, 5 months ago

It cannot be D&E because SES Event data with Cloudwatch is not able to retrieve recipient, mail headers, and timestamp, this is what it can as per this article: <https://docs.aws.amazon.com/ses/latest/dg/event-publishing-retrieving-cloudwatch.html>

A&C is a better choice as it is able to retrieve the information the questions is asking as per this article:

<https://docs.aws.amazon.com/ses/latest/dg/event-publishing-retrieving-firehose-contents.html>

upvoted 1 times

Question #524

A company migrated to AWS and uses AWS Business Support. The company wants to monitor the cost-effectiveness of Amazon EC2 instances across AWS accounts. The EC2 instances have tags for department, business unit, and environment. Development EC2 instances have high cost but low utilization.

The company needs to detect and stop any underutilized development EC2 instances. Instances are underutilized if they had 10% or less average daily CPU utilization and 5 MB or less network I/O for at least 4 of the past 14 days.

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

- A. Configure Amazon CloudWatch dashboards to monitor EC2 instance utilization based on tags for department, business unit, and environment. Create an Amazon EventBridge rule that invokes an AWS Lambda function to stop underutilized development EC2 instances.
- B. Configure AWS Systems Manager to track EC2 instance utilization and report underutilized instances to Amazon CloudWatch. Filter the CloudWatch data by tags for department, business unit, and environment. Create an Amazon EventBridge rule that invokes an AWS Lambda function to stop underutilized development EC2 instances.
- C. Create an Amazon EventBridge rule to detect low utilization of EC2 instances reported by AWS Trusted Advisor. Configure the rule to invoke an AWS Lambda function that filters the data by tags for department, business unit, and environment and stops underutilized development EC2 instances.
- D. Create an AWS Lambda function to run daily to retrieve utilization data for all EC2 instances. Save the data to an Amazon DynamoDB table. Create an Amazon QuickSight dashboard that uses the DynamoDB table as a data source to identify and stop underutilized development EC2 instances.

Correct Answer: C

Community vote distribution

C (82%)

A (18%)

 **Curious76** 5 months, 3 weeks ago

Selected Answer: C

CloudWatch dashboards are for visual monitoring, not detection.

upvoted 1 times

 **alexbraila** 1 year ago

Selected Answer: C

Due to the link posted by Kinnam and sam2ng, together with this

<https://docs.aws.amazon.com/awssupport/latest/user/cloudwatch-events-ta.html>

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

Option C, This solution meets the requirements with the least operational overhead because it uses Amazon EventBridge (formerly CloudWatch Events) to trigger a response based on low utilization reports from AWS Trusted Advisor.

AWS Trusted Advisor provides pre-configured dashboards that can be used to monitor various aspects of your AWS resources, including EC2 instance utilization. By leveraging these pre-configured dashboards, you don't need to set up additional monitoring infrastructure or write custom code.

The EventBridge rule will automatically invoke the Lambda function when a low utilization report is received from Trusted Advisor, which eliminates the need for daily polling or manual intervention. The other options are more resource-intensive and require additional setup and maintenance:

upvoted 1 times

 **JoeTromundo** 1 year, 2 months ago

Selected Answer: C

AWS Trusted Advisor provides insights into underutilized EC2 instances automatically, including recommendations for cost-saving based on utilization metrics like CPU and network usage. Since the company is using AWS Business Support, they already have access to Trusted Advisor, making this a low-overhead solution.

Amazon EventBridge can be used to create a rule that detects when Trusted Advisor reports low-utilization instances. This avoids the need for custom-built CloudWatch dashboards or manual tracking.

AWS Lambda can be triggered to handle the logic of stopping instances that meet the specific criteria of low CPU utilization and network I/O, filtering by tags for department, business unit, and environment. Lambda is serverless and scales automatically, so it minimizes operational overhead.

upvoted 3 times

✉ **Kinnam** 1 year, 4 months ago

Selected Answer: C

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html#low-utilization-amazon-ec2-instances>
upvoted 2 times

✉ **sam2ng** 1 year, 4 months ago

Selected Answer: C

This is exactly the same criteria provided by the Trusted Advisor:
<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html#low-utilization-amazon-ec2-instances>
upvoted 3 times

