



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

Custom View Settings

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

A company collects data for temperature, humidity, and atmospheric pressure in cities across multiple continents. The average volume of data that the company collects from each site daily is 500 GB. Each site has a high-speed Internet connection.

The company wants to aggregate the data from all these global sites as quickly as possible in a single Amazon S3 bucket. The solution must minimize operational complexity.

Which solution meets these requirements?

- A. Turn on S3 Transfer Acceleration on the destination S3 bucket. Use multipart uploads to directly upload site data to the destination S3 bucket.
- B. Upload the data from each site to an S3 bucket in the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket. Then remove the data from the origin S3 bucket.
- C. Schedule AWS Snowball Edge Storage Optimized device jobs daily to transfer data from each site to the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket.
- D. Upload the data from each site to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. At regular intervals, take an EBS snapshot and copy it to the Region that contains the destination S3 bucket. Restore the EBS volume in that Region.

Correct Answer: A*Community vote distribution*

[Removed] 3 months, 3 weeks ago

Last week i passed my exam with our dumps. Pass4surexams provide 100% valid and correct answers
upvoted 189 times

chelsealove 3 months, 3 weeks ago

Most of the questions were answered here. Thank you very much for making this easy for me.
upvoted 3 times

dijodot417 3 months, 3 weeks ago

Really thanks for your suggestion. I am glad that I selected this lab source and get 92%. I would recommend it a 100%
upvoted 43 times

walkerrrrr 3 months, 3 weeks ago

pdf is so accurate
upvoted 1 times

walkerrrrr 3 months, 3 weeks ago

Thank you I took SAA exam on 12/05/2023 and passed.
upvoted 2 times

chelsealove 3 months, 3 weeks ago

I just finished my exam and I passed, 929 out of 1000.
upvoted 2 times

D2w 1 year, 5 months ago

Selected Answer: A

S3 Transfer Acceleration is the best solution cz it's faster , good for high speed, Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets.

upvoted 60 times

BoboChow 1 year, 5 months ago

I thought S3 Transfer Acceleration is based on Cross Region Replication, I made a mistake.
upvoted 1 times

Blest012 8 months, 2 weeks ago

Correct the S3 Transfer Acceleration service is the best for this scenario
upvoted 1 times

ManikRoy 13 hours, 50 minutes ago

Selected Answer: A

Agree with option A. Using S3 Transfer acceleration together with multipart upload is the best option here considering that the site has a high speed internet connection and the solution must minimize operational complexity.

upvoted 1 times

 **48cd959** 1 week, 4 days ago

Answer - A, Just use S3 Transfer accelerator and use Multipart upload.

upvoted 1 times

 **JavierEF** 1 week, 5 days ago

Selected Answer: A

B and D are much more complex than needed. C is not right because, since there is a high-speed Internet in each location, Snow devices are not required.

upvoted 1 times

 **developer_404** 1 week, 5 days ago

Selected Answer: A

- A. No operational overhead and it can use edge locations to fast transfer. This is right answer.
- B. Uploading to different S3 bucket and enabling cross region replication is an operation overhead and this can be easily achieved by transfer accelerator.
- C. AWS Snowball is a physical device to be used for transfer which is not the requirement here.
- D. EBS volume is a traditional way of doing it and its operational overhead.

upvoted 1 times

 **xBUGx** 1 month ago

A is right

upvoted 1 times

 **tsr_01** 1 month, 3 weeks ago

Selected Answer: A

Passed on 1/30/2024, dump is still valid. About 70% of the questions on the exam were from here. Memorizing the questions alone is not enough though — reading through the discussions was absolutely crucial and helped me figure out most of the new questions that weren't covered in this dump

upvoted 3 times

 **atrickmapuranga** 2 months, 1 week ago

Selected Answer: A

The best solution

upvoted 2 times

 **atrickmapuranga** 2 months, 1 week ago

A is the Answer

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: A

correct answer-A

upvoted 1 times

 **Andreshere** 2 months, 2 weeks ago

A. Despite this option can be valid, it implies a bit of operational overhead compared with other options. Additionally, there is no need to aggregate that change to the existing architecture because we are already working in S3, and using other storage services incurs unnecessary costs.

B. To collect the logs, we use CloudTrail over CloudWatch. Running SQL queries from the Amazon CloudWatch console is not recommended for this use case, since it is more used for filtering.

C. Athena integrates seamlessly with S3 and allows you to run simple SQL queries in no time. When working with Apache Spark or with SQL in S3, using this service is the best option.

D. This option incurs elevated operational overhead. Glue is not used to catalog the logs. Analyzing logs with Spark on an EMR cluster is very common, but you can do it faster with the Athena service integrated with S3 directly.

upvoted 1 times

 **vip2** 2 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html>

<https://docs.aws.amazon.com/snowball/latest/developer-guide/whatisedge.html>

upvoted 3 times

 **thewalker** 2 months, 3 weeks ago

Selected Answer: A

B: Cross region replication attracts extra costs to transfer data across regions. No need to choose this option as each site is having high speed connection.

C. No need to go for device transfers as each site is having high speed connection.

D. Not a good solution to use EBS volumes as we can transfer the data directly to S3.
A is the best answer, especially going with multi-part upload, transferring the data to the destination bucket using transfer accelerator.
upvoted 2 times

 **NY4u** 2 months, 3 weeks ago

Please if you have the pdf or how to have access to practise the dumps, can you share with me damsey2022@gmail.com. Thanks in advance
I have the exam in few days.

upvoted 1 times

 **nampt19** 2 months, 3 weeks ago

Could someone please help with the PDF. Kindly send to namakainu@gmail.com. Thanks in advance.

upvoted 1 times

 **daejii** 2 months, 3 weeks ago

Could someone please help with the PDF. Kindly send to cybernords@protonmail.com. Thanks in advance.

upvoted 1 times

Question #2

Topic 1

A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket. Queries will be simple and will run on-demand. A solutions architect needs to perform the analysis with minimal changes to the existing architecture.

What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed.
- B. Use Amazon CloudWatch Logs to store the logs. Run SQL queries as needed from the Amazon CloudWatch console.
- C. Use Amazon Athena directly with Amazon S3 to run the queries as needed.
- D. Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed.

Correct Answer: C

Community vote distribution

C (100%)

✉  **airraid2010**  1 year, 5 months ago

Answer: C

<https://docs.aws.amazon.com/athena/latest/ug/what-is.html>

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds.

upvoted 51 times

✉  **BoboChow** 1 year, 5 months ago

I agree C is the answer

upvoted 2 times

✉  **tt79** 1 year, 5 months ago

C is right.

upvoted 1 times

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

Selected Answer: C

Keyword:

- Queries will be simple and will run on-demand.
- Minimal changes to the existing architecture.

A: Incorrect - We have to do 2 step. load all content to Redshift and run SQL query (This is simple query so we can use Athena, for complex query we will apply Redshift)

B: Incorrect - Our query will be run on-demand so we don't need to use CloudWatch Logs to store the logs.

C: Correct - This is simple query we can apply Athena directly on S3

D: Incorrect - This take 2 step: use AWS Glue to catalog the logs and use Spark to run SQL query

upvoted 33 times

✉  **48cd959**  1 week, 4 days ago

Answer should be C, Simple approach, Store logs in S3 and use Athena to query. Redshift will be costly approach. Cloudwatch does not store any data. So A and B ruled out.

upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

Selected Answer: C

S3 + Athena is simple approach

upvoted 1 times

✉  **A_jaa** 2 months, 1 week ago

Selected Answer: C

C seems right.

upvoted 1 times

✉  **Andreshere** 2 months, 2 weeks ago

- A. Despite this option can be valid, it implies a bit of operational overhead compared with other options. Additionally, there is no need to aggregate that change to the existing architecture because we are already working in S3, and using other storage services incurs unnecessary costs.
- B. To collect the logs, we use CloudTrail over CloudWatch. Running SQL queries from the Amazon CloudWatch console is not recommended for this use case, since it is more used for filtering.
- C. Correct answer. Athena integrates seamlessly with S3 and allows you to run simple SQL queries in no time. When working with Apache Spark or with SQL in S3, using this service is the best option.

D. This option incurs elevated operational overhead. Glue is not used to catalog the logs. Analyzing logs with Spark on an EMR cluster is very common, but you can do it faster with the Athena service integrated with S3 directly.

upvoted 3 times

andreadhelpra 2 months, 2 weeks ago

Selected Answer: C

Amazon Athena, because it provides the easiest way to run simple SQL service on a on-demand basis on an S3 bucket. The data is not complex so Redshift and EMR are a overhead or simply not suitable. CloudWatch does not have a console where you can run queries.

upvoted 3 times

RobertLi 3 months, 1 week ago

Appreciate if any friend can send the pdf version to my personal email: mroracle99@gmail.com. Thanks so much!

upvoted 1 times

karolmrozik 3 months, 2 weeks ago

Selected Answer: C

C seems to be fine

upvoted 1 times

Genlor 4 months ago

Selected Answer: C

No need to build a server and it is on the fly

upvoted 1 times

Ruffyit 4 months, 1 week ago

<https://docs.aws.amazon.com/athena/latest/ug/what-is.html>

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds.

upvoted 1 times

Ruffyit 5 months ago

C.

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. No operational overhead

upvoted 1 times

[Removed] 5 months ago

Selected Answer: C

General line: analyse the log files

Conditions: queries is simple and run on-demand

Task: perform the analysis

Requirements: minimal changes to the existing architecture, LEAST amount of operational overhead

Correct answer: C. Amazon Athena because:

- analytics service provides a simplified, flexible way to analyze data
- Use cases: run queries on S3, on premises, or on other clouds; prepare data for ML models; build distributed big data reconciliation engines, perform multicloud analytics

A - about analytics but more "hardcore"/ work with data warehousing

B - about collecting and monitoring. If you want to analyse some logs in this area you should use CloudWatch Logs Insights

D - about analytics but more 'hardcore'/ work with different data from all resources

upvoted 4 times

[Removed] 5 months, 1 week ago

Selected Answer: C

C. Use Amazon Athena directly with Amazon S3 to run the queries as needed.

upvoted 1 times

pedrogaf 5 months, 2 weeks ago

Selected Answer: C

Simple and fast

upvoted 1 times

Abitek007 5 months, 3 weeks ago

serverless operation simply

upvoted 1 times

thanhnv 7 months ago

Selected Answer: C

Keyword:

- needs to perform the analysis with minimal changes to the existing architecture.
- LEAST amount of operational overhead.

C

upvoted 1 times

Question #3

Topic 1

A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.
- B. Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.
- C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.
- D. Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.

Correct Answer: A*Community vote distribution*

ude Highly Voted 1 year, 5 months ago

Selected Answer: A

aws:PrincipalOrgID Validates if the principal accessing the resource belongs to an account in your organization.

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/>

upvoted 60 times

BoboChow 1 year, 5 months ago

the condition key aws:PrincipalOrgID can prevent the members who don't belong to your organization to access the resource

upvoted 17 times

Naneyerokey Highly Voted 1 year, 4 months ago

Selected Answer: A

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

Condition keys: AWS provides condition keys that you can query to provide more granular control over certain actions. The following condition keys are especially useful with AWS Organizations:

aws:PrincipalOrgID – Simplifies specifying the Principal element in a resource-based policy. This global key provides an alternative to listing all the account IDs for all AWS accounts in an organization. Instead of listing all of the accounts that are members of an organization, you can specify the organization ID in the Condition element.

aws:PrincipalOrgPaths – Use this condition key to match members of a specific organization root, an OU, or its children. The aws:PrincipalOrgPaths condition key returns true when the principal (root user, IAM user, or role) making the request is in the specified organization path. A path is a text representation of the structure of an AWS Organizations entity.

upvoted 17 times

Sleepy_Lazy_Coder 7 months, 2 weeks ago

are we not choosing ou because the least overhead term was use? option B also seems correct

upvoted 3 times

BlackMamba_4 7 months ago

Exactly

upvoted 1 times

awsgeek75 Most Recent 2 months, 1 week ago

Selected Answer: A

PrincipalOrgID global condition is simple way to limit access

BCD even if possible is too much work

upvoted 1 times

A_jaa 2 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

Andreshere 2 months, 2 weeks ago

Selected Answer: A

A. Correct answer. Bucket policy controls who can access to S3 and their objects. If we refer in the bucket policy to the organization, we can limit who can access inside that organization.

B. Despite this option is correct, it is unnecessarily complex. We don't need to separate the AWS Organization users for the requirements imposed

in the question. So, it only aggregates more operational overhead.

C. Using CloudTrail for controlling the S3 access permissions is not suitable and require so many events to be monitored. Additionally, it only registers the logs, so CloudTrail cannot impose restrictions over the accounts that access to S3.

D. Tagging each user is not an scalable or efficient solution since you need to tag every user in the infrastructure, which is probably not static. Additionally, it makes unnecessary verbose the S3 bucket policy associated to that bucket.

upvoted 2 times

 **Ruffyit** 4 months, 1 week ago

AWS Identity and Access Management (IAM) now makes it easier for you to control access to your AWS resources by using the AWS organization of IAM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, aws:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account (including the master account) in the organization.

upvoted 4 times

 **Ruffyit** 5 months ago

Answer: A

upvoted 1 times

 **[Removed]** 5 months, 1 week ago

Selected Answer: A

Add the aws PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy

upvoted 1 times

 **Guru4Cloud** 8 months, 1 week ago

Selected Answer: A

This is the least operationally overhead solution because it does not require any additional infrastructure or configuration. AWS Organizations already tracks the organization ID of each account, so you can simply add the aws:PrincipalOrgID condition key to the S3 bucket policy and reference the organization ID. This will ensure that only users of accounts within the organization can access the S3 bucket

upvoted 5 times

 **james2033** 8 months, 2 weeks ago

Selected Answer: A

See video "Ensure identities and networks can only be used to access trusted resources" at <https://youtu.be/cWVW0xAiWwc?t=677> at 11:17 use "aws:PrincipalOrgId": "o-fr75jjs531".

upvoted 3 times

 **miki111** 8 months, 2 weeks ago

Option A MET THE REQUIREMENT

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: A

Option A, which suggests adding the aws PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy, is a valid solution to limit access to the S3 bucket to users within the organization in AWS Organizations. It can effectively achieve the desired access control.

It restricts access to the S3 bucket based on the organization ID, ensuring that only users within the organization can access the bucket. This method is suitable if you want to restrict access at the organization level rather than individual departments or organizational units.

The operational overhead for Option A is also relatively low since it involves adding a global condition key to the S3 bucket policy. However, it is important to note that the organization ID must be accurately configured in the bucket policy to ensure the desired access control is enforced.

In summary, Option A is a valid solution with minimal operational overhead that can limit access to the S3 bucket to users within the organization using the aws PrincipalOrgID global condition key.

upvoted 1 times

 **karloscetina007** 9 months, 1 week ago

A is the correct answer.

upvoted 1 times

 **Musti35** 11 months, 2 weeks ago

You can now use the aws:PrincipalOrgID condition key in your resource-based policies to more easily restrict access to IAM principals from accounts in your AWS organization. For more information about this global condition key and policy examples using aws:PrincipalOrgID, read the IAM documentation.

upvoted 1 times

 **PhucVuu** 11 months, 3 weeks ago

Selected Answer: A

Keywords:

- Company uses AWS Organizations
- Limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations
- LEAST amount of operational overhead

A: Correct - We just add PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy

B: Incorrect - We can limit access by this way but this will take more amount of operational overhead

C: Incorrect - AWS CloudTrail only log API events, we can not prevent user access to S3 bucket. For update S3 bucket policy to make it work you

should manually add each account -> this way will not be cover in case of new user is added to Organization.

D: Incorrect - We can limit access by this way but this will take most amount of operational overhead

upvoted 11 times

 **linux_admin** 12 months ago

Selected Answer: A

Option A proposes adding the aws PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy. This would limit access to the S3 bucket to only users of accounts within the organization in AWS Organizations, as the aws PrincipalOrgID condition key can check if the request is coming from within the organization.

upvoted 2 times

 **martin451** 1 year ago

B. Create an organizational unit (OU) for each department. Add the AWS: Principal Org Paths global condition key to the S3 bucket policy. This solution allows for the S3 bucket to only be accessed by users within the organization in AWS Organizations while minimizing operational overhead by organizing users into OUs and using a single global condition key in the bucket policy. Option A, adding the Principal ID global condition key, would require frequent updates to the policy as new users are added or removed from the organization. Option C, using CloudTrail to monitor events, would require manual updating of the policy based on the events. Option D, tagging each user, would also require manual tagging updates and may not be scalable for larger organizations with many users.

upvoted 1 times

Question #4

Topic 1

An application runs on an Amazon EC2 instance in a VPC. The application processes logs that are stored in an Amazon S3 bucket. The EC2 instance needs to access the S3 bucket without connectivity to the internet.

Which solution will provide private network connectivity to Amazon S3?

- A. Create a gateway VPC endpoint to the S3 bucket.
- B. Stream the logs to Amazon CloudWatch Logs. Export the logs to the S3 bucket.
- C. Create an instance profile on Amazon EC2 to allow S3 access.
- D. Create an Amazon API Gateway API with a private link to access the S3 endpoint.

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

Keywords:

- EC2 in VPC
- EC2 instance needs to access the S3 bucket without connectivity to the internet

A: Correct - Gateway VPC endpoint can connect to S3 bucket privately without additional cost

B: Incorrect - You can set up interface VPC endpoint for CloudWatch Logs for private network from EC2 to CloudWatch. But from CloudWatch to S3 bucket: Log data can take up to 12 hours to become available for export and the requirement only need EC2 to S3

C: Incorrect - Create an instance profile just grant access but not help EC2 connect to S3 privately

D: Incorrect - API Gateway like the proxy which receive network from out site and it forward request to AWS Lambda, Amazon EC2, Elastic Load Balancing products such as Application Load Balancers or Classic Load Balancers, Amazon DynamoDB, Amazon Kinesis, or any publicly available HTTPS-based endpoint. But not S3

upvoted 39 times

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

Thank you so much

upvoted 1 times

✉️  **D2w**  1 year, 5 months ago

Selected Answer: A

VPC endpoint allows you to connect to AWS services using a private network instead of using the public Internet

upvoted 30 times

✉️  **48cd959**  1 week, 4 days ago

Answer -A

VPC endpoints are created to access any AWS services privately without going to internet.

upvoted 1 times

✉️  **TilTil** 1 week, 5 days ago

Selected Answer: A

VPC Endpoint is the TOP Notch choice, allows services to connect via private could. VPC literally means virtual private cloud. Best choice

upvoted 1 times

✉️  **Idruizsan** 1 month, 1 week ago

Selected Answer: A

Easiest way to avoid internet traffic is to use VPC endpoints to let services communicate with each other

upvoted 2 times

✉️  **awsgeek75** 2 months, 1 week ago

Selected Answer: A

gateway VPC to S3 ensures data stays within AWS

upvoted 1 times

✉️  **A_jaa** 2 months, 1 week ago

Selected Answer: A

Answer-A

upvoted 1 times

✉️  **Andreshere** 2 months, 2 weeks ago

Selected Answer: A

- A. Correct answer. The easiest way to get private network connectivity in S3 is using VPC gateway endpoint. This service is free, and it is integrated natively with S3.
 B. Amazon CloudWatch Logs only collects and monitors logs but natively has not mechanisms to use private connection.
 C. Instance profiles are used to assign IAM roles to an EC2 instance, but it is not related to network connectivity.
 D. API Gateway like the proxy which receive network from out site and it forward request to AWS Lambda, Amazon EC2, Elastic Load Balancing products such as Application Load Balancers or Classic Load Balancers, Amazon DynamoDB, Amazon Kinesis, or any publicly available HTTPS-based endpoint. But not S3.

upvoted 5 times

 **reynol** 3 months, 2 weeks ago

thank you

upvoted 1 times

 **Ruffyit** 4 months, 1 week ago

VPC endpoint allows you to connect to AWS services using a private network instead of using the public Internet

upvoted 1 times

 **Ruffyit** 5 months ago

Keywords:

- EC2 in VPC
- EC2 instance needs to access the S3 bucket without connectivity to the internet

VPC endpoint allows you to connect to AWS services using a private network instead of using the public Internet.

With a gateway endpoint, you can access Amazon S3 from your VPC, without requiring an internet gateway or NAT device for your VPC, and with no additional cost. However, gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway.

Ref. <https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html>

upvoted 3 times

 **[Removed]** 5 months, 1 week ago

Selected Answer: A

Create a gateway VPC endpoint to the S3 bucket

upvoted 1 times

 **namtp** 5 months, 2 weeks ago

Selected Answer: A

Create VPC endpoint is a private way to connect to AWS services without internet.

upvoted 1 times

 **RNess** 6 months, 3 weeks ago

Selected Answer: A

VPC endpoint is the best way to connect in private

upvoted 1 times

 **Bmarodi** 7 months, 1 week ago

Selected Answer: A

With a gateway endpoint, you can access Amazon S3 from your VPC, without requiring an internet gateway or NAT device for your VPC, and with no additional cost. However, gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway.

Ref. <https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html>

upvoted 1 times

 **TariqKipkemei** 8 months ago

Selected Answer: A

A VPC endpoint enables customers to privately connect to supported AWS services and VPC endpoint services powered by AWS PrivateLink.

<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/what-are-vpc-endpoints.html#:~:text=A-,VPC%20endpoint,-enables%20customers%20to>

upvoted 2 times

 **Guru4Cloud** 8 months, 1 week ago

Selected Answer: A

The answer is A. Create a gateway VPC endpoint to the S3 bucket.

A gateway VPC endpoint is a private way to connect to AWS services without using the internet. This is the best solution for the given scenario because it will allow the EC2 instance to access the S3 bucket without any internet connectivity

upvoted 1 times

Question #5

Topic 1

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that, each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.

What should a solutions architect propose to ensure users see all of their documents at once?

- A. Copy the data so both EBS volumes contain all the documents
- B. Configure the Application Load Balancer to direct a user to the server with the documents
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server

Correct Answer: C

Community vote distribution

C (98%)

✉️ **D2w** 1 year, 5 months ago

Selected Answer: C

Concurrent or at the same time key word for EFS

upvoted 39 times

✉️ **mikey2000** 1 year, 4 months ago

Ebs doesn't support cross az only reside in one Az but Efs does, that why it's c

upvoted 27 times

✉️ **pbpally** 10 months, 3 weeks ago

And just for clarification to others, you can have COPIES of the same EBS volume in one AZ and in another via EBS Snapshots, but don't confuse that with the idea of having some sort of global capability that has concurrent copying mechanisms.

upvoted 7 times

✉️ **TilTil** 1 week, 5 days ago

Selected Answer: C

The alternative is to use Aurora or DynamoDB with master-slave replication, otherwise EFS is the most logical.

upvoted 1 times

✉️ **TheFivePips** 1 month, 1 week ago

Selected Answer: C

EBS volumes must be in the same AZ as the instances they are attached to. So you cannot share an EBS across AZs. Unless you plan to have two separate volumes in each AZ, the simplest solution is to use EFS as a shared file system that can be used across both AZs

upvoted 3 times

✉️ **sidharthwader** 1 month, 1 week ago

Correct EBS can be used for one Az if you need a solution which could be accessed across a AZ then go for File storage which is a regional service

upvoted 1 times

✉️ **Idruizsan** 1 month, 1 week ago

Selected Answer: C

If the idea is to keep documents in different places, then the only solution here is a file sharing system, EFS in this case

upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

Selected Answer: C

ABD are not even possible without further details
C is EFS which is shared volume.

upvoted 1 times

✉️ **A_jaa** 2 months, 1 week ago

Selected Answer: C

Answer-c

upvoted 1 times

✉️ **adamslee** 3 months ago

EBS can exist only one AZ. so C

upvoted 2 times

 **wyejay** 3 months ago

Selected Answer: C

Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS: Amazon Elastic File System (EFS) provides a simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. It is designed to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as files are added and removed. By moving the documents to EFS, both EC2 instances can access all the documents at the same time, resolving the issue.

upvoted 2 times

 **Ruffyit** 4 months, 1 week ago

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#efs-regional-ec2>

upvoted 1 times

 **Hayden001** 4 months, 2 weeks ago

Proposed = new service = EFS

upvoted 1 times

 **Ruffyit** 5 months ago

Keyword "stores user-uploaded documents". Two EC2 instances behind Application Load Balancer. See <https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#efs-regional-ec2>. In the diagram, Per Amazon EC2 in a different Availability zone, and Amazon Elastic File System support this case.

upvoted 1 times

 **[Removed]** 5 months, 1 week ago

Selected Answer: C

Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS

upvoted 1 times

 **bnagaraja9099** 5 months, 1 week ago

C is correct

upvoted 1 times

 **mattuyghur** 5 months, 2 weeks ago

Selected Answer: D

Option C (copying data to Amazon EFS and modifying the application) is a valid alternative, but it may require more changes to the application code and data migration to EFS. This option is suitable when you want to centralize shared data storage.

In summary, option D is the most straightforward and scalable solution to ensure that users can access all of their documents when using multiple EC2 instances behind an Application Load Balancer.

upvoted 2 times

 **0xE8D4A51000** 3 months, 4 weeks ago

No. The point of an LB to achieve scalability is to send DIFFERENT requests to different instances of the service NOT the SAME request to different services. That doesn't scale well.

upvoted 1 times

 **RNess** 6 months, 3 weeks ago

Selected Answer: C

EFS is to muliple AZ

upvoted 1 times

 **TariqKipkemei** 8 months ago

Selected Answer: C

Shared file storage = EFS

upvoted 1 times

Question #6

Topic 1

A company uses NFS to store large video files in on-premises network attached storage. Each video file ranges in size from 1 MB to 500 GB. The total storage is 70 TB and is no longer growing. The company decides to migrate the video files to Amazon S3. The company must migrate the video files as soon as possible while using the least possible network bandwidth.

Which solution will meet these requirements?

- A. Create an S3 bucket. Create an IAM role that has permissions to write to the S3 bucket. Use the AWS CLI to copy all files locally to the S3 bucket.
- B. Create an AWS Snowball Edge job. Receive a Snowball Edge device on premises. Use the Snowball Edge client to transfer data to the device. Return the device so that AWS can import the data into Amazon S3.
- C. Deploy an S3 File Gateway on premises. Create a public service endpoint to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.
- D. Set up an AWS Direct Connect connection between the on-premises network and AWS. Deploy an S3 File Gateway on premises. Create a public virtual interface (VIF) to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.

Correct Answer: C

Community vote distribution

B (84%)

Other

 **Gatt**  1 year, 5 months ago

Selected Answer: B

Let's analyse this:

B. On a Snowball Edge device you can copy files with a speed of up to 100Gbps. 70TB will take around 5600 seconds, so very quickly, less than 2 hours. The downside is that it'll take between 4-6 working days to receive the device and then another 2-3 working days to send it back and for AWS to move the data onto S3 once it reaches them. Total time: 6-9 working days. Bandwidth used: 0.

C. File Gateway uses the Internet, so maximum speed will be at most 1Gbps, so it'll take a minimum of 6.5 days and you use 70TB of Internet bandwidth.

D. You can achieve speeds of up to 10Gbps with Direct Connect. Total time 15.5 hours and you will use 70TB of bandwidth. However, what's interesting is that the question does not specify what type of bandwidth? Direct Connect does not use your Internet bandwidth, as you will have a dedicated peer to peer connectivity between your on-prem and the AWS Cloud, so technically, you're not using your "public" bandwidth.

The requirements are a bit too vague but I think that B is the most appropriate answer, although D might also be correct if the bandwidth usage refers strictly to your public connectivity.

upvoted 84 times

 **Gatt** 1 year, 4 months ago

I will add that the question does not specify if the company already has DA in place or not. If they don't have DA in place, it will take a long time (weeks) for DA connectivity to be setup. Another point for B here, as Snowball is much quicker from this perspective.

upvoted 6 times

 **pentium75** 3 months ago

It does, because option D says "SET UP a DirectConnect connection", not "use an existing DirectConnect connection".

upvoted 1 times

 **ArielSchivo** 1 year, 5 months ago

Great answers! I would say D is the correct since it's not using your public connection at all (I assume they are talking about public connection).

upvoted 1 times

 **Ello2023** 1 year, 2 months ago

You missed the first part of the question "The company must migrate the video files as soon as possible..." hence C would be the best answer.

upvoted 2 times

 **abhishek_m89** 1 year, 4 months ago

and it says, "The total storage is 70 TB and is no longer growing". Thats why it should be B.

upvoted 3 times

 **tuloveu**  1 year, 5 months ago

Selected Answer: B

As using the least possible network bandwidth.

upvoted 33 times

 **ManikRoy** Most Recent 11 hours, 36 minutes ago

Selected Answer: B

Option B as the question mentions least possible network bandwidth though receiving the snowball device and sending the data will take some time. Option D will be fastest but 70Tb bandwidth will be used.

upvoted 1 times

 **Sewass** 1 day, 16 hours ago

Selected Answer: B

keyword: no longer growing

upvoted 1 times

 **TilTil** 1 week, 5 days ago

Selected Answer: B

KWs: As soon as possible, Using least possible bandwidth. 70TB is quite a bit so bandwidth is a priority. Off the bat, I would go with a Snowball device mainly due to the sheer size of data. So snowball edge takes this.

DX is good with speeds upto 100Mbps, but loses on both time to setup and bandwidth. S3 options lose on bandwidth but are immediate to setup.

upvoted 1 times

 **Rosy92** 3 weeks, 5 days ago

Selected Answer: B

you have to use snowball in this case because you have as requirement to migrate fast and 70TB of data, so definitely B.

upvoted 1 times

 **Prosen2522** 1 month, 1 week ago

Selected Answer: B

Here are the key hints to go for option B.

1. The company wants to migrate the data as early as possible
2. Don't want to use the network bandwidth
3. Side of the data is 70 TB. AWS suggest to use Snowball Edge Device if the data is more than 10TB.

upvoted 1 times

 **Kimaru21** 1 month, 2 weeks ago

B, is the correct answer

upvoted 1 times

 **stargodwin** 1 month, 4 weeks ago

Selected Answer: B

Given the requirement to migrate the video files to Amazon S3 as soon as possible while using the least possible network bandwidth, the most suitable solution would be:

B. Create an AWS Snowball Edge job. Receive a Snowball Edge device on premises. Use the Snowball Edge client to transfer data to the device. Return the device so that AWS can import the data into Amazon S3.

This solution involves physically transferring the data using a Snowball Edge device, which can handle large volumes of data with high-speed transfers while minimizing the impact on the network. It is particularly useful when dealing with large files and a significant amount of data. Additionally, it ensures secure transfer and efficient migration to Amazon S3.

upvoted 2 times

 **quocbaodoan** 1 month, 4 weeks ago

Selected Answer: B

I selected B

upvoted 1 times

 **Mani1401** 2 months ago

The correct answer provided by exam topic is different than the most voted answer. Which one should I refer .

upvoted 1 times

 **Awsbeginner87** 3 days, 22 hours ago

Same doubt ... Which one should we take as right answer?? Its so confusing

upvoted 1 times

 **awsgEEK75** 2 months, 1 week ago

Selected Answer: B

Data isn't growing, least possible bandwidth

AC will use a lot of bandwidth even if they can be done ASAP

D: Direct connect takes long time to setup

B: Snowball Edge shipment will be physically slow but takes least amount of bandwidth

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: B

B seems right

upvoted 1 times

✉ **A_jaa** 2 months, 1 week ago

Selected Answer: C

C seems right

upvoted 1 times

✉ **Andreshere** 2 months, 2 weeks ago

Selected Answer: B

The question states that the storage is no longer growing. This implies that we don't need to make any kind of data synchronization. Additionally, the total storage is 70 TB, which is a large amount of data. This implies high transfer costs. So, we can discard A, C and D options.

Correct option: A.

A Snowball device is a physical storage device which supports large data transfers. It is commonly used for transporting huge amounts of data from on-premises to AWS. Concretely, Snowball Edge is suitable for data transfers up to 80 TB. The transport times are between 1 and 2 weeks, so in case that we have hundreds of terabytes of data, we get them earlier than using Internet.

In case that we need to transfer petabytes of data, it is recommended to use AWS Snowmobile, which is a physical track that transports data, up to 10 PB.

upvoted 1 times

✉ **Andreshere** 2 months, 2 weeks ago

The correct answer is B not A, i misswrote that.

upvoted 2 times

✉ **thewalker** 2 months, 3 weeks ago

Selected Answer: B

"The company must migrate the video files as soon as possible while using the least possible network bandwidth." - We have to address only this part of the whole problem / architecture. Hence, B.

upvoted 1 times

✉ **pentium75** 3 months ago

Selected Answer: B

"Least possible bandwidth" = Snowball Edge as it's physically transported to AWS and doesn't use any bandwidth. Depending on the company's available bandwidth (that we should not use anyway) it would still be faster and A and C. D is out because setting up the DirectConnect circuit would take ages, and wouldn't make sense because the import is a one-time job (the archive is no longer growing). Thus it's a typical job for Snow family.

upvoted 2 times

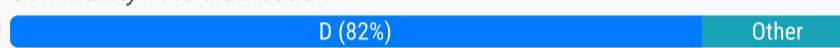
Question #7

Topic 1

A company has an application that ingests incoming messages. Dozens of other applications and microservices then quickly consume these messages. The number of messages varies drastically and sometimes increases suddenly to 100,000 each second. The company wants to decouple the solution and increase scalability.

Which solution meets these requirements?

- A. Persist the messages to Amazon Kinesis Data Analytics. Configure the consumer applications to read and process the messages.
- B. Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group to scale the number of EC2 instances based on CPU metrics.
- C. Write the messages to Amazon Kinesis Data Streams with a single shard. Use an AWS Lambda function to preprocess messages and store them in Amazon DynamoDB. Configure the consumer applications to read from DynamoDB to process the messages.
- D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SQS) subscriptions. Configure the consumer applications to process the messages from the queues.

Correct Answer: A*Community vote distribution*

rein_chau 1 year, 5 months ago

Selected Answer: D

D makes more sense to me.

upvoted 44 times

9014 1 year, 3 months ago

of course, the answer is D

upvoted 3 times

SilentMilli 1 year, 2 months ago

By default, an SQS queue can handle a maximum of 3,000 messages per second. However, you can request higher throughput by contacting AWS Support. AWS can increase the message throughput for your queue beyond the default limits in increments of 300 messages per second, up to a maximum of 10,000 messages per second.

It's important to note that the maximum number of messages per second that a queue can handle is not the same as the maximum number of requests per second that the SQS API can handle. The SQS API is designed to handle a high volume of requests per second, so it can be used to send messages to your queue at a rate that exceeds the maximum message throughput of the queue.

upvoted 10 times

Abdel42 1 year, 2 months ago

The limit that you're mentioning apply to FIFO queues. Standard queues are unlimited in throughput (<https://aws.amazon.com/sqs/features/>). Do you think that the use case require FIFO queue ?

upvoted 16 times

daizy 1 year, 1 month ago

D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SQS) subscriptions. Configure the consumer applications to process the messages from the queues.

This solution uses Amazon SNS and SQS to publish and subscribe to messages respectively, which decouples the system and enables scalability by allowing multiple consumer applications to process the messages in parallel. Additionally, using Amazon SQS with multiple subscriptions can provide increased resiliency by allowing multiple copies of the same message to be processed in parallel.

upvoted 12 times

Bevemo 1 year, 4 months ago

D. SNS Fan Out Pattern <https://docs.aws.amazon.com/sns/latest/dg/sns-common-scenarios.html> (A is wrong Kinesis Analysis does not 'persist' by itself.)

upvoted 19 times

ManikRoy 11 hours, 10 minutes ago

Selected Answer: D

Decouple systems and increase scalability - SNS & SQS.

upvoted 1 times

TilTil 1 week, 5 days ago

Selected Answer: D

Decouple and increase scalability are clear use cases for SNS and SQS.

D it is!

upvoted 2 times

 **Rosy92** 3 weeks, 5 days ago

Selected Answer: D

In this case is D because the requirement is to decouple the solution, the only way is to use AWS SQS.

upvoted 1 times

 **Prosen2522** 1 month, 1 week ago

Selected Answer: D

SNS and SQS combination is the only feasible option provided here.

upvoted 1 times

 **Idruizsan** 1 month, 1 week ago

Selected Answer: D

Tricky wording. If we focus on decoupling and scalability. SNS + SQS is the easiest way to go. FIFO queues can reach high throughput of 90,000 per second but the standard is unlimited in the transactions per second. Using KDS I am not sure if that meets the decoupling requirement in the question so it seems the question is presenting conflicting scenarios.

upvoted 2 times

 **Thee_tee** 1 month, 3 weeks ago

In my opinion D is wrong because of the way the words are ordered... perfect distractor SNS is the one that has subscribers and not SQS. therefore in this case, SQS would subscribe to a topic on SNS and process the queue accordingly.

upvoted 2 times

 **Piyu15** 1 month, 3 weeks ago

Selected Answer: D

Decoupling + scalability, so SNS and SQS is the right combination. Hence d
A and B doesn't make sense.