✉ **gfhbox0083** 1 year, 5 months ago

Selected Answer: C

C, for sure.
TA for 10% or less average daily CPU utilization and 5 MB or less network I/O for at least 4 of the past 14 days.
And least operational overhead
upvoted 2 times

✉ **Moumita** 1 year, 5 months ago

Selected Answer: C

A - involves continuous monitoring and potential updates to dashboards and metrics.
C - minimizes ongoing maintenance by relying on Trusted Advisor's automated reports.
upvoted 1 times

✉ **asquared16** 1 year, 5 months ago

Selected Answer: C

A is not correct as it's missing setting up alarms for the "detect" part. I go with C.
upvoted 1 times

✉ **vip2** 1 year, 5 months ago

Selected Answer: A

It would be A as correct answer
Tagging with EC2 instances for department, business unit, and environment .

CloudWatch to collect and monitor CPU utilization and network I/O metrics.

Create CloudWatch Alarms to detect underutilized instances with composite alarmwith boh CPU utilization and network I/O are low.

AWS Lambda Function to be triggered by the CloudWatch Alarms and check
the conditions (10% or less average daily CPU utilization and 5 MB or less network I/O) hold true for at least 4 of the past 14 days. Stop the instances that meet these criteria.
upvoted 3 times

✉ **zolthar_z** 1 year, 3 months ago

Unless you create an alarm or something cloudwatch dashboard will not take any action to delete the instances, it will only show the metric data

upvoted 1 times

✉ **0dc6cac** 6 months, 1 week ago

Feels like the proper way to do it is by cloudwatch alarm that invokes a lambda function. But assuming A doesn't include an alarm, I guess it has to be C
upvoted 1 times

✉ **paderni** 1 year, 5 months ago

Not c because AWS Trusted Advisor does not provide real-time utilization metrics suitable for detecting underutilized instances over a specific timeframe. It focuses more on best practices and recommendations rather than real-time operational metrics. Should be B
upvoted 1 times

✉ **c22ddd8** 1 year, 5 months ago

Will B monitor multi account ? NO Ans is C , question says to stop of the instance is low for 4 days in last 14 days.
upvoted 2 times

Question #525

Topic 1

A company is hosting an application on AWS for a project that will run for the next 3 years. The application consists of 20 Amazon EC2 On-Demand Instances that are registered in a target group for a Network Load Balancer (NLB). The instances are spread across two Availability Zones. The application is stateless and runs 24 hours a day, 7 days a week.

The company receives reports from users who are experiencing slow responses from the application. Performance metrics show that the instances are at 10% CPU utilization during normal application use. However, the CPU utilization increases to 100% at busy times, which typically last for a few hours.

The company needs a new architecture to resolve the problem of slow responses from the application.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an Auto Scaling group. Attach the Auto Scaling group to the target group of the NLB. Set the minimum capacity to 20 and the desired capacity to 28. Purchase Reserved Instances for 20 instances.
- B. Create a Spot Fleet that has a request type of request. Set the TotalTargetCapacity parameter to 20. Set the DefaultTargetCapacityType parameter to On-Demand. Specify the NLB when creating the Spot Fleet.
- C. Create a Spot Fleet that has a request type of maintain. Set the TotalTargetCapacity parameter to 20. Set the DefaultTargetCapacityType parameter to Spot. Replace the NLB with an Application Load Balancer.
- D. Create an Auto Scaling group. Attach the Auto Scaling group to the target group of the NLB. Set the minimum capacity to 4 and the maximum capacity to 28. Purchase Reserved Instances for four instances.

Correct Answer: D

Community vote distribution

D (60%)

A (40%)

 **redipa** 1 month, 3 weeks ago

Selected Answer: D

20 instances are running at 10% cpu utilization for 20 out of 24 hours. Reducing to only 4 instances would be average 50% cpu. Purchase RIs for the 4 instances running all day. Change the ASG to go to 28 total instances to handle the busy 4 hour period.

upvoted 2 times

 **ciscochamps** 3 months, 2 weeks ago

Selected Answer: D

COST EFFECTIVE

upvoted 2 times

 **Kaps443** 6 months, 1 week ago

Selected Answer: A

D is incorrect you'd run 16 On-Demand instances 24/7, which is more expensive than reserving 20 baseline instances.

upvoted 2 times

 **BelloMio** 8 months, 2 weeks ago

Selected Answer: A

A

But why is option D (min=4, max=28) not ideal, even though it seems efficient?

Current complaints are about latency and slow responses during peak usage, not normal usage.

That means the important thing is to be able to scale quickly and high enough when needed — and option D doesn't pre-warm or reserve any of that burst capacity.

Only 4 Reserved Instances means:

You're paying On-Demand for up to 24 extra instances during every traffic spike.

Over 3 years of usage, this is less cost-effective than reserving the always-needed baseline of 20.

Latency in scaling:

If peak load hits suddenly, starting from 4 → 28 takes time (EC2 warm-up, app boot time, etc).

Option A, with 20 already provisioned and reserved, absorbs sudden spikes without lag.

upvoted 2 times

 **AzureDP900** 1 year, 1 month ago

D is more cost effective solution, most of the time CPU 10% and peak time only we need more instance to serve customer traffic.
upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

The minimum capacity of 4 instances will provide sufficient resources to handle normal traffic, while the maximum capacity of 28 instances can be scaled up to handle busy periods.

By purchasing Reserved Instances for four instances, the company can also take advantage of a discounted rate for usage of EC2 instances, which will help reduce costs further.

upvoted 1 times

 **altonh** 10 months, 1 week ago

How do you know that 28 is enough during peak?

upvoted 2 times

 **Alagong** 1 year, 5 months ago

Selected Answer: D

It should be D

upvoted 2 times

 **kupo777** 1 year, 5 months ago

D

D

Since the CPU utilization of the instance is 10% during normal application use, a minimum capacity of 4 is required, which is the minimum configuration and most cost-effective.

upvoted 4 times

Question #526

Accompany is building an application to collect and transmit sensor data from a factory. The application will use AWS IoT Core to send data from hundreds of devices to an Amazon S3 data lake. The company must enrich the data before loading the data into Amazon S3.

The application will transmit the sensor data every 5 seconds. New sensor data must be available in Amazon S3 less than 30 minutes after the application collects the data. No other applications are processing the sensor data from AWS IoT Core.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a topic in AWS IoT Core to ingest the sensor data. Create an AWS Lambda function to enrich the data and to write the data to Amazon S3. Configure an AWS IoT rule action to invoke the Lambda function.
- B. Use AWS IoT Core Basic Ingest to ingest the sensor data. Configure an AWS IoT rule action to write the data to Amazon Kinesis Data Firehose. Set the Kinesis Data Firehose buffering interval to 900 seconds. Use Kinesis Data Firehose to invoke an AWS Lambda function to enrich the data, Configure Kinesis Data Firehose to deliver the data to Amazon S3.
- C. Create a topic in AWS IoT Core to ingest the sensor data. Configure an AWS IoT rule action to send the data to an Amazon Timestream table. Create an AWS Lambda, function to read the data from Timestream. Configure the Lambda function to enrich the data and to write the data to Amazon S3.
- D. Use AWS IoT Core Basic Ingest to ingest the sensor data. Configure an AWS IoT rule action to write the data to Amazon Kinesis Data Streams. Create a consumer AWS Lambda function to process the data from Kinesis Data Streams and to enrich the data. Call the S3 PutObject API operation from the Lambda function to write the data to Amazon S3.

Correct Answer: B

Community vote distribution

B (65%)

A (35%)

 mark_232323 Highly Voted 1 year, 5 months ago

Selected Answer: B

<https://aws.amazon.com/blogs/iot/ingesting-enriched-iot-data-into-amazon-s3-using-amazon-kinesis-data-firehose/>
upvoted 10 times

 053081f Highly Voted 1 year, 5 months ago

Selected Answer: A

In this application, sensor data is transmitted at the following intervals:

1. Device to IoT Core (every 5 seconds)
2. IoT Core to S3 (every 30 minutes)

The data load from IoT Core to S3 doesn't necessarily need to be real-time, and the most cost-effective solution is option A. Option A uses the simplest method to load data without using resources like Kinesis.