C Kinesis data stream is more suitable for live events

upvoted 1 times

 **Techie_G** 2 months, 1 week ago

Can someone please tell me what then is the correct answer? When I click on reveal answer it says A is the correct answer but states that most people voted for D. So which answer am I supposed to go with? Thanks

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: D

D: SNS + SQS is most scalable option here

A: Data analytics is not for messaging

B: EC2 Autoscaling based on CPU metrics won't scale with message quantity

C: KDS with single shard for large number of messages won't work

upvoted 2 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: D

D seems correct

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: B

B seems right

upvoted 1 times

 **Andreshere** 2 months, 2 weeks ago

Selected Answer: D

The key word for this question is "decouple". When we want to decouple an application (with microservices), we want to factor it as much as possible. One pattern that allows that decoupling is the fan-out pattern, which sets an SNS topic with many SQS queues that process the messages. So, the correct answer is D.

A. Using Amazon KDA is not suitable because the lack of consumers and customers. It is better to use Amazon Kinesis Data Streams, which processes real-time data from many different sources (consumers). Additionally, persisting does not make sense for the statement requirements.

B. EC2 instances are not feasible for supporting high workloads with unpredictable traffic spikes. Moreover, it is expensive and inefficient because EC2 has no mechanisms to avoid traffic spikes and decoupling.

C. Even though using Amazon KDS is okay, it cannot handle with traffic spikes with that number of shards. Additionally, this solution is operationally complex since we use DynamoDB, which can have a bottleneck.

upvoted 2 times

 **Choufan_Monk** 2 months, 2 weeks ago

Answer: D - keywords: microservices, decoupling = SQS

upvoted 1 times

 **mohamedsambo** 2 months, 2 weeks ago

Answer is D

cause A would be suitable if Amazon Kinesis Data Streams, not Amazon Kinesis Data Analytics
who is talking about data analytics, and monitoring here ?!!

upvoted 1 times

 **pentium75** 3 months ago

Selected Answer: D

A and B is nonsense, and even C would be unable to handle the spikes; also the Dynamo DB would be overhead - its a DB, not a queuing engine. Stem asks for decoupling, this is exactly what D does.

upvoted 1 times

Question #8

Topic 1

A company is migrating a distributed application to AWS. The application serves variable workloads. The legacy platform consists of a primary server that coordinates jobs across multiple compute nodes. The company wants to modernize the application with a solution that maximizes resiliency and scalability.

How should a solutions architect design the architecture to meet these requirements?

- A. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling to use scheduled scaling.
- B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling based on the size of the queue.
- C. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure AWS CloudTrail as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the primary server.
- D. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure Amazon EventBridge (Amazon CloudWatch Events) as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the compute nodes.

Correct Answer: C

Community vote distribution

B (95%) 3%

✉️ **rein_chau** Highly Voted 1 year, 5 months ago

Selected Answer: B

A - incorrect: Schedule scaling policy doesn't make sense.
 C, D - incorrect: Primary server should not be in same Auto Scaling group with compute nodes.
 B is correct.

upvoted 72 times

✉️ **Wilson_S** 1 year, 4 months ago

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>
 upvoted 4 times

✉️ **Sinaneos** Highly Voted 1 year, 5 months ago

Selected Answer: B

The answer seems to be B for me:
 A: doesn't make sense to schedule auto-scaling
 C: Not sure how CloudTrail would be helpful in this case, at all.
 D: EventBridge is not really used for this purpose, wouldn't be very reliable
 upvoted 20 times

✉️ **ManikRoy** Most Recent 10 hours, 18 minutes ago

Selected Answer: B

Correct option B. SQS is used to decouple the distributed architecture (primary server and compute nodes). Scheduled auto scaling doesn't make sense as the workload is variable, so based on size of the queue is the correct option.
 upvoted 1 times

✉️ **Rosy92** 3 weeks, 5 days ago

Selected Answer: B

the correct solution is B, because in the requirement is said "the application serves variable workloads" and we need to decouple monolithic infrastructure here so this required SQS.
 upvoted 1 times

✉️ **fsp52** 3 weeks, 5 days ago

Selected Answer: B

This option leverages Amazon SQS to decouple the primary server from the compute nodes, ensuring resiliency and scalability. The compute nodes can be managed in an Auto Scaling group, scaling based on the size of the SQS queue, which reflects the workload. This design allows the system to handle variable workloads efficiently while maximizing scalability and resiliency.
 upvoted 1 times

✉️ **anandavinash** 1 month ago

Selected Answer: B

B is a correct answer
 upvoted 1 times

 **Idruizsan** 1 month, 1 week ago

Not sure how CloudTrail would be useful when the requirement is that the solution be resilient and scalable. You build resiliency by decoupling workflows use SQS and then using that queue size as the metric by which to scale the Auto Scaling groups. CloudTrail is for logging and visibility of resources and shouldn't be used for jobs.

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: B

SQS + EC2 scaling based on size of queue is best solution

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: B

B seems correct

upvoted 1 times

 **Andreshere** 2 months, 2 weeks ago

Selected Answer: B

SQS helps to process messages in case of variable workloads. The compute nodes must be implemented using EC2 instances (or alternatively, ECS tasks or managed Kubernetes nodes, but this option is not available). AutoScaling must be based on the workload, which is controlled by the queue. So, the correct option is B.

A is not correct because the instances should not scale based on a schedule which is not deterministic. On the contrary, scales based on the workload (queue size) is more effective.

AWS CloudTrail should not be used as a destination job and it is not related to the question. The same applies to EventBridge.

upvoted 2 times

 **thewalker** 2 months, 2 weeks ago

Selected Answer: B

B - Based on the size of queue, the auto scaling should done.

upvoted 1 times

 **pentium75** 3 months ago

Selected Answer: B

B, scale per queue size and replace the scheduling server with the cloud service. C is nonsense because CloudTrail is not a job scheduler.

upvoted 1 times

 **mullins** 3 months ago

Selected Answer: B

B for decoupling

upvoted 1 times

 **Debabrata1234** 3 months ago

Selected Answer: D

Auto scale based on other nodes other than master node

upvoted 1 times

 **achechen** 4 months ago

Selected Answer: B

B of course

upvoted 1 times

 **ssz123** 4 months, 1 week ago

Selected Answer: B

B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling based on the size of the queue.

upvoted 1 times

 **nathanss** 4 months, 2 weeks ago

Selected Answer: B

B is the right answer here.

upvoted 1 times

Question #9

Topic 1

A company is running an SMB file server in its data center. The file server stores large files that are accessed frequently for the first few days after the files are created. After 7 days the files are rarely accessed.

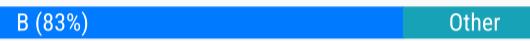
The total data size is increasing and is close to the company's total storage capacity. A solutions architect must increase the company's available storage space without losing low-latency access to the most recently accessed files. The solutions architect must also provide file lifecycle management to avoid future storage issues.

Which solution will meet these requirements?

- A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.
- B. Create an Amazon S3 File Gateway to extend the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.
- C. Create an Amazon FSx for Windows File Server file system to extend the company's storage space.
- D. Install a utility on each user's computer to access Amazon S3. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

Correct Answer: D

Community vote distribution



✉️ **Sinaneos** 1 year, 5 months ago

Answer directly points towards file gateway with lifecycles, <https://docs.aws.amazon.com/filegateway/latest/files3/CreatingAnSMBFileShare.html>

D is wrong because utility function is vague and there is no need for flexible storage.

upvoted 45 times

✉️ **Udoyen** 1 year, 3 months ago

Yes it might be vague but how do we keep the low-latency access that only flexible can offer?

upvoted 3 times

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

Low-latency access is only required for the first 7 days, B maintains that fast access for 7 days and only then are the files sent to Glacier Archive

upvoted 2 times

✉️ **Nava702** 7 months ago

It says low-latency is required for the most recently accessed files, not new ones. So if an older file is retrieved from deep archive, it should then readily be accessible, according to the question, which points toward Flexible retrieval. However the utility portion in the answer D is vague.

upvoted 1 times

✉️ **Ander927** 3 months, 1 week ago

file gateway comes with a cache volume on-premise which ensures the low latency for the most recently accessed files

upvoted 3 times

✉️ **javitech83** 1 year, 3 months ago

Selected Answer: B

B answer is correct. low latency is only needed for newer files. Additionally, File GW provides low latency access by caching frequently accessed files locally so answer is B

upvoted 25 times

✉️ **ManikRoy** 9 hours, 52 minutes ago

Selected Answer: B

S3 File gateway with lifecycle policy for auto transition of old files.

upvoted 1 times

✉️ **ManikRoy** 9 hours, 53 minutes ago

S3 File Gateway with lifecycle policy transition.

upvoted 1 times

✉️ **Liam_W** 1 week, 4 days ago

Selected Answer: D

Initially when reading this question, I wanted to use S3 Intelligent Tiering as the answer but it was not mentioned.

I was then torn between B and D due to the life cycle policies that were required as stated by the question: I chose D because it covers the need to be accessed whenever, without reducing the latency. This answer is also the best choice as it would reduce any storage issues users could face.

upvoted 2 times

 **hro** 5 days, 22 hours ago

AWS would not have you install a utility do something a service can do. The answer is B.

upvoted 3 times

 **cygao** 3 weeks, 4 days ago

Selected Answer: B

absolutely B

upvoted 1 times

 **Rosy92** 3 weeks, 5 days ago

Selected Answer: B

Amazon s3 file gateway is a solution to transfer data from storage on prem to storage in cloud and it supports SMB, ISCSI and NFS protocols so B is the correct answer.

upvoted 2 times

 **Beln** 4 weeks, 1 day ago

This was on the Test! I got a 965 on it!

upvoted 2 times

 **cryptics** 1 month, 1 week ago

Selected Answer: B

B innit

upvoted 1 times

 **NachoDevOps** 1 month, 2 weeks ago

Selected Answer: B

gateway to connect on premise with cloud and lifecycle to prevent space issues in the future .

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: B

Problems: SMB + Out of space + require low latency access to recent file + 7 day old files can go in archive

A: Can work but not a continuous process so storage problems not solved

C: FSx needs to connect to something on other side to transfer data. This is not specified here

D: There is not data on user computer.

B File gateway is for extending on-prem to S3. <https://aws.amazon.com/storagegateway/file/>

upvoted 3 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: B

B seems correct

upvoted 1 times

 **Andreshere** 2 months, 2 weeks ago

A. DataSync is focused on transferring data when we need synchronization (for example, from an on-premises DB that updates daily to a DB in AWS). In this case, we don't need to transfer data or synchronize data, we only need to increase the storage. So, this option is not correct.

B. S3 File Gateway allows communication between a File System/Server and S3, and it supports SMB protocol. We can use S3 FGW to move files from the FS to the S3 bucket. Then, the question says that files older than seven days are rarely accessed, so we can transition to S3 Glacier for those files to archive, in a costly-efficient way. So, this option is correct.

C. You have two different storages for saving the files, making the interoperability unnecessarily more complex (and you need constant data synchronization, regarding to option A).

D. This is a mess. The solution is not scalable and It depends on the number of users, which is not a static number. Additionally, Flexible Retrieval is unnecessary.

upvoted 4 times

 **thewalker** 2 months, 2 weeks ago

Selected Answer: B

After 7 days the files are rarely accessed. Hence, B

upvoted 1 times

 **Debabrata1234** 3 months ago

Selected Answer: D

test the prep

upvoted 1 times

 **Hams0** 3 months ago

Check this out. S3 file gateway meets all the requirements

<https://aws.amazon.com/storagegateway/faqs/#:~:text=Amazon%20S3%20File%20Gateway%20securely,latency%20access%20to%20cached%20data>.

upvoted 3 times

 **jaswantn** 1 month, 2 weeks ago

yes it does say- Amazon S3 File Gateway securely and durably stores both file contents and metadata as objects, while providing your on-premises applications low-latency access to cached data. thus proving option B the viable choice.

upvoted 1 times

 **riadS** 3 months, 1 week ago

Selected Answer: D

B is the cheapest option, but I think the question is kind of vague and can be tricky because they specify that they need access to the most recently accessed files not the files that have been recently created, which points to the need of some flexible retrieval. Still I'll have to agree with some other comments regarding that the question directs to file gateway, but since the option is not available I would go for the D option.

upvoted 1 times

Question #10

Topic 1

A company is building an ecommerce web application on AWS. The application sends information about new orders to an Amazon API Gateway REST API to process. The company wants to ensure that orders are processed in the order that they are received. Which solution will meet these requirements?

- A. Use an API Gateway integration to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when the application receives an order. Subscribe an AWS Lambda function to the topic to perform processing.
- B. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order. Configure the SQS FIFO queue to invoke an AWS Lambda function for processing.
- C. Use an API Gateway authorizer to block any requests while the application processes an order.
- D. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order. Configure the SQS standard queue to invoke an AWS Lambda function for processing.

Correct Answer: A*Community vote distribution*

B (98%)

 **Sinaneos**  1 year, 5 months ago

Selected Answer: B

B because FIFO is made for that specific purpose
upvoted 57 times

 **rein_chau**  1 year, 5 months ago

Selected Answer: B

Should be B because SQS FIFO queue guarantees message order.
upvoted 25 times

 **ManikRoy**  9 hours, 49 minutes ago

Selected Answer: B

SQS FIFO Queue is for this use case.
upvoted 1 times

 **hro** 5 days, 22 hours ago

B
SNS - PubSub (think pass along)
SQS - Queueing (think batch)
Kinesis - Real-time
SWF - Queuing but with people
upvoted 1 times

 **JavierEF** 1 week, 5 days ago

Selected Answer: B

A is not correct because, if we do not specify that it is an SNS FIFO, we have no guarantee the messages will be processed in publishing order.
upvoted 1 times

 **Rosy92** 3 weeks, 5 days ago

Selected Answer: B

Orders have to be processed in order so SQS FIFO is requested here.
upvoted 1 times

 **Idruizsan** 1 month, 1 week ago

Selected Answer: B

Although A is a viable option, the statement says it needs to ensure that messages are processed in the order they are received. That is FIFO by definition.
upvoted 1 times

 **bigmancloud** 1 month, 2 weeks ago

Amazon SQS FIFO Queue ensures that messages are processed in the order they are received
upvoted 1 times

 **kioks23** 1 month, 3 weeks ago

B - FIFO is designed for that
upvoted 1 times

✉  **Hirriz** 1 month, 3 weeks ago

At the beginning I saw people praising this dump because they passed but now I only attempted 10 questions and 5 of them have wrong answers upvoted 2 times

✉  **kioks23** 1 month, 3 weeks ago

You have to read the discussions for the correct answers
upvoted 4 times

✉  **Sivadocker7** 2 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

Selected Answer: B

SQS FIFO is the only working solution here
upvoted 1 times

✉  **A_jaa** 2 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

✉  **Andreshere** 2 months, 2 weeks ago

Selected Answer: B

A. This option could be correct if we use SNS FIFO option, but this is not the case stated in the question. Additionally, this task is more efficient done by a queue than a subscription service. So, this option is not correct.
B. We use a queue, which is efficient processing messages. Additionally, it preserves the order since it is a FIFO queue. Meanwhile we don't have any kind of messages throughput limitation, this option is correct.
C. This option discards any messages that are still processing, which is not a good solution.
D. Same option as B but using a normal queue, which does not preserve the order. Incorrect.
upvoted 2 times

✉  **Pangian** 2 months, 3 weeks ago

What's wrong with this website? Are they intentionally chose the wrong answer? 5 Qs in a row wrong?! How can someone be prepared for the exams if he is confused about the correct answer?

upvoted 3 times

✉  **awsgeek75** 2 months, 3 weeks ago

B is the right answer because FIFO is a core requirement of the question.
upvoted 1 times

✉  **cardebab** 2 months, 3 weeks ago

Why it says is A when of course B is the right answer?

upvoted 2 times

Question #11

Topic 1

A company has an application that runs on Amazon EC2 instances and uses an Amazon Aurora database. The EC2 instances connect to the database by using user names and passwords that are stored locally in a file. The company wants to minimize the operational overhead of credential management.

What should a solutions architect do to accomplish this goal?

- A. Use AWS Secrets Manager. Turn on automatic rotation.
- B. Use AWS Systems Manager Parameter Store. Turn on automatic rotation.
- C. Create an Amazon S3 bucket to store objects that are encrypted with an AWS Key Management Service (AWS KMS) encryption key. Migrate the credential file to the S3 bucket. Point the application to the S3 bucket.
- D. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume for each EC2 instance. Attach the new EBS volume to each EC2 instance. Migrate the credential file to the new EBS volume. Point the application to the new EBS volume.

Correct Answer: B

Community vote distribution



✉️ **Sinaneos** 1 year, 5 months ago

Selected Answer: A

B is wrong because parameter store does not support auto rotation, unless the customer writes it themselves, A is the answer.
upvoted 82 times

✉️ **hro** 4 days, 23 hours ago

A - additionally, Aurora manages the settings for the secret and rotates the secret every seven days by default.
upvoted 1 times

✉️ **iCdma** 1 year, 5 months ago

ty bro, I was confused about that and you just mentioned the "key" phrase, B doesn't support autorotation
upvoted 2 times

✉️ **kewl** 1 year, 3 months ago

correct. see link <https://tutorialsdojo.com/aws-secrets-manager-vs-systems-manager-parameter-store/> for differences between SSM Parameter Store and AWS Secrets Manager
upvoted 17 times

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

That was a fantastic link. This part of their site "comparison of AWS services" is superb. Thanks.
upvoted 6 times

✉️ **17Master** 1 year, 4 months ago

READ!!! AWS Secrets Manager is a secrets management service that helps you protect access to your applications, services, and IT resources. This service enables you to rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.
<https://aws.amazon.com/cn/blogs/security/how-to-connect-to-aws-secrets-manager-service-within-a-virtual-private-cloud/> y
https://aws.amazon.com/secrets-manager/?nc1=h_ls
upvoted 20 times

✉️ **HarishArul** 10 months ago

Read this - https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_parameterstore.html
It says SSM Parameter store cant rotate automatically.
upvoted 5 times

✉️ **Leo1688** 3 months, 3 weeks ago

you are right
upvoted 1 times

✉️ **leeyoung** 1 year, 2 months ago

Admin is trying to fail everybody in the exam.
upvoted 67 times

✉️ **perception** 11 months ago

He wants you to read discussion part as well for better understanding
upvoted 5 times

✉️ **acuaws** 12 months ago

RIGHT? I found a bunch of "correct" answers on here are not really correct, but they're not corrected? hhmmmmm

upvoted 2 times

✉ **OctavioBatera** Most Recent 1 week, 4 days ago

Selected Answer: A

Secrets Manager, as The Mandalorian would say "this is the way!"

upvoted 1 times

✉ **TilTil** 1 week, 4 days ago

Selected Answer: A

SSM has no automatic rotation.

upvoted 1 times

✉ **Shalini10dec** 2 weeks, 1 day ago

The most suitable option for minimizing operational overhead of credential management in this scenario is:

B. Use AWS Systems Manager Parameter Store. Turn on automatic rotation.

AWS Systems Manager Parameter Store is a service that helps you manage configuration data, including sensitive information such as passwords and database strings, in a central, secure store. With automatic rotation enabled, the credentials can be automatically updated at scheduled intervals, reducing the manual effort required for credential management.

upvoted 1 times

✉ **Kanagarajd** 3 weeks, 1 day ago

Selected Answer: A

Secret manager with auto rotation.

upvoted 1 times

✉ **andyngkh86** 2 months, 1 week ago

I copy and paste the question & options to ChatGPT, and ChatGPT give the answer is A

upvoted 2 times

✉ **awsgeek75** 2 months, 1 week ago

Selected Answer: A

BCD are extremely high operational overhead and not secure like A

upvoted 1 times

✉ **A_jaa** 2 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

✉ **ifaby** 4 months, 2 weeks ago

Selected Answer: B

B because the user wants reduce costs and SSM Parameter Store layer Standard is free and the type SecureString uses KMS

upvoted 3 times

✉ **Ruffyit** 5 months ago

A: READ!!! AWS Secrets Manager is a secrets management service that helps you protect access to your applications, services, and IT resources. This service enables you to rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.
<https://aws.amazon.com/cn/blogs/security/how-to-connect-to-aws-secrets-manager-service-within-a-virtual-private-cloud/>
https://aws.amazon.com/secrets-manager/?nc1=h_ls

Read this - https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_parameterstore.html

It says SSM Parameter store cant rotate automatically.

upvoted 2 times

✉ **AbirAbu** 5 months, 1 week ago

It should be "A."

upvoted 2 times

✉ **santbot** 5 months, 3 weeks ago

Selected Answer: A

A - SECRETS MANAGER

upvoted 1 times

✉ **Mandar15** 5 months, 3 weeks ago

Selected Answer: A

Aurora automatically stores and manages database credentials in AWS Secrets Manager. Aurora rotates database credentials regularly, without requiring application changes. Secrets Manager secures database credentials from human access and plain text view.

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

upvoted 3 times

✉ **NaaVeeN** 5 months, 3 weeks ago

If most Voted answers is done by us, then Who is marking the answers as Correct ?

upvoted 4 times

 **novice16** 6 months ago

Selected Answer: A

Secret manager and auto rotation does the job

upvoted 1 times

 **Shaansd** 6 months ago

can anyone please share the pdf to my email sstanudas@gmail.com

upvoted 1 times

Question #12

Topic 1

A global company hosts its web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The web application has static data and dynamic data. The company stores its static data in an Amazon S3 bucket. The company wants to improve performance and reduce latency for the static data and dynamic data. The company is using its own domain name registered with Amazon Route 53. What should a solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution that has the S3 bucket and the ALB as origins. Configure Route 53 to route traffic to the CloudFront distribution.
- B. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Configure Route 53 to route traffic to the CloudFront distribution.
- C. Create an Amazon CloudFront distribution that has the S3 bucket as an origin. Create an AWS Global Accelerator standard accelerator that has the ALB and the CloudFront distribution as endpoints. Create a custom domain name that points to the accelerator DNS name. Use the custom domain name as an endpoint for the web application.
- D. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Create two domain names. Point one domain name to the CloudFront DNS name for dynamic content. Point the other domain name to the accelerator DNS name for static content. Use the domain names as endpoints for the web application.

Correct Answer: C

Community vote distribution

A (79%) C (21%)

✉️  **Kartikey140**  1 year, 4 months ago

Answer is A

Explanation - AWS Global Accelerator vs CloudFront

- They both use the AWS global network and its edge locations around the world
- Both services integrate with AWS Shield for DDoS protection.
- CloudFront
- Improves performance for both cacheable content (such as images and videos)
- Dynamic content (such as API acceleration and dynamic site delivery)
- Content is served at the edge
- Global Accelerator
- Improves performance for a wide range of applications over TCP or UDP
- Proxying packets at the edge to applications running in one or more AWS Regions.
- Good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP
- Good for HTTP use cases that require static IP addresses
- Good for HTTP use cases that required deterministic, fast regional failover

upvoted 92 times

✉️  **daizy** 1 year, 1 month ago

By creating a CloudFront distribution that has both the S3 bucket and the ALB as origins, the company can reduce latency for both the static and dynamic data. The CloudFront distribution acts as a content delivery network (CDN), caching the data closer to the users and reducing the latency. The company can then configure Route 53 to route traffic to the CloudFront distribution, providing improved performance for the web application.

upvoted 13 times

✉️  **kanweng**  1 year, 4 months ago

Selected Answer: A

Q: How is AWS Global Accelerator different from Amazon CloudFront?

A: 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 31 times

✉️  **chickenmf**  1 week, 4 days ago

This question is absolutely insane

upvoted 2 times

✉️  **Kangtong** 3 weeks, 5 days ago

Selected Answer: A

My chatGPT4 answer me it is A.

It said C has a structural problem so it cannot really be made in practice.

I leave this comment for who be confused by chatGPT3.5.

upvoted 1 times

 **Prosen2522** 1 month, 1 week ago

Selected Answer: A

CloudFront can be used for both static and dynamic content distribution.

upvoted 2 times

 **hi2vaisakh** 2 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

 **andyngkh86** 2 months, 1 week ago

chatGPT give the answer is C

upvoted 1 times

 **tsdsmth** 2 months, 1 week ago

chatGPT is not ALWAYS right. Beware!

upvoted 3 times

 **Parul25** 2 months, 1 week ago

The company is using its own domain name registered with Amazon Route 53 so C cannot be the answer.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: A

GlobaAccelerator helps routing users to closest region. The question doesn't say anything about latency due to region so BCD don't really solve much problems.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

<https://aws.amazon.com/blogs/networking-and-content-delivery/deliver-your-apps-dynamic-content-using-amazon-cloudfront-getting-started-template/>

upvoted 2 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: A

Answer: A

upvoted 2 times

 **Mutahir1** 2 months, 3 weeks ago

Ans is C; This solution involves using Amazon CloudFront for caching the static content, which will improve performance and reduce latency for the static data. Additionally, by creating an AWS Global Accelerator standard accelerator with the ALB and the CloudFront distribution as endpoints, the company can further improve the availability and performance of the web application. Finally, creating a custom domain name that points to the accelerator DNS name will allow the company to use the custom domain name as an endpoint for the web application, providing a seamless experience for the users.

The search results provide information about the benefits of using a standard accelerator in AWS Global Accelerator to improve the availability and performance of applications, as well as the steps for creating a standard accelerator and working with standard accelerators in AWS Global Accelerator

upvoted 1 times

 **Wang87** 3 months ago

Selected Answer: A

Answer is A

upvoted 1 times

 **ale_brd_** 3 months, 3 weeks ago

Selected Answer: A

A is correct;

Option B and option C are incorrect because they include invalid endpoint configurations for Global Accelerator. Global Accelerator Standard does not support S3 endpoints or CloudFront distribution endpoints.

upvoted 3 times

 **theonlyhero** 4 months, 2 weeks ago

I just tested, there is no option in Global Accelerator to make CloudFront distribution as endpoints. so anwer is A

upvoted 8 times

 **Ruffyit** 5 months ago

I'm wavering between A and C.

With dynamic content, CloudFront is cacheable and that's not good.

But with answer C, AWS Global doesn't support Cloudfont endpoint

"Endpoints for standard accelerators in AWS Global Accelerator can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances,

or Elastic IP addresses. "

So I choose A

upvoted 1 times

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

Selected Answer: C

C seems reasonable due to the fact that CloudFront is tedious when it comes to Dynamic content, you need to expire the content everytime it changes, which adds extra work and might lead to inconsistent results.

upvoted 1 times

✉ **eladbeV2** 2 months, 3 weeks ago

As mentioned before by others, Global Accelerator Standard can't use S3 or CloudFront distribution as Endpoints.

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

upvoted 2 times

✉ **danielpark99** 5 months, 2 weeks ago

Answer is A

CloudFront vs Global Accelerator has some differences

1. CloudFront : Improves performance for both cacheable contents

2. Global Accelerator : proxying packets at the edge to applications running in one or more AWS regions as working like anycast with closer to the pop and no-cache

Good use case for required fast regional failover

upvoted 1 times

✉ **rainiverse** 5 months, 4 weeks ago

Selected Answer: A

I'm wavering between A and C.

With dynamic content, CloudFront is cacheable and that's not good.

But with answer C, AWS Global doesn't support Cloudfront endpoint

"Endpoints for standard accelerators in AWS Global Accelerator can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses. "

So I choose A

upvoted 2 times

Question #13

Topic 1

A company performs monthly maintenance on its AWS infrastructure. During these maintenance activities, the company needs to rotate the credentials for its Amazon RDS for MySQL databases across multiple AWS Regions. Which solution will meet these requirements with the LEAST operational overhead?

- A. Store the credentials as secrets in AWS Secrets Manager. Use multi-Region secret replication for the required Regions. Configure Secrets Manager to rotate the secrets on a schedule.
- B. Store the credentials as secrets in AWS Systems Manager by creating a secure string parameter. Use multi-Region secret replication for the required Regions. Configure Systems Manager to rotate the secrets on a schedule.
- C. Store the credentials in an Amazon S3 bucket that has server-side encryption (SSE) enabled. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function to rotate the credentials.
- D. Encrypt the credentials as secrets by using AWS Key Management Service (AWS KMS) multi-Region customer managed keys. Store the secrets in an Amazon DynamoDB global table. Use an AWS Lambda function to retrieve the secrets from DynamoDB. Use the RDS API to rotate the secrets.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **rein_chau**  1 year, 5 months ago

Selected Answer: A

A is correct.

<https://aws.amazon.com/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/>
upvoted 22 times

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

Selected Answer: A

Keywords:

- rotate the credentials for its Amazon RDS for MySQL databases across multiple AWS Regions
- LEAST operational overhead

A: Correct - AWS Secrets Manager supports

- Encrypt credential for RDS, DocumentDb, Redshift, other DBs and key/value secret.
- multi-region replication.
- Remote base on schedule

B: Incorrect - Secure string parameter only apply for Parameter Store. All the data in AWS Secrets Manager is encrypted

C: Incorrect - don't mention about replicate S3 across region.

D: Incorrect - So many steps compare to answer A =))

upvoted 9 times

✉️  **ics_911**  1 month, 1 week ago

Selected Answer: A

A is correct.

upvoted 1 times

✉️  **A_jaa** 2 months, 1 week ago

Selected Answer: A

Answer-A

upvoted 1 times

✉️  **Ruffyit** 5 months ago

<https://aws.amazon.com/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/> A is answer
upvoted 2 times

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

Selected Answer: A

Clearly A is the correct one.

upvoted 1 times

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

So this is what I thought

<https://youtube.com/shorts/6YSBv95V2cs?feature=share>

What is a secure string parameter?

<https://youtube.com/shorts/-6wJOqZ93co?feature=share>

upvoted 1 times

✉ **TariqKipkemei** 8 months ago

Selected Answer: A

'The company needs to rotate the credentials for its Amazon RDS for MySQL databases across multiple AWS Regions' = AWS Secrets Manager

upvoted 1 times

✉ **miki111** 8 months, 2 weeks ago

Option A MET THE REQUIREMENT

upvoted 1 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: A

Option A: Storing the credentials as secrets in AWS Secrets Manager provides a dedicated service for secure and centralized management of secrets. By using multi-Region secret replication, the company ensures that the secrets are available in the required Regions for rotation. Secrets Manager also provides built-in functionality to rotate secrets automatically on a defined schedule, reducing operational overhead. This automation simplifies the process of rotating credentials for the Amazon RDS for MySQL databases during monthly maintenance activities.

upvoted 5 times

✉ **Bmarodi** 9 months, 4 weeks ago

Selected Answer: A

A is correct answer.

upvoted 1 times

✉ **Musti35** 11 months, 2 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/>

With Secrets Manager, you can store, retrieve, manage, and rotate your secrets, including database credentials, API keys, and other secrets. When you create a secret using Secrets Manager, it's created and managed in a Region of your choosing. Although scoping secrets to a Region is a security best practice, there are scenarios such as disaster recovery and cross-Regional redundancy that require replication of secrets across Regions. Secrets Manager now makes it possible for you to easily replicate your secrets to one or more Regions to support these scenarios.

upvoted 3 times

✉ **linux_admin** 12 months ago

Selected Answer: A

A. Store the credentials as secrets in AWS Secrets Manager. Use multi-Region secret replication for the required Regions. Configure Secrets Manager to rotate the secrets on a schedule.

This solution is the best option for meeting the requirements with the least operational overhead. AWS Secrets Manager is designed specifically for managing and rotating secrets like database credentials. Using multi-Region secret replication, you can easily replicate the secrets across the required AWS Regions. Additionally, Secrets Manager allows you to configure automatic secret rotation on a schedule, further reducing the operational overhead.

upvoted 1 times

✉ **cheese929** 1 year, 1 month ago

Selected Answer: A

A is correct.

upvoted 1 times

✉ **BlueVolcano1** 1 year, 2 months ago

Selected Answer: A

It's A, as Secrets Manager does support replicating secrets into multiple AWS Regions:

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

upvoted 3 times

✉ **Abdel42** 1 year, 2 months ago

Selected Answer: A

it's A, here the question specify that we want the LEAST overhead

upvoted 2 times

✉ **MichaelCarrasco** 1 year, 1 month ago

<https://aws.amazon.com/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/>

upvoted 1 times

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

Selected Answer: A

AWS Secrets Manager is a secrets management service that enables you to store, manage, and rotate secrets such as database credentials, API keys, and SSH keys. Secrets Manager can help you minimize the operational overhead of rotating credentials for your Amazon RDS for MySQL databases across multiple Regions. With Secrets Manager, you can store the credentials as secrets and use multi-Region secret replication to replicate the secrets to the required Regions. You can then configure Secrets Manager to rotate the secrets on a schedule so that the credentials are rotated automatically without the need for manual intervention. This can help reduce the risk of secrets being compromised and minimize the operational overhead of credential management.

upvoted 3 times

Question #14

Topic 1

A company runs an ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales based on CPU utilization metrics. The ecommerce application stores the transaction data in a MySQL 8.0 database that is hosted on a large EC2 instance.

The database's performance degrades quickly as application load increases. The application handles more read requests than write transactions. The company wants a solution that will automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability.

Which solution will meet these requirements?

- A. Use Amazon Redshift with a single node for leader and compute functionality.
- B. Use Amazon RDS with a Single-AZ deployment Configure Amazon RDS to add reader instances in a different Availability Zone.
- C. Use Amazon Aurora with a Multi-AZ deployment. Configure Aurora Auto Scaling with Aurora Replicas.
- D. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.

Correct Answer: C

Community vote distribution

C (100%)

✉️  **D2w**  1 year, 5 months ago

Selected Answer: C

C, AURORA is 5x performance improvement over MySQL on RDS and handles more read requests than write;; maintaining high availability = Multi-AZ deployment

upvoted 39 times

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

Selected Answer: C

Option C, using Amazon Aurora with a Multi-AZ deployment and configuring Aurora Auto Scaling with Aurora Replicas, would be the best solution to meet the requirements.

Aurora is a fully managed, MySQL-compatible relational database that is designed for high performance and high availability. Aurora Multi-AZ deployments automatically maintain a synchronous standby replica in a different Availability Zone to provide high availability. Additionally, Aurora Auto Scaling allows you to automatically scale the number of Aurora Replicas in response to read workloads, allowing you to meet the demand of unpredictable read workloads while maintaining high availability. This would provide an automated solution for scaling the database to meet the demand of the application while maintaining high availability.

upvoted 17 times

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

Option A, using Amazon Redshift with a single node for leader and compute functionality, would not provide high availability.

Option B, using Amazon RDS with a Single-AZ deployment and configuring RDS to add reader instances in a different Availability Zone, would not provide high availability and would not automatically scale the number of reader instances in response to read workloads.