upvoted 6 times

 zolthar_z 1 year, 3 months ago

Answer is C, hundreds of devices sending data every 5 seconds, if you have 100 devices you will trigger the lambda 1200 times in one minute,
upvoted 3 times

 Blair77 Most Recent 2 months, 4 weeks ago

Selected Answer: B

B is good. A - While this solution would work, invoking a Lambda function for every single message from every device would be extremely expensive. You would be paying for hundreds of thousands, if not millions, of Lambda invocations daily, which is far less cost-effective than using Firehose to batch and invoke Lambda in bulk.

upvoted 1 times

 mik_asa 7 months ago

Selected Answer: B

Option B stands out as the most cost-effective and efficient solution. Kinesis Data Firehose is specifically designed for this type of workload: collecting streaming data, optionally transforming it with Lambda, and delivering it to S3 in optimized batches. The 900-second buffering interval ensures that the data is available in S3 well within the 30-minute requirement while minimizing S3 PUT requests and optimizing Lambda invocation costs for enrichment. AWS IoT Core Basic Ingest further contributes to cost savings by providing a leaner ingestion path.

upvoted 2 times

 **85b5b55** 10 months, 2 weeks ago

Selected Answer: A

the requirements is MOST cost-effective solutions. hence, I choosed A. (i.e. Less resources)

upvoted 1 times

 **AzureDP900** 1 year, 1 month ago

B is right, this meets the requirement of making new sensor data available in Amazon S3 less than 30 minutes after the application collects the data. The buffering interval of 900 seconds (15 minutes) is sufficient to meet this requirement, and the use of Kinesis Data Firehose ensures that the data is processed and delivered to Amazon S3 in a timely manner.

This solution is also cost-effective because it:

Uses AWS IoT Core Basic Ingest, which is free for up to 10 GB of incoming data per month.

Uses Kinesis Data Firehose, which has a low cost compared to other services like Lambda or Timestream.

Does not require the creation of multiple resources (e.g., Lambda functions, topics) as in some other solutions.

upvoted 1 times

 **sashenka** 1 year, 1 month ago

Selected Answer: A

Option A is the most cost-effective solution because:

- * Uses minimal services while meeting all requirements
- * Leverages serverless architecture for automatic scaling
- * Provides immediate processing without buffering delays
- * Minimizes costs by eliminating unnecessary services
- * Direct integration between IoT Core and Lambda ensures low latency

The Lambda function can process messages immediately as they arrive from IoT Core, enrich the data, and write to S3 well within the 30-minute requirement. This architecture is both simple and cost-effective, avoiding unnecessary services and their associated costs.

upvoted 1 times

 **sashenka** 1 year, 1 month ago

Why not Option B? : IoT Core → Firehose → Lambda → S3

- * 900-second (15-minute) buffer adds unnecessary delay
- * Additional cost for Firehose service
- * More complex than necessary for the use case

upvoted 1 times

 **doobc** 1 year, 1 month ago

B. buffering helps with cost of lambda

upvoted 1 times

 **Danm86** 1 year, 2 months ago

AWS IoT Core Basic is cheaper than AWS IoT core, also Kinesis Data Firehose Batching will reduce the number of write operations to S3 and Lambda invocations by buffering data. Hence even though there is an additional component of Kinesis Data Firehose, it is more cost effective than option A. According to me, the answer is Option B

upvoted 2 times

 **Daniel76** 1 year, 3 months ago

Selected Answer: B

No other applications are processing the sensor data from AWS IoT Core:

Use AWS IoT Core Basic Ingest to ingest the sensor data to reduce messaging cost: B or D

<https://docs.aws.amazon.com/iot/latest/developerguide/iot-basic-ingest.html>

Configure an AWS IoT rule action to write the data to Amazon KDF or KDS? "New sensor data must be available in Amazon S3 less than 30 minutes after the application collects the data." =>near real time, stream data to s3, no need storage or replay, we shd use autoscaling and fully managed KDF.

upvoted 2 times

 **liuliangzhou** 1 year, 3 months ago

Selected Answer: A

A. The advantage of this method is its simplicity and high real-time performance, as Lambda functions can immediately respond to IoT events. The cost of Lambda functions is based on execution time and resource usage, which is very economical for small data processing tasks.

B. The 900 second buffer interval of Kinesis Data Firehose does not meet real-time requirements (data needs to be processed within 30 minutes, while the set buffer here is 15 minutes). In addition, introducing Kinesis Data Firehose adds additional cost and complexity, especially when Lambda functions can directly process data.

upvoted 1 times

 **jopaca1216** 1 year, 3 months ago

Selected Answer: B

Many devices sending data every 5 seconds, it's not necessary, due that you just need the data available in S3 within 30 minutes!

upvoted 2 times

 **_Jassybang_** 1 year, 3 months ago

the data emitting time is 5 sec and lambda may take upto 15 mins to enrich the data , this detail is only captured in buffer section of KFS , hence going with B, If there is SQS queue in option A before lambda then i would have chosen that

upvoted 1 times

 **dzidis** 1 year, 4 months ago

Selected Answer: B

As per this link it is B, firehose is used:

<https://aws.amazon.com/blogs/iot/ingesting-enriched-iot-data-into-amazon-s3-using-amazon-kinesis-data-firehose/>

upvoted 2 times

 **Incognito013** 1 year, 4 months ago

Selected Answer: A

We need simple and cost effective so choosing A

upvoted 2 times

 **tsangckl** 1 year, 5 months ago

Selected Answer: B

I prefer B

upvoted 3 times

 **Chakanetsa** 1 year, 5 months ago

Selected Answer: B

Best Answer: B. Use AWS IoT Core Basic Ingest to ingest the sensor data. Configure an AWS IoT rule action to write the data to Amazon Kinesis Data Firehose. Set the Kinesis Data Firehose buffering interval to 900 seconds. Use Kinesis Data Firehose to invoke an AWS Lambda function to enrich the data, Configure Kinesis Data Firehose to deliver the data to Amazon S3.

Reasoning:

Cost-effective: IoT Core Basic Ingest is the most cost-effective option for high-volume, low-value data.

Low latency: Kinesis Data Firehose with a 900-second buffering interval provides a balance between cost and latency, meeting the requirement of data availability in S3 within 30 minutes.

Scalability: Kinesis Data Firehose can handle high throughput, making it suitable for large volumes of sensor data.

Simplicity: The solution involves a straightforward pipeline with minimal components.

upvoted 4 times

Question #527

Topic 1

A company is collecting data from a large set of IoT devices. The data is stored in an Amazon S3 data lake. Data scientists perform analytics on Amazon EC2 instances that run in two public subnets in a VPC in a separate AWS account.

The data scientists need access to the data lake from the EC2 instances. The EC2 instances already have an assigned role with permissions to access Amazon S3.

According to company policies, only authorized networks are allowed to have access to the IoT data.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Create a gateway VPC endpoint for Amazon S3 in the data scientists' VPC.
- B. Create an S3 access point in the data scientists' AWS account for the data lake.
- C. Update the EC2 instance role. Add a policy with a condition that allows the s3:GetObject action when the value for the s3:DataAccessPointArn condition key is a valid access point ARN.
- D. Update the VPC route table to route S3 traffic to an S3 access point.
- E. Add an S3 bucket policy with a condition that allows the s3:GetObject action when the value for the s3:DataAccessPointArn condition key is a valid access point ARN.

Correct Answer: AE

Community vote distribution

AE (58%)

BE (40%)

 **TBI** 5 months, 2 weeks ago

Migration Evalutor is a cost comparison calculator that looks at what you are currently spending on-premises versus what you would spend on AWS

upvoted 1 times

 **strike3test** 5 months, 2 weeks ago

Selected Answer: AE

Why not the others?

B (Create an S3 access point in the data scientists' AWS account): Access points are created in the bucket owner's account (the data lake account), not in the data scientists' account. So this is not applicable here.

C (Update the EC2 instance role with s3:DataAccessPointArn condition): The IAM role on EC2 controls permissions for the instance, but the bucket policy is the primary place to restrict access by network or access point. The EC2 role already has permissions, so this is not necessary.