Option D, using Amazon ElastiCache for Memcached with EC2 Spot Instances, would not provide a database solution and would not meet the requirements.

upvoted 5 times

✉️  **A_jaa**  2 months, 1 week ago

Selected Answer: C

Answer-c

upvoted 1 times

✉️  **Ndlesty** 4 months, 1 week ago

Selected Answer: C

key statement: "...will automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability.

upvoted 1 times

✉️  **AWSGuru123** 5 months, 3 weeks ago

Selected Answer: C

Aurora

upvoted 1 times

✉️  **Syruis** 7 months, 2 weeks ago

Selected Answer: C

C fit perfectly

upvoted 1 times

✉ **TariqKipkemei** 8 months ago

Selected Answer: C

Unpredictable read workloads while maintaining high availability = Amazon Aurora with a Multi-AZ deployment, Auto Scaling with Aurora read replicas.

upvoted 1 times

✉ **Guru4Cloud** 8 months, 1 week ago

Selected Answer: C

As the application handles more read requests than write transactions, using read replicas with Aurora is an ideal choice as it allows read scaling without sacrificing write performance on the primary instance.

upvoted 1 times

✉ **miki111** 8 months, 2 weeks ago

Option C MET THE REQUIREMENT

upvoted 1 times

✉ **hiepdz98** 9 months ago

Selected Answer: C

Option C

upvoted 1 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: C

Option C: Using Amazon Aurora with a Multi-AZ deployment and configuring Aurora Auto Scaling with Aurora Replicas is the most appropriate solution. Aurora is a MySQL-compatible relational database engine that provides high performance and scalability. With Multi-AZ deployment, the database is automatically replicated across multiple Availability Zones for high availability. Aurora Auto Scaling allows the database to automatically add or remove Aurora Replicas based on the workload, ensuring that read requests can be distributed effectively and the database can scale to meet demand. This provides both high availability and automatic scaling to handle unpredictable read workloads.

upvoted 2 times

✉ **Bmarodi** 9 months, 4 weeks ago

Selected Answer: C

C meets the requirements.

upvoted 1 times

✉ **Mehkay** 10 months ago

C Aurora with read replicas

upvoted 1 times

✉ **big0007** 10 months, 2 weeks ago

Key words:

- Must support MySQL
- High Availability (must be multi-az)
- Auto Scaling

upvoted 4 times

✉ **cheese929** 10 months, 2 weeks ago

Selected Answer: C

C is correct since cost is not a concern.

upvoted 1 times

✉ **Abrar2022** 10 months, 2 weeks ago

It's Aurora with Multi-AZ deployment - Keywords > "unpredictable read workloads while maintaining high availability"

upvoted 2 times

✉ **Abrar2022** 10 months, 2 weeks ago

To automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability, you can use Amazon Aurora with a Multi-AZ deployment. Aurora is a fully managed, MySQL-compatible database service that can automatically scale up or down based on workload demands. With a Multi-AZ deployment, Aurora maintains a synchronous standby replica in a different Availability Zone (AZ) to provide high availability in the event of an outage.

upvoted 2 times

Question #15

Topic 1

A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC. The company had an inspection server in its on-premises data center. The inspection server performed specific operations such as traffic flow inspection and traffic filtering. The company wants to have the same functionalities in the AWS Cloud.

Which solution will meet these requirements?

- A. Use Amazon GuardDuty for traffic inspection and traffic filtering in the production VPC.
- B. Use Traffic Mirroring to mirror traffic from the production VPC for traffic inspection and filtering.
- C. Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.
- D. Use AWS Firewall Manager to create the required rules for traffic inspection and traffic filtering for the production VPC.

Correct Answer: C

Community vote distribution



✉️ **SilentMilli** Highly Voted 1 year, 2 months ago

Selected Answer: C

I would recommend option C: Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.

AWS Network Firewall is a managed firewall service that provides filtering for both inbound and outbound network traffic. It allows you to create rules for traffic inspection and filtering, which can help protect your production VPC.

Option A: Amazon GuardDuty is a threat detection service, not a traffic inspection or filtering service.

Option B: Traffic Mirroring is a feature that allows you to replicate and send a copy of network traffic from a VPC to another VPC or on-premises location. It is not a service that performs traffic inspection or filtering.

Option D: AWS Firewall Manager is a security management service that helps you to centrally configure and manage firewalls across your accounts. It is not a service that performs traffic inspection or filtering.

upvoted 97 times

✉️ **Clouddon** 7 months, 3 weeks ago

Thank you for this reply

upvoted 6 times

✉️ **BoboChow** Highly Voted 1 year, 5 months ago

Selected Answer: C

I agree with C.

AWS Network Firewall is a stateful, managed network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) that you created in Amazon Virtual Private Cloud (Amazon VPC). With Network Firewall, you can filter traffic at the perimeter of your VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect.

upvoted 23 times

✉️ **BoboChow** 1 year, 5 months ago

And I'm not sure Traffic Mirroring can be for filtering

upvoted 3 times

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

Selected Answer: C

I didn't realize the network firewall could do inspection, but here's what the documentation says:

AWS Network Firewall supports Transport Layer Security (TLS) inspection, allowing customers to strengthen their security posture on AWS by improving visibility into encrypted traffic flows. You can use AWS Network Firewall to decrypt TLS sessions and inspect both inbound and outbound Amazon Virtual Private Cloud (VPC) traffic without the need to deploy or manage any additional network security infrastructure. Encryption and decryption happen on the same firewall instance natively, so traffic does not cross any network boundaries.

upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

Selected Answer: C

Network Firewall to define firewall rules for traffic inspection.

A: GuardDuty is not for this

B: Wrong product

D: Firewall Manager does not monitor traffic, it manages firewall

upvoted 1 times

✉  **A_jaa** 2 months, 1 week ago

Selected Answer: C

Answer-C

upvoted 1 times

✉  **danielpark99** 5 months, 2 weeks ago

Selected Answer: C

AWS Network Firewall to support from layer 3 to layer 7 protection, it is able to inspect any direction lets say vpc to vpc and outbound and inbound and even supporting direct connect and site to site vpn

upvoted 1 times

✉  **reema908516** 6 months, 2 weeks ago

Selected Answer: C

AWS Network Firewall is a managed firewall service that provides filtering for both inbound and outbound network traffic. It allows you to create rules for traffic inspection and filtering, which can help protect your production VPC.

upvoted 1 times

✉  **nmywrld** 7 months, 1 week ago

Why isn't D viable? Firewall Manager will help to provision network firewall as required if you define it in firewall manager. And it's fully managed, not requiring you to do any configuration or set up.

upvoted 1 times

✉  **pentium75** 3 months ago

Because we need a firewall, not a service that we COULD IN THEORY use to create a firewall?

upvoted 2 times

✉  **Syruis** 7 months, 2 weeks ago

Selected Answer: C

C with no doubt

upvoted 1 times

✉  **Guru4Cloud** 8 months, 1 week ago

Selected Answer: C

- AWS Network Firewall is a managed network security service that provides stateful inspection of traffic and allows you to define firewall rules to control the traffic flow in and out of your VPC.
- With AWS Network Firewall, you can create custom rule groups to define specific operations for traffic inspection and filtering.
- It can perform deep packet inspection and filtering at the network level to enforce security policies, block malicious traffic, and allow or deny traffic based on defined rules.
- By integrating AWS Network Firewall with the production VPC, you can achieve similar functionalities as the on-premises inspection server, performing traffic flow inspection and filtering.

upvoted 1 times

✉  **miki111** 8 months, 2 weeks ago

Option C MET THE REQUIREMENT

upvoted 1 times

✉  **cookieMr** 9 months, 1 week ago

Selected Answer: C

AWS Network Firewall is a managed network firewall service that allows you to define firewall rules to filter and inspect network traffic. You can create rules to define the traffic that should be allowed or blocked based on various criteria such as source/destination IP addresses, protocols, ports, and more. With AWS Network Firewall, you can implement traffic inspection and filtering capabilities within the production VPC, helping to protect the network traffic.

In the context of the given scenario, AWS Network Firewall can be a suitable choice if the company wants to implement traffic inspection and filtering directly within the VPC without the need for traffic mirroring. It provides an additional layer of security by enforcing specific rules for traffic filtering, which can help protect the production environment.

upvoted 2 times

✉  **Danni** 9 months, 1 week ago

Anyone with the contributor access, kindly help me. I'm in need of the last set of questions as a means of retake preparations.

upvoted 1 times

✉  **AJAYSINGH0807** 9 months, 3 weeks ago

B is correct answer

upvoted 2 times

✉  **mbuck2023** 9 months, 3 weeks ago

Selected Answer: B

option B with Traffic Mirroring is the most suitable solution for mirroring the traffic from the production VPC to an inspection instance or tool, allowing you to perform traffic inspection and filtering as required.

upvoted 3 times

✉  **abhishek2021** 10 months, 1 week ago

Selected Answer: C

C is correct as the option uses AWS services to fully meet the requirement.

Has the question not been asking "in the AWS cloud", option B could be a correct option too, but a costlier one though as the user has to pay for network data for every bit of traffic replication between AWS cloud and on-prem location.

upvoted 1 times

 **sbnpj** 10 months, 1 week ago

Selected Answer: B

Traffic Mirroring will allow you to inspect and filter traffic using a server, (note company had a on-premise server for Traffic filtering)

upvoted 2 times

Question #16

Topic 1

A company hosts a data lake on AWS. The data lake consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides data visualization and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access.

Which solution will meet these requirements?

- A. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles.
- B. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.
- C. Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce reports. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.
- D. Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL. Generate reports by using Amazon Athena. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

Correct Answer: D*Community vote distribution*

rodriiviru 1 year, 5 months ago

Selected Answer: B

<https://docs.aws.amazon.com/quicksight/latest/user/sharing-a-dashboard.html>
upvoted 62 times

BoboChow 1 year, 5 months ago

Agree with you
upvoted 2 times

mattlai 1 year, 5 months ago

<https://docs.aws.amazon.com/quicksight/latest/user/share-a-dashboard-grant-access-users.html>
^ more percise link
upvoted 10 times

PhucVuu 11 months, 3 weeks ago

Selected Answer: B

Keywords:
 - Data lake on AWS.
 - Consists of data in Amazon S3 and Amazon RDS for PostgreSQL.
 - The company needs a reporting solution that provides data VISUALIZATION and includes ALL the data sources within the data lake.

A - Incorrect: Amazon QuickSight only support users(standard version) and groups (enterprise version). users and groups only exists without QuickSight. QuickSight don't support IAM. We use users and groups to view the QuickSight dashboard
 B - Correct: as explained in answer A and QuickSight is used to created dashboard from S3, RDS, Redshift, Aurora, Athena, OpenSearch, Timestream
 C - Incorrect: This way don't support visulization and don't mention how to process RDS data
 D - Incorrect: This way don't support visulization and don't mention how to combine data RDS and S3
 upvoted 33 times

awsgeek75 2 months, 1 week ago

Selected Answer: B

CD: AWS Glue is ETL so not required here
 A: Doable but IAM roles is not provided for each user so this cannot be implemented
 B: Correct, QuickSight can be used for visualisation reports from S3 and RDS . Comapny's management team sounds like an appropriate role for distribution.
 upvoted 1 times

A_jaa 2 months, 1 week ago

Selected Answer: B

Answer- B
upvoted 1 times

OlaFemi 2 months, 2 weeks ago

I will go with B after watching the video on this link

upvoted 1 times

✉ **OlaFemi** 2 months, 2 weeks ago

<https://aws.amazon.com/quicksight/>

upvoted 1 times

✉ **fimlajirki** 3 months, 1 week ago

itexamstest.com

no dissclusion b :)

upvoted 2 times

✉ **jjcode** 3 months, 2 weeks ago

Going with D only because it mentions S3 permissions A and B do not.

upvoted 1 times

✉ **pentium75** 3 months ago

But they want visualizations, not reports. Thus QuickSight.

upvoted 2 times

✉ **cris93** 3 months, 4 weeks ago

Selected Answer: D

the correct answer is d:

the headers of questions A and B are wrong!

"Create an analysis in Amazon QuickSight."

quickSight does NOT create analyses, it is a dashboard that displays data via graphs

upvoted 1 times

✉ **SaurabhTiwari1** 3 months, 1 week ago

Correct answer is B.

Amazon QuickSight is a business analytics tool that can connect to various data sources, including Amazon S3 and Amazon RDS for PostgreSQL. By creating an analysis in Amazon QuickSight, you can connect to all the data sources within the data lake.

upvoted 2 times

✉ **Hamso** 3 months ago

Actually it can <https://docs.aws.amazon.com/quicksight/latest/user/how-quicksight-works.html>

upvoted 1 times

✉ **Ndlesty** 4 months, 1 week ago

Selected Answer: B

QuickSight supports users (standard) and groups (Enterprise), no support for IAM.

Other keywords: VISUALIZATION

upvoted 1 times

✉ **aptx4869** 5 months ago

Selected Answer: B

<https://docs.aws.amazon.com/quicksight/latest/user/sharing-a-dashboard.html>

upvoted 1 times

✉ **Ruffyit** 5 months ago

Explanation:

Option B involves using Amazon QuickSight, which is a business intelligence tool provided by AWS for data visualization and reporting. With this option, you can connect all the data sources within the data lake, including Amazon S3 and Amazon RDS for PostgreSQL. You can create datasets within QuickSight that pull data from these sources.

The solution allows you to publish dashboards in Amazon QuickSight, which will provide the required data visualization capabilities. To control access, you can use appropriate IAM (Identity and Access Management) roles, assigning full access only to the company's management team and limiting access for the rest of the company. You can share the dashboards selectively with the users and groups that need access.

upvoted 1 times

✉ **danielpark99** 5 months, 2 weeks ago

Selected Answer: B

quicksight can share to all users, group email and a specific email with remaining access

glue has limited access so this cannot be a way to share to all users.

upvoted 1 times

✉ **IdanAWS** 5 months, 3 weeks ago

My opinion is divided here, and I will explain:

Option C can be correct because glue crawler is used to access S3, and athena federated query is used to access RDS.

My problem with answer C is that it says:

"Generate Reports by using athena"

And I think that is not true. athena alone does not generate reports, it has to integrate with services such as quickSight and then it generates

reports, therefore the answer is not written properly and I think C is a mistake.

Since C is wrong I think B is the correct answer.

upvoted 1 times

 **oddnoises** 6 months ago

For anyone wondering how to know what answers to pick when the voted answer and "official" answer are different:

Ask ChatGPT the question without giving it the answer choices. This will give you an idea of what the best answer is and a thorough explanation to help your learning

upvoted 8 times

 **MakaylaLearns** 6 months, 3 weeks ago

Hey, I made a video to quickly teach you what AWS Glue is

<https://youtube.com/shorts/ECynBsEaWKo?feature=share>

upvoted 1 times

 **Meytiam** 6 months, 4 weeks ago

Selected Answer: B

Option D does involve useful components like AWS Glue and Amazon Athena, which can be great for data processing and querying. However, given the emphasis on data visualization, limited access, and user-friendliness, option B (Amazon QuickSight) still seems more suitable for this particular scenario.

upvoted 2 times

 **hsinchang** 8 months ago

Selected Answer: B

An IAM role is associated with AWS resources instead of a specific person or group, so not A.

In C and D no visualization.

So B.

upvoted 2 times

Question #17

Topic 1

A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket. What should the solutions architect do to meet this requirement?

- A. Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.
- B. Create an IAM policy that grants access to the S3 bucket. Attach the policy to the EC2 instances.
- C. Create an IAM group that grants access to the S3 bucket. Attach the group to the EC2 instances.
- D. Create an IAM user that grants access to the S3 bucket. Attach the user account to the EC2 instances.

Correct Answer: A

Community vote distribution



A (99%)

 **sba21**  1 year, 5 months ago

Selected Answer: A

Always remember that you should associate IAM roles to EC2 instances
upvoted 75 times

 **Buruguduystunstugudunstuy**  1 year, 2 months ago

Selected Answer: A

The correct option to meet this requirement is A: Create an IAM role that grants access to the S3 bucket and attach the role to the EC2 instances.

An IAM role is an AWS resource that allows you to delegate access to AWS resources and services. You can create an IAM role that grants access to the S3 bucket and then attach the role to the EC2 instances. This will allow the EC2 instances to access the S3 bucket and the documents stored within it.

Option B is incorrect because an IAM policy is used to define permissions for an IAM user or group, not for an EC2 instance.

Option C is incorrect because an IAM group is used to group together IAM users and policies, not to grant access to resources.

Option D is incorrect because an IAM user is used to represent a person or service that interacts with AWS resources, not to grant access to resources.
upvoted 51 times

 **A_jaa**  2 months, 1 week ago

Selected Answer: A

Answer-A

upvoted 1 times

 **thewalker** 2 months, 2 weeks ago

Selected Answer: A

Below is the response from Amazon Q:

To access S3 from an EC2 instance, you need to create an IAM role and associate that role with the EC2 instance. Here are the basic steps:

1. Create an IAM role and attach the AmazonS3ReadOnlyAccess or AmazonS3FullAccess managed policy to grant S3 access.
2. Launch the EC2 instance and select the IAM role you created during launch.
3. The instance will now have the permissions defined in the IAM role and you can access S3 from the instance.

upvoted 1 times

 **thewalker** 2 months, 2 weeks ago

Some key points:

1. Attaching an IAM role is preferred over creating a resource-based policy for S3 access from EC2 as it provides centralized access management.
2. The instance will need internet access to communicate with S3. Make sure the associated security group and NACL rules allow outbound internet access.
3. Check AWS documentation for latest steps to create and associate an IAM role with an EC2 instance. The console and CLI provide options to automate this process.

Sources:

[1] How can I grant my Amazon EC2 instance access to an Amazon S3 bucket? (<https://repost.aws/knowledge-center/ec2-instance-access-s3-bucket>)

[2] How can I troubleshoot access denied or unauthorized operation errors with an IAM policy? (<https://repost.aws/knowledge-center/troubleshoot-iam-policy-issues>)

upvoted 1 times

 **jjcode** 3 months, 2 weeks ago

Strangely straight forward, Almost had me confused.
upvoted 1 times

 **GabrielSGoncalves** 4 months, 3 weeks ago

Selected Answer: A

For sure
upvoted 1 times

 **Ruffyit** 5 months ago

The correct option to meet this requirement is A: Create an IAM role that grants access to the S3 bucket and attach the role to the EC2 instances.

An IAM role is an AWS resource that allows you to delegate access to AWS resources and services. You can create an IAM role that grants access to the S3 bucket and then attach the role to the EC2 instances. This will allow the EC2 instances to access the S3 bucket and the documents stored within it.

Option B is incorrect because an IAM policy is used to define permissions for an IAM user or group, not for an EC2 instance.

Option C is incorrect because an IAM group is used to group together IAM users and policies, not to grant access to resources.

Option D is incorrect because an IAM user is used to represent a person or service that interacts with AWS resources, not to grant access to resources.

upvoted 1 times

 **danielpark99** 5 months, 2 weeks ago

Selected Answer: A

EC2 instances should be associated with IAM roles.
Policies can be applying to users and groups can help to apply multiple roles.
upvoted 1 times

 **Abdou1604** 7 months, 2 weeks ago

Option B may work but ,
suggests creating an IAM policy directly and attaching it to the EC2 instances. While this might work, it's not the recommended approach. Using an IAM role is more secure and manageable.
upvoted 1 times

 **Guru4Cloud** 8 months, 1 week ago

Selected Answer: A

Always remember that you should associate IAM roles to EC2 instances.
An IAM role is an AWS resource that allows you to delegate access to AWS resources and services. You can create an IAM role that grants access to the S3 bucket and then attach the role to the EC2 instances. This will allow the EC2 instances to access the S3 bucket and the documents stored within it.
upvoted 1 times

 **Rexino** 8 months, 1 week ago

Selected Answer: A

IAM roles should be associated to EC2 instance
upvoted 2 times

 **miki111** 8 months, 2 weeks ago

Option A MET THE REQUIREMENT
upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: A

Option A is the correct approach because IAM roles are designed to provide temporary credentials to AWS resources such as EC2 instances. By creating an IAM role, you can define the necessary permissions and policies that allow the EC2 instances to access the S3 bucket securely.
Attaching the IAM role to the EC2 instances will automatically provide the necessary credentials to access the S3 bucket without the need for explicit access keys or secrets.