D (Update the VPC route table to route S3 traffic to an S3 access point): Route tables route traffic to VPC endpoints, not to S3 access points. Access points are used in bucket policies and requests, not routing.

upvoted 2 times

 **Kaps443** 6 months, 1 week ago

Selected Answer: AE

A: Enables secure private S3 access using Gateway Endpoint

E: Bucket policy enforces access only via secure access point

upvoted 2 times

 **sergza888** 7 months, 2 weeks ago

Selected Answer: AC

The question is really about network policies instead of object policies assuming that is already being in place that is reason i am favoring C

upvoted 1 times

 **Deztroyer88** 9 months, 3 weeks ago

Selected Answer: AE

A gateway VPC endpoint allows EC2 instances to access S3 privately without using the public internet.

E. The S3 bucket policy ensures that only authorized access via the S3 access point is permitted.

B is wrong because S3 Access Points are tied to the bucket's AWS account, not the requester's AWS account.

The access point should be created in the same AWS account as the S3 data lake, not in the data scientists' account.

upvoted 3 times

 **Spike2020** 1 year ago

Selected Answer: AE

A: Gateway VPC endpoints provide secure access to S3 without requiring internet access. Can be used in a multi-account setting.
 E: Bucket policies can restrict access to specific VPC endpoints.
 Not B: While S3 access points can be useful, they're not necessary in this scenario where the primary requirement is network-level access control.

upvoted 4 times

AzureDP900 1 year, 1 month ago

B: Creating an S3 access point in the data scientists' AWS account provides a secure and controlled way to expose the data lake to EC2 instances. The access point allows you to manage who can access the bucket, and you can configure the bucket policy to include conditions that restrict access.

E: Adding an S3 bucket policy with a condition that allows the s3:GetObject action when the value for the s3:DataAccessPointArn condition key is a valid access point ARN provides additional security and control over who can access the data lake. This ensures that only authorized networks (in this case, the data scientists' AWS account) can access the bucket.

upvoted 3 times

doobc 1 year, 1 month ago

BE. <https://aws.amazon.com/blogs/storage/setting-up-cross-account-amazon-s3-access-with-s3-access-points/>

upvoted 2 times

sam2ng 1 year, 1 month ago

I feel the combination of A,B and E would be the correct answer

upvoted 2 times

kgp0j 1 year, 3 months ago

This question is really bad.

It feels like if A is selected, then E needs to be adjusted to enable access between VPC endpoints and the bucket directly

Or if B is selected, then B needs to be reworded to say creating access point in data lake account, then E would be valid without any modification

upvoted 4 times

eboehm 2 weeks ago

or your just wrong

Cross-account access point

Consumer account (data scientists' account) creates the access point

The access point references a bucket in another account (the data lake account)

The bucket owner must explicitly allow that access point ARN in the bucket policy

AWS documents this explicitly under "Using S3 access points across AWS accounts"

upvoted 1 times

backbencher2022 1 year, 4 months ago**Selected Answer: BE**

B & E are correct options. A isn't correct because gateway VPC endpoint doesn't work outside of VPC. In this question, we are talking about 2 different accounts which implies 2 different VPCs as well

upvoted 4 times

kgp0j 1 year, 4 months ago**Selected Answer: AE**

S3 Access Point should be created in destination account.

You need VPC endpoint to keep the network private.

This question might just assumed that the S3 access point is already created in destination account

upvoted 4 times

zolthar_z 1 year, 4 months ago**Selected Answer: BE**

S3 access point is used If you want to share your bucket with other accounts

upvoted 3 times

paultantony 1 year, 3 months ago

You can also create a cross-account access point that's associated with a bucket in another AWS account, as long as you know the bucket name and the bucket owner's account ID. However, creating cross-account access points doesn't grant you access to data in the bucket until you are granted permissions from the bucket owner. The bucket owner must grant the access point owner's account (your account) access to the bucket through the bucket policy. For more information, see Granting permissions for cross-account access points.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/create-access-points.html>

upvoted 1 times

✉  **dzidis** 1 year, 5 months ago

Selected Answer: BE

Gateway endpoint do not work cross account, so BE. 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, which is available for an additional cost.
<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

upvoted 3 times

✉  **RotterDam** 1 year, 5 months ago

Selected Answer: BE

Anyone who is picking A/E - please realize DataAccessPointArn ONLY WORKS when there is an access point created. A does NOT mention creating an Access Point. B is completely possible and combine with E restricts all traffic coming from the VPC that has the access point mentioned in B.