Option B is not recommended in this case because IAM policies alone cannot be directly attached to EC2 instances. Policies are usually attached to IAM users, groups, or roles.

Option C is not the most appropriate choice because IAM groups are used to manage collections of IAM users and their permissions, rather than granting access to specific resources like S3 buckets.

Option D is not the optimal solution because IAM users are intended for individual user accounts and are not the recommended approach for granting access to resources within EC2 instances.

upvoted 3 times

 **big0007** 10 months, 1 week ago

IAM Roles manage who/what has access to your AWS resources, whereas IAM policies control their permissions.

Therefore, a Policy alone is useless without an active IAM Role or IAM User.

upvoted 1 times

👤 **cheese929** 10 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

👤 **zoblazo** 11 months, 2 weeks ago

Selected Answer: A

always role for ec2 instance

upvoted 1 times

👤 **PhucVuu** 11 months, 3 weeks ago

Keywords: EC2 instances can access the S3 bucket.

A: Correct - IAM role is used to grant access for AWS services like EC2, Lambda,...

B: Incorrect - IAM policy only apply for users cannot attach it to EC2 (AWS service).

C: Incorrect - IAM group is used to group of permission and attach to list of users.

D: Incorrect - To make EC2 work we need access key and secret access key but not user account. But even when we use access key and secret access key of user it's not recommended because anyone can access EC2 instance can get your access key and secret access key and get all permission from the owner. The secure way is using IAM role which we just specify enough role for EC2 instance.

upvoted 4 times

Question #18

Topic 1

An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.

A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically. Which combination of actions will meet these requirements? (Choose two.)

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.
- B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.
- C. Configure the Lambda function to monitor the S3 bucket for new uploads. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed.
- D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function.
- E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket. When an image is uploaded, send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing.

Correct Answer: AB

Community vote distribution

AB (99%)

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

Selected Answer: AB

To design a solution that uses durable, stateless components to process images automatically, a solutions architect could consider the following actions:

Option A involves creating an SQS queue and configuring the S3 bucket to send a notification to the queue when an image is uploaded. This allows the application to decouple the image upload process from the image processing process and ensures that the image processing process is triggered automatically when a new image is uploaded.

Option B involves configuring the Lambda function to use the SQS queue as the invocation source. When the SQS message is successfully processed, the message is deleted from the queue. This ensures that the Lambda function is invoked only once per image and that the image is not processed multiple times.

upvoted 28 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Option C is incorrect because it involves storing state (the file name) in memory, which is not a durable or scalable solution.

Option D is incorrect because it involves launching an EC2 instance to monitor the SQS queue, which is not a stateless solution.

Option E is incorrect because it involves using Amazon EventBridge (formerly Amazon CloudWatch Events) to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic, which is not related to the image processing process.

upvoted 20 times

 **hsinchang** 8 months ago

So storing states invokes the stateless principle, nice understanding!

upvoted 2 times

 **op22233** 5 months, 2 weeks ago

A stateless system sends a request to the server and relays the response (or the state) back without storing any information. On the other hand, stateful systems expect a response, track information, and resend the request if no response is received

upvoted 1 times

 **sba21** Highly Voted  1 year, 5 months ago

Selected Answer: AB

It looks like A-B

upvoted 15 times

 **han.ds** Most Recent  1 month ago

Selected Answer: AB

A/B make the most sense and in practice this works, I've done it.

upvoted 2 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: AB

Answer- A,B

upvoted 1 times

 **mohamedsambo** 2 months, 2 weeks ago

I can not understand why it is not as simple like s3-1 event destination to notify the lambda function to process and upload to s3-2
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html> ?

upvoted 1 times

 **DigitalDanny** 3 months, 2 weeks ago

Selected Answer: AB

A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.

B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.

Explanation:

A (SQS Queue): Using SQS to decouple the S3 bucket from the processing components provides durability and scalability. When an image is uploaded, a notification is sent to the SQS queue.

B (Lambda with SQS Trigger): Configuring the Lambda function to use the SQS queue as the invocation source allows for stateless and scalable image processing. Lambda can be triggered by messages in the SQS queue, and upon successful processing, the message can be deleted, ensuring that each message (image) is processed once.

This combination ensures a durable, stateless, and scalable architecture for processing images automatically in response to user uploads.
 upvoted 1 times

 **Gulbakyt** 4 months, 2 weeks ago

Anybody that would like to share their contributor access with me ? My email is srbassovagulbakyty@gmail.com
 Any help would be appreciated.

upvoted 2 times

 **Nava702** 6 months, 3 weeks ago

Anybody that would like to share their contributor access with me ? My email is dinkanisgod@gmail.com
 Any help would be appreciated.

upvoted 1 times

 **Guru4Cloud** 8 months, 1 week ago

Selected Answer: AB

Explanation:

Option A: By creating an Amazon SQS queue and configuring the S3 bucket to send a notification to the SQS queue when an image is uploaded, the system establishes a durable and scalable way to handle incoming image processing tasks.

Option B: Configuring the Lambda function to use the SQS queue as the invocation source allows it to retrieve messages from the queue and process them in a stateless manner. After successfully processing the image, the Lambda function can delete the message from the queue to avoid duplicate processing.

upvoted 1 times

 **miki111** 8 months, 2 weeks ago

Option AB MET THE REQUIREMENT

upvoted 1 times

 **RupeC** 8 months, 2 weeks ago

Selected Answer: AB

D and E are distractions. C seems a valid solution. However, as you have to select two, A and B are the only two that work in conjunction with each other.

upvoted 2 times

 **tester0071** 8 months, 2 weeks ago

Selected Answer: AB

A and B are optimal solutions

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: AB

Option A is a correct because it allows for decoupling between the image upload process and image processing. By configuring S3 to send a notification to SQS, image upload event is recorded and can be processed independently by microservice.

Option B is also a correct because it ensures that Lambda is triggered by messages in SQS. Lambda can retrieve image information from SQS, process and compress image, and store compressed image in a different S3. Once processing is successful, Lambda can delete processed message from SQS, indicating that image has been processed.

Option C is not recommended because it introduces a stateful approach by using a text file to keep track of processed images.

Option D is not optimal solution as it introduces unnecessary complexity by involving an EC2 to monitor SQS and maintain a text file.

Option E is not directly related to requirement of processing images automatically. Although EventBridge and SNS can be useful for event notifications and further processing, they don't provide the same level of durability and scalability as SQS.

upvoted 5 times

 **beginnercloud** 10 months, 1 week ago

Selected Answer: AB

Option A nad B

upvoted 1 times

 **cheese929** 10 months, 2 weeks ago

Selected Answer: AB

A and B

upvoted 1 times

 **PhucVuu** 11 months, 3 weeks ago

Selected Answer: AB

Keywords:

- Store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function.
- Durable, stateless components to process the images automatically

A,B: Correct - SQS has message retention function(store message) default 4 days(can increase update 14 days) so that you can re-run lambda if there are any errors when processing the images.

C: Incorrect - Lambda function just run the request then stop, the max tmeout is 15 mins. So we cannot store data in the ram of Lambda function.

D: Incorrect - we can trigger Lambda directly from SQS no need EC2 instance in this case

E: Incorrect - It kinds of manually step -> the owner has to read email then process it :))

upvoted 4 times

 **linux_admin** 12 months ago

Selected Answer: AB

A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.

B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.

upvoted 2 times

Question #19

Topic 1

A company has a three-tier web application that is deployed on AWS. The web servers are deployed in a public subnet in a VPC. The application servers and database servers are deployed in private subnets in the same VPC. The company has deployed a third-party virtual firewall appliance from AWS Marketplace in an inspection VPC. The appliance is configured with an IP interface that can accept IP packets.

A solutions architect needs to integrate the web application with the appliance to inspect all traffic to the application before the traffic reaches the web server.

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

- A. Create a Network Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
- B. Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
- C. Deploy a transit gateway in the inspection VPC and configure route tables to route the incoming packets through the transit gateway.
- D. Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

Correct Answer: B*Community vote distribution*

CloudGuru99 Highly Voted 1 year, 5 months ago

Answer is D . Use Gateway Load balancer

REF: <https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-network-traffic-inspection-using-aws-gateway-load-balancer/>
upvoted 43 times

pm2229 Highly Voted 1 year, 4 months ago

It's D, Coz.. Gateway Load Balancer is a new type of load balancer that operates at layer 3 of the OSI model and is built on Hyperplane, which is capable of handling several thousands of connections per second. Gateway Load Balancer endpoints are configured in spoke VPCs originating or receiving traffic from the Internet. This architecture allows you to perform inline inspection of traffic from multiple spoke VPCs in a simplified and scalable fashion while still centralizing your virtual appliances.

upvoted 39 times

dangvanduc90 Most Recent 1 week, 6 days ago

Selected Answer: A

just public subnet and LEAST overhead

upvoted 1 times

awsgEEK75 2 months, 1 week ago

Selected Answer: D

Literally discussed over here:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html>

upvoted 4 times

A_jaa 2 months, 1 week ago

Selected Answer: D

Answer-D

upvoted 1 times

OlaFemi 2 months, 2 weeks ago

I'm choosing D, based on "A Gateway Load Balancer routes traffic to third-party virtual appliances. It is ideal for incorporating a third-party appliance, such as a network firewall, into your network traffic in a scalable and easy-to-manage way."

upvoted 1 times

app12 2 months, 2 weeks ago

We have 3 VPCs:

Inspection --> Public --> Private

In the Inspection VPC we have only the firewall which should then direct the traffic towards the Public VPC. So in any case the firewall is the only endpoint for incoming traffic so you don't need Load balancer in front of it.

So if I understand correctly the setup should be:

InspectionVPC(Firewall) --> Load Balancer --> PublicVPC(WebServers) --> PrivateVPC(DB Servers)

So answer B looks correct to me.

upvoted 1 times

NZaf985 4 weeks, 1 day ago

Wrong there are only 2 VPC's in this example. Don't confuse VPC's with Subnets.

upvoted 1 times

✉️ **viru** 3 months, 1 week ago

Selected Answer: D

Gateway load balancer when inline virtual appliance load balancing
upvoted 1 times

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

Selected Answer: D

Gateway Load Balancer (GWLB): GWLB is designed for deploying third-party appliances and provides a scalable and easy way to route traffic through appliances. It operates at the network layer and can handle both TCP and UDP traffic.

Operational Overhead: Deploying a GWLB in the inspection VPC and creating an endpoint involves less operational overhead compared to managing Load Balancers in the application's VPC. It allows for centralized management of the inspection process.

This solution ensures that all traffic is routed through the Gateway Load Balancer for inspection before reaching the web servers, providing a scalable and efficient way to integrate the third-party virtual firewall appliance

upvoted 3 times

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

D: 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

✉️ **leosmal** 4 months ago

Selected Answer: D

Gateway load balancer is the answer
upvoted 1 times

✉️ **Ruffyit** 5 months ago

Organizations use next-generation firewalls (NGFW) and intrusion prevention systems (IPS) as part of their defense in depth strategy. In an on-premises network, these often take the form of dedicated hardware or software or virtual "appliances." As companies move to the cloud, they want to add virtual appliances to their AWS environments. While spinning up these appliances from the AWS Marketplace is a relatively straight forward process, architecting for high availability and scalability are not always easy. The new AWS Gateway Load Balancer (GWLB) service is designed specifically to address these architectural challenges and make deploying, scaling, and running virtual appliances easier.

upvoted 1 times

✉️ **Ruffyit** 5 months ago

D. GAteway load balancer
upvoted 1 times

✉️ **rlamberti** 5 months, 1 week ago

Selected Answer: A

No one said that the Inspection VPC has a public subnet, so the more feasible and least overhead answer is using a NLB to receive incoming internet traffic and route to the inspection appliance.

upvoted 1 times

✉️ **danielpark99** 5 months, 2 weeks ago

Selected Answer: D

Gateway load balancer can support to deploy, scale and manager 3rd party network virtual appliances in aws, the gateway to take all traffic from the users and inspect to pass to destination to the applications

upvoted 4 times

✉️ **David_Ang** 6 months ago

Selected Answer: A

the key part is the LEAST overhead, and answer "D" adds more complexity and cost, "A" is the most correct answer
upvoted 2 times

✉️ **jonsnow1210** 6 months, 1 week ago

Selected Answer: D

Answer is D . Use Gateway Load balancer
upvoted 1 times

Question #20

Topic 1

A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS Region. The data is stored in Amazon EC2 instances on Amazon Elastic Block Store (Amazon EBS) volumes. Modifications to the cloned data must not affect the production environment. The software that accesses this data requires consistently high I/O performance.

A solutions architect needs to minimize the time that is required to clone the production data into the test environment.

Which solution will meet these requirements?

- A. Take EBS snapshots of the production EBS volumes. Restore the snapshots onto EC2 instance store volumes in the test environment.
- B. Configure the production EBS volumes to use the EBS Multi-Attach feature. Take EBS snapshots of the production EBS volumes. Attach the production EBS volumes to the EC2 instances in the test environment.
- C. Take EBS snapshots of the production EBS volumes. Create and initialize new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.
- D. Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.

Correct Answer: D

Community vote distribution

D (92%) 6%

✉  **UWSFish**  1 year, 5 months ago

Selected Answer: D

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-fast-snapshot-restore.html>

Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation. This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance.

upvoted 37 times

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

Selected Answer: D

Keywords:

- Modifications to the cloned data must not affect the production environment.
- Minimize the time that is required to clone the production data into the test environment.

A: Incorrect - we can do this But it is not minimize the time as requirement.

B: Incorrect - This approach use same EBS volumes for producion and test. If we modify test then it will be affected prodution environment.

C: Incorrect - EBS snapshot will create new EBS volumes. It can not restore from existing volumes.

D: Correct - Turn on the EBS fast snapshot restore feature on the EBS snapshots -> no latency on first use

upvoted 21 times

✉  **1dfed2b**  2 weeks, 3 days ago

Selected Answer: C

<https://docs.aws.amazon.com/ebs/latest/userguide/ebs-restoring-volume.html>

Its C. reate a new volume from the snapshot. Use the create-volume command. For --snapshot-id, specify the ID of the snapshot to use. For --availability-zone, specify the same Availability Zone as the instance. Configure the remaining parameters as needed.

upvoted 1 times

✉  **Isomas** 1 month, 1 week ago

Answer is D because volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance.

Volumes created from normal snapshots will take time to initialize

upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

Selected Answer: D

A: Can work but long cloning time

B: Wrong as multi attach will mean changes by test will affect production

C: Slow

D: Fast restore makes this a quicker option

upvoted 1 times

✉  **A_jaa** 2 months, 1 week ago

Selected Answer: D

Answer-D

upvoted 1 times

 **Ruffyit** 5 months ago

Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation. This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance.

upvoted 1 times

 **ukivanlampli** 7 months, 2 weeks ago

Selected Answer: A
why not A? high I/O, no need durability
upvoted 1 times

 **JackLo** 6 months, 2 weeks ago

Although it is test environment, its data should be durable
upvoted 3 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected Answer: D
Needs to minimize the time that is required to clone the production data into the test environment = EBS fast snapshot restore feature
upvoted 1 times

 **Anil_Awasthi** 8 months ago

Selected Answer: C
Option C provides an effective solution for cloning large amounts of production data into a test environment with minimized time, high I/O performance, and without affecting the production environment.
upvoted 1 times

 **pentium75** 3 months ago

But you don't need a new, empty volume, you need a restore of the PROD snapshot. Thus D.
upvoted 2 times

 **Guru4Cloud** 8 months, 1 week ago

Selected Answer: D
The correct answer is D.
Here is a step-by-step explanation of how to clone production data into a test environment using EBS snapshots:
Take EBS snapshots of the production EBS volumes.
Turn on the EBS fast snapshot restore feature on the EBS snapshots.
Restore the snapshots into new EBS volumes.
Attach the new EBS volumes to EC2 instances in the test environment.
The EBS fast snapshot restore feature allows you to restore snapshots more quickly than the default method. This is because the feature uses a process called parallel restore, which allows multiple EBS volumes to be restored at the same time.
The EBS fast snapshot restore feature is only available for EBS snapshots that are created in the same AWS Region as the EC2 instances that you are using to restore the snapshots.
upvoted 5 times

 **Thornessen** 8 months, 2 weeks ago

For consistently high IO, option A is the solution. Instance store has the highest IO
upvoted 1 times

 **idanr391** 8 months, 2 weeks ago

Its not, D its the solution. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-fast-snapshot-restore.html>
upvoted 1 times

 **miki111** 8 months, 2 weeks ago

Option D is the ideal answer.
upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: D
Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.
Enabling the EBS fast snapshot restore feature allows you to restore EBS snapshots into new EBS volumes almost instantly, without needing to wait for the data to be fully copied from the snapshot. This significantly reduces the time required to clone the production data.

By taking EBS snapshots of the production EBS volumes and restoring them into new EBS volumes in the test environment, you can ensure that the cloned data is separate and does not affect the production environment. Attaching the new EBS volumes to the EC2 instances in the test environment allows you to access the cloned data.

upvoted 2 times

 **TienHuynh** 9 months, 2 weeks ago

Selected Answer: D
Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation. This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance.

upvoted 1 times

 **cheese929** 10 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **Abrar2022** 10 months, 2 weeks ago

You can use EBS Fast Snapshot restore feature to restore EBS snapshots to a new EBS volume with minimal downtime.

upvoted 1 times

Question #21

Topic 1

An ecommerce company wants to launch a one-deal-a-day website on AWS. Each day will feature exactly one product on sale for a period of 24 hours. The company wants to be able to handle millions of requests each hour with millisecond latency during peak hours. Which solution will meet these requirements with the LEAST operational overhead?

- A. Use Amazon S3 to host the full website in different S3 buckets. Add Amazon CloudFront distributions. Set the S3 buckets as origins for the distributions. Store the order data in Amazon S3.
- B. Deploy the full website on Amazon EC2 instances that run in Auto Scaling groups across multiple Availability Zones. Add an Application Load Balancer (ALB) to distribute the website traffic. Add another ALB for the backend APIs. Store the data in Amazon RDS for MySQL.
- C. Migrate the full application to run in containers. Host the containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use the Kubernetes Cluster Autoscaler to increase and decrease the number of pods to process bursts in traffic. Store the data in Amazon RDS for MySQL.
- D. Use an Amazon S3 bucket to host the website's static content. Deploy an Amazon CloudFront distribution. Set the S3 bucket as the origin. Use Amazon API Gateway and AWS Lambda functions for the backend APIs. Store the data in Amazon DynamoDB.

Correct Answer: D

Community vote distribution

D (100%)

✉️  **Sinaneos**  1 year, 5 months ago

Selected Answer: D

D because all of the components are infinitely scalable dynamoDB, API Gateway, Lambda, and of course s3+cloudfront
upvoted 38 times

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

Selected Answer: D

The solution that will meet these requirements with the least operational overhead is D: Use an Amazon S3 bucket to host the website's static content, deploy an Amazon CloudFront distribution, set the S3 bucket as the origin, and use Amazon API Gateway and AWS Lambda functions for the backend APIs. Store the data in Amazon DynamoDB.

Using Amazon S3 to host static content and Amazon CloudFront to distribute the content can provide high performance and scale for websites with millions of requests each hour. Amazon API Gateway and AWS Lambda can be used to build scalable and highly available backend APIs to support the website, and Amazon DynamoDB can be used to store the data. This solution requires minimal operational overhead as it leverages fully managed services that automatically scale to meet demand.

upvoted 16 times

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

Option A is incorrect because using multiple S3 buckets to host the full website would not provide the required performance and scale for millions of requests each hour with millisecond latency.

Option B is incorrect because deploying the full website on EC2 instances and using an Application Load Balancer (ALB) and an RDS database would require more operational overhead to maintain and scale the infrastructure.

Option C is incorrect because while deploying the application in containers and hosting them on Amazon Elastic Kubernetes Service (EKS) can provide high performance and scale, it would require more operational overhead to maintain and scale the infrastructure compared to using fully managed services like S3 and CloudFront.

upvoted 19 times

✉️  **awsgeek75**  2 months, 1 week ago

Selected Answer: D

Least operational overhead is only possible with managed services that deliver the required solution.

A: Cannot store order data in S3 as there is no processing in S3

B: Overhead of EC2 and RDS and ALB, too many moving parts

C: Container management is overhead and RDS too

D: S3 for static is best practice. CloudFront helps with scaling. API GW with Lambda is fully managed. DynamoDB for transactions is managed scalable solution.

upvoted 1 times

✉️  **A_jaa** 2 months, 1 week ago

Selected Answer: D

Answer-D

upvoted 1 times

✉  **bujuman** 3 months ago

Selected Answer: D

D is the best answer for least operation
upvoted 1 times

✉  **ddement0r** 3 months, 2 weeks ago

Selected Answer: D

D because it is the most logical solution
upvoted 1 times

✉  **Avirexirex** 3 months, 3 weeks ago

Selected Answer: D

correct answer
upvoted 1 times

✉  **numark** 3 months, 3 weeks ago

So in this question, how do you know FOR SURE that the website is static because it does not give you any clues. I know the API gateway makes the most sense with "millions of requests each hour", but it's very vague and leaves a grey area if the web site is static or not.
upvoted 1 times

✉  **Charumathi** 2 months, 2 weeks ago

1 deal a day, which is a static content for 24 hours.
upvoted 1 times

✉  **Ruffyt** 5 months ago

Using Amazon S3 to host static content and Amazon CloudFront to distribute the content can provide high performance and scale for websites with millions of requests each hour. Amazon API Gateway and AWS Lambda can be used to build scalable and highly available backend APIs to support the website, and Amazon DynamoDB can be used to store the data. This solution requires minimal operational overhead as it leverages fully managed services that automatically scale to meet demand.

upvoted 1 times

✉  **danielpark99** 5 months, 2 weeks ago

Selected Answer: D

static cache in CloudFront can help to handle millions traffic and every 24 hours data can be in store DynamoDB to maintain data for past traffic to get analyzed
upvoted 1 times

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

Selected Answer: D

Autoscale with least Ops = AWS managed services: Dynamo DB, API Gateway, Lambda, S3, CF.
upvoted 2 times

✉  **hsinchang** 8 months ago

So services fully managed by AWS usually deliver less operational overhead?
upvoted 2 times

✉  **Guru4Cloud** 8 months, 1 week ago

Selected Answer: D

Option D leverages various serverless and managed services, minimizing the operational overhead compared to other options. The auto-scaling capabilities of Lambda, API Gateway, and DynamoDB ensure the system can handle the required peak traffic without requiring manual intervention in scaling infrastructure
upvoted 2 times

✉  **james2033** 8 months, 1 week ago

Selected Answer: D

Answer A "host the full website in different S3 buckets", remove A.

Answer B "Deploy full website on EC2", remove B.

Answer C, use Kubernetes is quite overhead, Amazon DynamoDB faster than Amazon RDS for MySQL.

Answer D is suitable in technical architect design, with Amazon S3, Amazon CloudFront, Amazon API Gateway, AWS Lambda, Amazon DynamoDB. for "LEAD operational overhead" (not mean migration/re-architect overhead, it is operational). Choose D.
upvoted 1 times

✉  **miki111** 8 months, 1 week ago

Option D is the right answer for this.
upvoted 1 times

✉  **cookieMr** 9 months, 1 week ago

Selected Answer: D

Use an Amazon S3 bucket to host the website's static content. Deploy an Amazon CloudFront distribution. Set the S3 bucket as the origin. Use Amazon API Gateway and AWS Lambda functions for the backend APIs. Store the data in Amazon DynamoDB.

This solution leverages the scalability, low latency, and operational ease provided by AWS services.

This solution minimizes operational overhead because it leverages managed services, eliminating the need for manual scaling or management of infrastructure. It also provides the required scalability and low-latency response times to handle peak-hour traffic effectively.

Options A, B, and C involve more operational overhead and management responsibilities, such as managing EC2 instances, Auto Scaling groups, RDS for MySQL, containers, and Kubernetes clusters. These options require more manual configuration and maintenance compared to the serverless and managed services approach provided by option D.

upvoted 3 times

 **Globus777** 9 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

Question #22

Topic 1

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: B

Community vote distribution

B (100%)

✉  **123jh10**  1 year, 5 months ago

Selected Answer: B

"unpredictable pattern" - always go for Intelligent Tiering of S3
It also meets the resiliency requirement: "S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, and S3 Glacier Deep Archive redundantly store objects on multiple devices across a minimum of three Availability Zones in an AWS Region" <https://docs.aws.amazon.com/AmazonS3/latest/userguide/DataDurability.html>
upvoted 36 times

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

Selected Answer: B

The storage option that meets these requirements is B: S3 Intelligent-Tiering.

Amazon S3 Intelligent Tiering is a storage class that automatically moves data to the most cost-effective storage tier based on access patterns. It can store objects in two access tiers: the frequent access tier and the infrequent access tier. The frequent access tier is optimized for frequently accessed objects and is charged at the same rate as S3 Standard. The infrequent access tier is optimized for objects that are not accessed frequently and are charged at a lower rate than S3 Standard.

S3 Intelligent Tiering is a good choice for storing media files that are accessed frequently and infrequently in an unpredictable pattern because it automatically moves data to the most cost-effective storage tier based on access patterns, minimizing storage and retrieval costs. It is also resilient to the loss of an Availability Zone because it stores objects in multiple Availability Zones within a region.

upvoted 13 times

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

Option A, S3 Standard, is not a good choice because it does not offer the cost optimization of S3 Intelligent-Tiering.

Option C, S3 Standard-Infrequent Access (S3 Standard-IA), is not a good choice because it is optimized for infrequently accessed objects and does not offer the cost optimization of S3 Intelligent-Tiering.

Option D, S3 One Zone-Infrequent Access (S3 One Zone-IA), is not a good choice because it is not resilient to the loss of an Availability Zone. It stores objects in a single Availability Zone, making it less durable than other storage classes.

upvoted 6 times

✉  **awsgeek75**  2 months, 1 week ago

Selected Answer: B

Unpredictable pattern = Intelligent tiering

upvoted 1 times

✉  **A_jaa** 2 months, 1 week ago

Selected Answer: B

Answer-B

upvoted 1 times

✉  **bujuman** 3 months ago

Selected Answer: B

The right answer due to "unpredictable pattern"

upvoted 1 times

✉  **ddement0r** 3 months, 2 weeks ago

Selected Answer: B

B because intelligent tiering is what we choose when we don't have a pattern

upvoted 1 times

 **Ruffyit** 5 months ago

Amazon S3 Intelligent Tiering is a storage class that automatically moves data to the most cost-effective storage tier based on access patterns. It can store objects in two access tiers: the frequent access tier and the infrequent access tier. The frequent access tier is optimized for frequently accessed objects and is charged at the same rate as S3 Standard. The infrequent access tier is optimized for objects that are not accessed frequently and are charged at a lower rate than S3 Standard.

upvoted 1 times

 **awsleffe** 5 months, 3 weeks ago

(B) The question mentions that some files are accessed frequently while others are rarely accessed, and the pattern is unpredictable. This makes S3 Intelligent-Tiering a good fit because it automatically moves data between different access tiers based on how frequently they are accessed, optimizing costs.

Intelligent-Tiering is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead.

B meets the requirements

upvoted 1 times

 **reema908516** 6 months, 2 weeks ago

Selected Answer: B

Amazon S3 Intelligent Tiering is a storage class that automatically moves data to the most cost-effective storage tier based on access patterns.

upvoted 1 times

 **benacert** 6 months, 3 weeks ago

Unpredictable pattern, intelligent tiering will handle that.

B - is the answer..

upvoted 1 times

 **TariqKipkemei** 7 months, 3 weeks ago

Files are accessed in an unpredictable pattern, must minimize the costs of storing and retrieving the media files = S3 Intelligent-Tiering.

upvoted 1 times

 **Guru4Cloud** 8 months, 1 week ago

Selected Answer: B

S3 Intelligent-Tiering: This storage class is designed to optimize costs by automatically moving objects between two access tiers based on their usage patterns. It uses frequent access and infrequent access tiers. The frequently accessed objects stay in the frequent access tier, while the objects that are not accessed frequently are moved to the infrequent access tier. Intelligent-Tiering maintains high availability across AZs, just like S3 Standard, but it also helps reduce costs by moving data to the lower-cost tier when appropriate.

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option B is the right answer for this.

upvoted 1 times

 **james2033** 8 months, 2 weeks ago

Selected Answer: B

"S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, and S3 Glacier Deep Archive are all designed to sustain data in the event of the loss of an entire Amazon S3 Availability Zone." source:

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

upvoted 1 times

 **james2033** 8 months, 1 week ago

S3 Intelligent-Tiering is designed for data with changing or unknown access patterns, while S3 Standard-IA is designed for long-lived, infrequently accessed data [1]. S3 Intelligent-Tiering automatically reduces your storage costs on a granular object level by automatically moving data to the most cost-effective access tier based on access frequency, without performance impact, retrieval fees, or operational overhead [2]. However, it's important to note that by using S3 Intelligent-Tiering, you need to pay for a small object monitoring fee to keep track of access patterns to your data [3].

upvoted 1 times

 **james2033** 8 months, 1 week ago

[1] S3 Intelligent Tiering: How it Helps to Optimize Storage Costs? <https://www.stormit.cloud/blog/s3-intelligent-tiering-storage-class/>

[2] Object Storage Classes – Amazon S3. <https://aws.amazon.com/s3/storage-classes/>

[3] S3 Standard vs Intelligent Tiering – What's the difference? <https://www.beabetterdev.com/2021/10/16/s3-standard-vs-intelligent-tiering/>

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B

S3 Intelligent-Tiering is designed to optimize costs by automatically moving objects between two access tiers: frequent access and infrequent access. It uses machine learning algorithms to analyze access patterns and determine the most appropriate tier for each object.

In the given scenario, where some media files are accessed frequently while others are rarely accessed in an unpredictable pattern, S3 Intelligent-Tiering can be a suitable choice. It automatically adjusts the storage tier based on the access patterns, ensuring that frequently accessed files remain in the frequent access tier for fast retrieval, while rarely accessed files are moved to the infrequent access tier for cost savings.

Compared to S3 Standard-IA, S3 Intelligent-Tiering provides more granular cost optimization and may be more suitable if the access patterns of the media files fluctuate over time. However, it's worth noting that S3 Intelligent-Tiering may have slightly higher storage costs compared to S3 Standard-IA due to the added flexibility and automation it offers.

upvoted 3 times

 **Abrar2022** 10 months, 2 weeks ago

B - for unpredictable patterns use intelligent tiering

upvoted 1 times

 **Rahulbit34** 10 months, 4 weeks ago

B - "UNPREDICTABLE pattern" is the key

upvoted 2 times

Question #23

Topic 1

A company is storing backup files by using Amazon S3 Standard storage. The files are accessed frequently for 1 month. However, the files are not accessed after 1 month. The company must keep the files indefinitely.

Which storage solution will meet these requirements MOST cost-effectively?

- A. Configure S3 Intelligent-Tiering to automatically migrate objects.
- B. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.
- C. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 month.
- D. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 month.

Correct Answer: B*Community vote distribution*

B (98%)

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

Selected Answer: B

The storage solution that will meet these requirements most cost-effectively is B: Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.

Amazon S3 Glacier Deep Archive is a secure, durable, and extremely low-cost Amazon S3 storage class for long-term retention of data that is rarely accessed and for which retrieval times of several hours are acceptable. It is the lowest-cost storage option in Amazon S3, making it a cost-effective choice for storing backup files that are not accessed after 1 month.

You can use an S3 Lifecycle configuration to automatically transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month. This will minimize the storage costs for the backup files that are not accessed frequently.

upvoted 10 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Option A, configuring S3 Intelligent-Tiering to automatically migrate objects, is not a good choice because it is not designed for long-term storage and does not offer the cost benefits of S3 Glacier Deep Archive.

Option C, transitioning objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 month, is not a good choice because it is not the lowest-cost storage option and would not provide the cost benefits of S3 Glacier Deep Archive.

Option D, transitioning objects from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 month, is not a good choice because it is not the lowest-cost storage option and would not provide the cost benefits of S3 Glacier Deep Archive.

upvoted 4 times

 **vgchan** 1 year, 2 months ago

Also S3 Standard-IA & One Zone-IA stores the data for max of 30 days and not indefinitely.

upvoted 4 times

 **ninjawrz** Highly Voted 1 year, 5 months ago

B: Transition to Glacier deep archive for cost efficiency

upvoted 7 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: B

A: Possible but expensive

CD: One zone so no guarantee of being stored indefinitely.

B: S3GDA is cost effective indefinite storage

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: B

Answer-B

upvoted 1 times

 **RNess** 3 months, 1 week ago

It's can't be B!!

because objects that are archived to S3 Glacier Instant Retrieval and S3 Glacier Flexible Retrieval are charged for a minimum storage duration of 90 days, and S3 Glacier Deep Archive has a minimum storage duration of 180 days.

upvoted 1 times

 **pentium75** 3 months ago

But the items must be kept forever, so where's the issue with that?
upvoted 1 times

 **RNess** 2 months, 2 weeks ago

I mean, that min duration **before** can move to S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive
upvoted 1 times

 **ddement0r** 3 months, 2 weeks ago

Selected Answer: B
B because since the files should be kept but never accessed we can put them in Deep Archive
upvoted 1 times

 **Ruffyit** 5 months ago

Amazon S3 Glacier Deep Archive is a secure, durable, and extremely low-cost Amazon S3 storage class for long-term retention of data that is rarely accessed and for which retrieval times of several hours are acceptable
upvoted 1 times

 **AhmedAbdelhedi** 5 months, 3 weeks ago

Selected Answer: B
Answer is B
upvoted 1 times

 **sujanakakarla** 6 months, 4 weeks ago

Selected Answer: B
B as these files will be stored indefinitely after 1 month
upvoted 1 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected Answer: B
Files are accessed frequently for 1 month = S3 Standard. Files are not accessed after 1 month and must be kept indefinitely at low costs = S3 Glacier Deep Archive.
No requirement for low Ops but S3 Lifecycle to the rescue...whoooosh!
upvoted 1 times

 **Guru4Cloud** 8 months, 1 week ago

Selected Answer: B
Option B (Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month) is the most cost-effective storage solution for this specific scenario. It allows you to maintain accessibility for the initial 1 month while achieving significant cost savings in the long term.
upvoted 1 times

 **miki111** 8 months, 1 week ago

Option B is the right answer for this.
upvoted 1 times

 **Kaab_B** 8 months, 2 weeks ago

Selected Answer: B
Correct answer is B
upvoted 1 times

 **Debmalya_aws** 8 months, 2 weeks ago

It will be C. Can not move to Glacier directly from standard using Lifecycle
upvoted 1 times

 **bingusbongus** 8 months, 2 weeks ago

You absolutely can.
upvoted 2 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B
S3 Glacier Deep Archive is designed for long-term archival storage with very low storage costs. It offers the lowest storage prices among the storage classes in Amazon S3. However, it's important to note that accessing data from S3 Glacier Deep Archive has a significant retrieval time, ranging from several minutes to hours, which may not be suitable if you require immediate access to the backup files.

If the files need to be accessed frequently within the first month but not after that, transitioning them to S3 Glacier Deep Archive using an S3 Lifecycle configuration can provide cost savings. However, keep in mind that retrieving the files from S3 Glacier Deep Archive will have a significant time delay.
upvoted 3 times

 **MostafaWardany** 10 months, 1 week ago

Selected Answer: B
B is the correct answer

upvoted 1 times

 **beginnercloud** 10 months, 1 week ago

Selected Answer: B

B is correct answer

upvoted 1 times

Question #24

Topic 1

A company observes an increase in Amazon EC2 costs in its most recent bill. The billing team notices unwanted vertical scaling of instance types for a couple of EC2 instances. A solutions architect needs to create a graph comparing the last 2 months of EC2 costs and perform an in-depth analysis to identify the root cause of the vertical scaling.

How should the solutions architect generate the information with the LEAST operational overhead?