B+E is the correct answer

upvoted 3 times

✉  **kgpoj** 1 year, 4 months ago

B is completely wrong because the access point is created in the wrong account.

You need the access point to be created in the source s3 bucket account

upvoted 2 times

✉  **hanson1028** 1 year, 4 months ago

I just try it. You can create a cross-account s3 access point

upvoted 1 times

✉  **luuthang2011** 1 year, 5 months ago

a,d gateway VPC endpoint needs config route table

upvoted 1 times

✉  **vip2** 1 year, 5 months ago

Selected Answer: AE

A, E are correct

upvoted 2 times

Question #528

Topic 1

A company wants to migrate its website to AWS. The website uses containers that are deployed in an on-premises, self-managed Kubernetes cluster. All data for the website is stored in an on-premises PostgreSQL database.

The company has decided to migrate the on-premises Kubernetes cluster to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster will use EKS managed node groups with a static number of nodes. The company will also migrate the on-premises database to an Amazon RDS for PostgreSQL database.

A solutions architect needs to estimate the total cost of ownership (TCO) for this workload before the migration.

Which solution will provide the required TCO information?

- A. Request access to Migration Evaluator. Run the Migration Evaluator Collector and import the data. Configure a scenario. Export a Quick Insights report from Migration Evaluator.
- B. Launch AWS Database Migration Service (AWS DMS) for the on-premises database. Generate an assessment report. Create an estimate in AWS Pricing Calculator for the costs of the EKS migration.
- C. Initialize AWS Application Migration Service. Add the on-premises servers as source servers. Launch a test instance. Output a TCO report from Application Migration Service.
- D. Access the AWS Cloud Economics Center webpage to assess the AWS Cloud Value Framework. Create an AWS Cost and Usage report from the Cloud Value Framework.

Correct Answer: A

Community vote distribution

A (91%)	9%
---------	----

 **AzureDP900** 1 year, 1 month ago

A

Migration Evaluator is a tool provided by AWS that helps estimate the costs of migrating an on-premises workload to AWS, including both the migration cost and the estimated TCO (Total Cost of Ownership) for the new AWS resources.

By using Migration Evaluator, the solutions architect can:

Import data about the existing on-premises Kubernetes cluster and PostgreSQL database.

Configure a scenario that accurately reflects the planned migration to Amazon EKS and Amazon RDS.

Export a Quick Insights report that provides an estimate of the TCO for the migrated workload.

upvoted 2 times

 **kgpoj** 1 year, 4 months ago

Selected Answer: A

Quick catch: when you see TCO, think about Migration Evaluator

upvoted 4 times

 **Chakanetsa** 1 year, 5 months ago

Selected Answer: A

Best Answer: A. Request access to Migration Evaluator. Run the Migration Evaluator Collector and import the data. Configure a scenario. Export a Quick Insights report from Migration Evaluator.

Reasoning:

Comprehensive TCO Analysis: Migration Evaluator is specifically designed to assess migration projects and provides detailed cost estimates.

Accurate Data: By collecting data from the on-premises environment, Migration Evaluator can generate more accurate cost estimates.

Scenario Modeling: The ability to configure scenarios allows for testing different migration options and their associated costs.

Quick Insights Report: This provides a summarized overview of the potential TCO.

upvoted 3 times

 **vip2** 1 year, 5 months ago

Selected Answer: A

B:Estimate AWS service costs

A: Assess current environment and plan migration to AWS

upvoted 1 times

 **mark_232323** 1 year, 5 months ago

Selected Answer: A

Option B is incorrect because AWS Database Migration Service (AWS DMS) is used for migrating databases, not for estimating the TCO.

Additionally, the AWS Pricing Calculator alone cannot provide a comprehensive TCO analysis for a complex migration scenario involving

Kubernetes and databases.

Option C is incorrect because AWS Application Migration Service is primarily used for migrating and modernizing applications, not for estimating the TCO of a migration.

upvoted 2 times

 **Moumita** 1 year, 5 months ago

Selected Answer: B

Option B (AWS DMS assessment + AWS Pricing Calculator) is typically more appropriate and practical.

upvoted 1 times

 **Moumita** 1 year, 5 months ago

<https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/aws-pricingtco-tools.html>

upvoted 1 times

 **kupo777** 1 year, 5 months ago

A

Migration Evaluator is used to estimate TCO.

upvoted 3 times

Question #529

Topic 1

An events company runs a ticketing platform on AWS. The company's customers configure and schedule their events on the platform. The events result in large increases of traffic to the platform. The company knows the date and time of each customer's events.

The company runs the platform on an Amazon Elastic Container Service (Amazon ECS) cluster. The ECS cluster consists of Amazon EC2 On-Demand Instances that are in an Auto Scaling group. The Auto Scaling group uses a predictive scaling policy.

The ECS cluster makes frequent requests to an Amazon S3 bucket to download ticket assets. The ECS cluster and the S3 bucket are in the same AWS Region and the same AWS account. Traffic between the ECS cluster and the S3 bucket flows across a NAT gateway.

The company needs to optimize the cost of the platform without decreasing the platform's availability.

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

- A. Create a gateway VPC endpoint for the S3 bucket.
- B. Add another ECS capacity provider that uses an Auto Scaling group of Spot Instances. Configure the new capacity provider strategy to have the same weight as the existing capacity provider strategy.
- C. Create On-Demand Capacity Reservations for the applicable instance type for the time period of the scheduled scaling policies.
- D. Enable S3 Transfer Acceleration on the S3 bucket.
- E. Replace the predictive scaling policy with scheduled scaling policies for the scheduled events.

Correct Answer: AE*Community vote distribution*

AE (92%)

8%

 **0b43291** Highly Voted  1 year, 1 month ago

If you made it this far you will pass.. Good luck everyone! This is a great service.
upvoted 15 times

 **marchelok** 6 months, 2 weeks ago

For sure, I'm reviewing the material again for the recertification ;)
upvoted 2 times

 **wbedair** Highly Voted  1 year, 6 months ago

Selected Answer: AE

Options A and E will meet the requirements most cost-effectively by leveraging the predictability of the workload of known customer events to optimize scaling operations and reducing data transfer costs
upvoted 5 times

 **itsjunukim** Most Recent  9 months, 1 week ago

Selected Answer: AE

Tomorrow is the exam. To everyone who has made it this far, good luck and do your best!
upvoted 3 times

 **AzureDP900** 1 year, 1 month ago

A,E
By creating a gateway VPC endpoint for the S3 bucket (option A), you can reduce latency and improve performance by routing traffic directly through Amazon's network, rather than relying on the NAT gateway.

And by replacing the predictive scaling policy with scheduled scaling policies for the scheduled events (option E), you can avoid scaling instances during low-traffic periods, which would reduce costs and prevent unnecessary charges.

upvoted 1 times

 **Chakanetsa** 1 year, 3 months ago

Selected Answer: AB

- A. Create a gateway VPC endpoint for the S3 bucket: This will allow the ECS cluster to access the S3 bucket directly without the need for traffic to flow through the NAT gateway, reducing costs associated with NAT data transfer.
- B. Add another ECS capacity provider that uses an Auto Scaling group of Spot Instances: By introducing Spot Instances with the same weight as On-Demand Instances, the company can take advantage of the cost savings from Spot Instances while maintaining the ability to scale with On-Demand Instances when needed.

These steps will reduce network traffic costs and take advantage of lower-cost compute options without compromising platform availability.

upvoted 1 times

 **c22ddd8** 1 year, 5 months ago

Selected Answer: AE

Since it is scheduled event , E is correct ans

upvoted 2 times

 **vip2** 1 year, 5 months ago

Selected Answer: AE

A: no charge for S3 access

E: know details of date and time --- can scheduled for saving cost

upvoted 2 times

 **kupo777** 1 year, 5 months ago

A

For S3 communication in the same region, the communication fee is waived by using the gateway VPC endpoint.

B

Availability is reduced when spot instances are used.

C

Using on-demand capacity reservation increases costs.

D

Using S3 Transfer Acceleration increases costs.

E

Scheduled scaling policies allow resources to be used according to events.

The answers are A and E.

upvoted 3 times

Browse atleast 50% to increase passing rate 



Viewing page 1 out of 1 pages.

Viewing questions 1-529 out of 529 questions