- A. Use AWS Budgets to create a budget report and compare EC2 costs based on instance types.
- B. Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.
- C. Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months.
- D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

Correct Answer: C

Community vote distribution



✉️ **sba21** 1 year, 5 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/68306-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 31 times

✉️ **123jh10** 1 year, 5 months ago

Selected Answer: C

The requested result is a graph, so...
 A - can't be as the result is a report
 B - can't be as it is limited to 14 days visibility and the graph has to cover 2 months
 C - seems to provide graphs and the best option available, as...
 D - could provide graphs, BUT involves operational overhead, which has been requested to be minimised.
upvoted 22 times

✉️ **lofzee** 1 year, 1 month ago

14 days? Fam, you ever logged into the console?
upvoted 12 times

✉️ **goku58** 1 year, 5 months ago

12 months data visible on Cost Explorer.
upvoted 9 times

✉️ **Udoyen** 1 year, 3 months ago

Cost Explorer, AWS prepares the data about your costs for the current month and the last 12 months: <https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>
upvoted 14 times

✉️ **Ello2023** 1 year, 1 month ago

B. This is correct because there is no limit of 14 days. Quoted from Amazon "AWS prepares the data about your costs for the current month and the last 12 months, and then calculates the forecast for the next 12 months." (<https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>).
upvoted 10 times

✉️ **vi24** 2 weeks, 4 days ago

Cost and usage report is the right tool for analyzing and understanding your bill. Cost explorer is mostly used for monitoring usage/expenditure over time to forecast and decide on more suitable plan/ package.
upvoted 1 times

✉️ **cheroh_tots** 1 month, 1 week ago

The answer is B.
 You can enable Cost Explorer for your account using this procedure on the Billing and Cost Management console. You can't enable Cost Explorer using the API. After you enable Cost Explorer, AWS prepares the data about your costs for the current month and the last 12 months, and then calculates the forecast for the next 12 months. The current month's data is available for viewing in about 24 hours. The rest of your data takes a few days longer. Cost Explorer updates your cost data at least once every 24 hours.
upvoted 1 times

✉️ **Ikki77** 1 month, 2 weeks ago

Selected Answer: B

Cost Explorer

upvoted 1 times

andryngkh86 2 months, 1 week ago

The option that provides the least operational overhead for generating a graph comparing the last 2 months of EC2 costs based on instance types is:

D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

This option leverages the AWS Cost and Usage Reports to export detailed billing information to an Amazon S3 bucket. Then, using Amazon QuickSight, you can easily create interactive graphs and perform in-depth analysis based on instance types. This approach provides flexibility and customization in analyzing the cost data with minimal operational overhead.

upvoted 1 times

awsgeek75 2 months, 1 week ago

Selected Answer: B

B is least operational overhead

A: Can't do that

C: Not granular enough

D: Too much operational overhead

upvoted 2 times

A_jaa 2 months, 1 week ago

Selected Answer: B

Answer-B

upvoted 1 times

yonwick 2 months, 2 weeks ago

Honestly... I'm mad with this kind of questions...To be honest, there are several ways to do so, but none of them will affect (in a major way) your day to day operations. I'm just saying, useless questions that adds nothing of value.

upvoted 6 times

firstpirateking 2 months, 2 weeks ago

I agree.

upvoted 2 times

boooliyooo 2 months, 3 weeks ago

Selected Answer: B

In order to clarify why some chosen C, the limitation is only meant for HOURLY COST.

"By enabling hourly granularity you can view your hourly costs up to the past 14 days to track costs during nights or off peak hours."

<https://aws.amazon.com/about-aws/whats-new/2019/11/aws-cost-explorer-supports-hourly-resource-level-granularity/>

upvoted 3 times

tipopeso 3 months ago

Selected Answer: D

Cost Explorer is a tool within AWS that allows for detailed analysis of AWS costs and usage. It provides an interactive interface where you can visualize your data, detect cost trends, and dive deeper into cost drivers. By using its granular filtering features, you can specifically look at EC2 costs, filter by instance type, and compare the costs over the last two months. This direct approach requires no additional setup or external tools and is designed for in-depth cost analysis, making it the most efficient choice for the task at hand.

upvoted 2 times

SVDK 2 months, 3 weeks ago

D is incorrect because the question says "with the LEAST overhead". Although D is a viable option it takes more effort and hence cannot be the correct answer.

upvoted 2 times

viru 3 months, 1 week ago

Selected Answer: B

Verified this in AWS console

upvoted 4 times

firstpirateking 2 months, 2 weeks ago

good job!

upvoted 1 times

byteb 3 months, 2 weeks ago

Billing and Cost management dashboard doesn't provide cost analysis feature, cost explorer does. We have granularity options there to select monthly, daily, and hourly analysis.

upvoted 2 times

awstime 3 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/cost-management/latest/userguide/ce-filtering.html>

You can filter costs by instance type using AWS Cost Explorer.

upvoted 1 times

 **bsfl** 3 months, 3 weeks ago

At an initial glance without getting deep into both it can cause confusion, but I'll try to break them down below.

AWS Billing and Cost Management provides a summarised view of spending i.e. what you spent so far this month, and the predicted end of month bill, this is quite static and gives you a high level overview of spending. In addition you can configure your billing details from here. All of these features are free to use with no charge for accessing the interface.

AWS Cost explorer on the other hand is a paid service (\$0.01 per query). By using cost explorer you can dig down into the finer details of expenditure, such as on a region, service, usage type or even tag based level. Using this you can identify costs by targeting your query to be specific enough to identify these charges. Additionally you can make use of hourly billing to get the most accurate upto date billing

upvoted 4 times

 **t0nx** 4 months ago

Selected Answer: D

D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

Explanation:

- AWS Cost and Usage Reports provide detailed billing information, including usage and costs broken down by services and resources, making it suitable for in-depth analysis.
- Sending the report to an Amazon S3 bucket allows for storage and easy access to historical data.
- Amazon QuickSight can connect to the S3 bucket and create interactive graphs, providing a more detailed and customizable analysis.
- This approach offers flexibility and control for a comprehensive analysis of EC2 costs based on instance types over the last two months with the least operational overhead.

While other options (A, B, C) provide certain capabilities, using AWS Cost and Usage Reports along with Amazon QuickSight provides a more robust and customizable solution for detailed analysis.

upvoted 3 times

 **Ruffyit** 5 months ago

B. Quoted from Amazon "AWS prepares the data about your costs for the current month and the last 12 months, and then calculates the forecast for the next 12 months." (<https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>).

upvoted 1 times

Question #25

Topic 1

A company is designing an application. The application uses an AWS Lambda function to receive information through Amazon API Gateway and to store the information in an Amazon Aurora PostgreSQL database.

During the proof-of-concept stage, the company has to increase the Lambda quotas significantly to handle the high volumes of data that the company needs to load into the database. A solutions architect must recommend a new design to improve scalability and minimize the configuration effort.

Which solution will meet these requirements?

- A. Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances. Connect the database by using native Java Database Connectivity (JDBC) drivers.
- B. Change the platform from Aurora to Amazon DynamoDB Provision a DynamoDB Accelerator (DAX) cluster. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.
- C. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).
- D. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Correct Answer: D

Community vote distribution

D (98%)

123jh10 Highly Voted 1 year, 5 months ago

Selected Answer: D

A - refactoring can be a solution, BUT requires a LOT of effort - not the answer
 B - DynamoDB is NoSQL and Aurora is SQL, so it requires a DB migration... again a LOT of effort, so no the answer
 C and D are similar in structure, but...
 C uses SNS, which would notify the 2nd Lambda function... provoking the same bottleneck... not the solution
 D uses SQS, so the 2nd lambda function can go to the queue when responsive to keep with the DB load process.
 Usually the app decoupling helps with the performance improvement by distributing load. In this case, the bottleneck is solved by using queues... so D is the answer.

upvoted 79 times

PhucVuu Highly Voted 11 months, 3 weeks ago

Selected Answer: D

Keywords:
 - Company has to increase the Lambda quotas significantly to handle the high volumes of data that the company needs to load into the database.
 - Improve scalability and minimize the configuration effort.

A: Incorrect - Lambda is Serverless and automatically scales - EC2 instance we have to create load balancer, auto scaling group,.. a lot of things. using native Java Database Connectivity (JDBC) drivers don't improve the performance.
 B: Incorrect - a lot of things to change and DynamoDB Accelerator use for cache(read) not for write.
 C: Incorrect - SNS is used for sending notifications (e-mail, SMS).
 D: Correct - with SQS we can scale application well by queuing the data.

upvoted 15 times

TheFivePips Most Recent 1 month, 1 week ago

Selected Answer: D

D. Set up two Lambda functions, one for receiving information and another for loading data into the database. Integrate them using an Amazon SQS queue. This approach allows for better scalability, maintains the serverless paradigm, and minimizes manual configuration effort. It leverages Amazon SQS as a reliable message queue between Lambda functions.

Options A and B introduce complexities and changes in architecture, while Option C introduces an additional service that may not be as suitable for decoupling processes in this scenario.

upvoted 1 times

awsgeek75 2 months, 1 week ago

Selected Answer: D

SQS will help Lambda scale even more.
 A EC2 + Tomcat will be slower than Lambda for this usecase
 B is wrong because the problem is with Lambda scaling not the DB
 C SNS is not the best option for this usecase when SQS is an option

upvoted 1 times

A_jaa 2 months, 1 week ago

Selected Answer: D

Answer-D

upvoted 1 times

 **ddement0r** 3 months, 2 weeks ago

Selected Answer: D

D : other ones just don't make sense

upvoted 1 times

 **pedestrianlove** 4 months, 1 week ago

Sorry, but the question does not make sense by itself. What are you asking for more scalability from an already scalable Lambda function?

If you're concerned about the concurrency limits of Lambda function, decoupling just doesn't make sense, since it'll keep even more lambda instances running in a given time period(including 2 phases of execution for each request, let alone the cold start issues).

If you're concerned about bottleneck database induced, that'll even be more ridiculous since you're supposed to resolve the scalability issue of the database(e.g. Aurora) instead of decoupling the Lambda function to improve the throughput of this entire data flow.

upvoted 2 times

 **mohamedsambo** 2 months, 2 weeks ago

i think it is clear that he want to enhance the lambda even more than "The default concurrency limit across all functions per region in a given account is 1,000"

cause sqs can scale and store the data till new available revoked lambda consume it

upvoted 2 times

 **Ruffyit** 5 months ago

Lambda and SQS are serverless. No involvement will be required in execution.

upvoted 2 times

 **xdkonorek2** 5 months ago

Selected Answer: B

I think B would be better solution.

How splitting one function into 2 increase scalability when company already increased service quota? Effectively they will have same compute time. Changing Aurora to DAX will shorten the time for data loads by ~100x requiring way less time for data loading, and it's most time consuming thing this lambda does. DAX has better scaling than aurora and is better fit with lambda

upvoted 2 times

 **MakaylaLearns** 6 months, 3 weeks ago

Lambda Functions: A review

Run your code in response to events

You can build chatbots using Lambda functions to process user input, execute business logic, and generate responses.

Scales automatically

They can be triggered in response to API events

Lambda functions can process files as they are uploaded to S3 buckets. This is often used for tasks like image resizing, data extraction, or file validation.

upvoted 1 times

 **learndigitalcloud** 6 months, 3 weeks ago

AWS Cost Explorer is a tool that enables you to view and analyze your costs and usage. You can explore your usage and costs using the main graph, the Cost Explorer cost and usage reports, or the Cost Explorer RI reports. You can view data for up to the last 12 months, forecast how much you're likely to spend for the next 12 months, and get recommendations for what Reserved Instances to purchase.

Ans: B is correct

<https://docs.aws.amazon.com/cost-management/latest/userguide/ce-what-is.html>

upvoted 1 times

 **doujones** 7 months, 3 weeks ago

Do you all have to take the whole practice exam on here, in order to pass AWS SAA C03

upvoted 2 times

 **TariqKipkemei** 7 months, 3 weeks ago

Increase Lambda quotas = Set up two Lambda functions. Improve scalability = Amazon Simple Queue Service.

upvoted 1 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected answer D

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option D is the right answer for this.

upvoted 1 times

 **Kaab_B** 8 months, 2 weeks ago

Selected Answer: D

Lambda and SQS are serverless. No involvement will be required in execution.

upvoted 2 times

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

This threw me off - because ideally, I see no need for two lambdas. It can be done with one: APIGW -> SQS -> Lambda.

upvoted 2 times

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

By, @cookieMr [<https://www.examtopics.com/user/cookieMr/>]

"By dividing the functionality into two Lambda functions, one for receiving the information and the other for loading it into the database, you can independently scale and optimize each function based on their specific requirements. This approach allows for more efficient resource allocation and reduces the potential impact of high volumes of data on the overall system."

upvoted 2 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: D

Option D, setting up two Lambda functions and integrating them using an SQS, would be the most suitable solution to improve scalability and minimize configuration effort in this scenario.

By dividing the functionality into two Lambda functions, one for receiving the information and the other for loading it into the database, you can independently scale and optimize each function based on their specific requirements. This approach allows for more efficient resource allocation and reduces the potential impact of high volumes of data on the overall system.

Integrating the Lambda functions using an SQS adds another layer of scalability and reliability. The receiving function can push the information to the SQS, and the loading function can retrieve messages from the queue and process them independently. This asynchronous decoupling ensures that the receiving function can handle high volumes of incoming requests without overwhelming the loading function. Additionally, SQS provides built-in retries and guarantees message durability, ensuring that no data is lost during processing.

upvoted 5 times

Question #26

Topic 1

A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets do not have unauthorized configuration changes. What should a solutions architect do to accomplish this goal?

- A. Turn on AWS Config with the appropriate rules.
- B. Turn on AWS Trusted Advisor with the appropriate checks.
- C. Turn on Amazon Inspector with the appropriate assessment template.
- D. Turn on Amazon S3 server access logging. Configure Amazon EventBridge (Amazon Cloud Watch Events).

Correct Answer: A*Community vote distribution*

A (97%)

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

Selected Answer: A

The solution that will accomplish this goal is A: Turn on AWS Config with the appropriate rules.

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. You can use AWS Config to monitor and record changes to the configuration of your Amazon S3 buckets. By turning on AWS Config and enabling the appropriate rules, you can ensure that your S3 buckets do not have unauthorized configuration changes.

upvoted 43 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

AWS Trusted Advisor (Option B) is a service that provides best practice recommendations for your AWS resources, but it does not monitor or record changes to the configuration of your S3 buckets.

Amazon Inspector (Option C) is a service that helps you assess the security and compliance of your applications. While it can be used to assess the security of your S3 buckets, it does not monitor or record changes to the configuration of your S3 buckets.

Amazon S3 server access logging (Option D) enables you to log requests made to your S3 bucket. While it can help you identify changes to your S3 bucket, it does not monitor or record changes to the configuration of your S3 bucket.

upvoted 35 times

 **gokalpkocer3** Highly Voted 1 year, 4 months ago

Configuration changes= AWS Config

upvoted 27 times

 **andyngkh86** Most Recent 2 months, 1 week ago

ChatGPT give the answer is D

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: A

Answer-A

upvoted 1 times

 **Ruffyit** 5 months ago

A: <https://aws.amazon.com/config/#:~:text=How%20it%20works-,AWS%20Config,-continually%20assesses%2C%20audits>

upvoted 1 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected Answer: A

AWS Config continually assesses, audits, and evaluates the configurations and relationships of your resources on AWS, on premises, and on other clouds. It normalizes changes into a consistent format and checks resource compliance with custom and managed rules before and after provisioning.

<https://aws.amazon.com/config/#:~:text=How%20it%20works-,AWS%20Config,-continually%20assesses%2C%20audits>

upvoted 2 times

 **Guru4Cloud** 8 months ago

Selected Answer: A

AWS Config provides a detailed inventory of the company's AWS resources and configuration history, and can be configured with rules to evaluate resource configurations for compliance with policies and best practices.

The solutions architect can enable AWS Config and configure rules specifically checking for S3 bucket settings like public access blocking, encryption settings, access control lists, etc. AWS Config will record configuration changes to S3 buckets over time, allowing the company to review

changes and be alerted about any unauthorized modifications.

By. Claude.ai

upvoted 1 times

✉ **miki111** 8 months, 1 week ago

Option A is the right answer for this.

upvoted 1 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: A

AWS Config is a service that provides a detailed view of the configuration of AWS resources in your account. By enabling AWS Config, you can capture configuration changes and maintain a record of resource configurations over time. It allows you to define rules that check for compliance with desired configurations and can generate alerts or automated actions when unauthorized changes occur.

To accomplish the goal of preventing unauthorized configuration changes in Amazon S3 buckets, you can configure AWS Config rules specifically for S3 bucket configurations. These rules can check for a variety of conditions, such as ensuring that encryption is enabled, access control policies are correctly configured, and public access is restricted.

While options B, C, and D offer valuable services for various aspects of AWS deployment, they are not specifically focused on preventing unauthorized configuration changes in Amazon S3 buckets as effectively as enabling AWS Config.

upvoted 2 times

✉ **Abrar2022** 10 months, 2 weeks ago

Don't be mistaken in thinking that it's Server access logs because that's for detailed records for requests made to S3. It's AWS Config because it records configuration changes.

upvoted 1 times

✉ **Rahulbit34** 10 months, 4 weeks ago

AWS trusted Adviser is for providing recommendation only.

For any configuration use AWS config

Inspector is for scanning for any software vulnerabilities and unintended network exposure

upvoted 1 times

✉ **PhucVuu** 11 months, 1 week ago

Selected Answer: A

To accomplish the goal of ensuring that Amazon S3 buckets do not have unauthorized configuration changes, a solutions architect should turn on AWS Config with the appropriate rules. AWS Config enables continuous monitoring and recording of AWS resource configurations, including S3 buckets. By turning on AWS Config with the appropriate rules, the solutions architect can be notified of any unauthorized changes made to the S3 bucket configurations, allowing for prompt corrective action. Options B, C, and D are not directly related to monitoring and preventing unauthorized configuration changes to Amazon S3 buckets.

upvoted 1 times

✉ **channn** 11 months, 4 weeks ago

Selected Answer: A

Key words:configuration changes

upvoted 1 times

✉ **linux_admin** 12 months ago

Selected Answer: A

Option A is the correct solution. AWS Config is a service that allows you to monitor and record changes to your AWS resources over time. You can use AWS Config to track changes to Amazon S3 buckets and their configuration settings, and set up rules to identify any unauthorized configuration changes. AWS Config can also send notifications through Amazon SNS to alert you when these changes occur.

upvoted 1 times

✉ **al64** 1 year, 1 month ago

Selected Answer: A

aws: A - aws config

upvoted 1 times

✉ **Khushna** 1 year, 1 month ago

AAAAaaaaaaaaaaaaaaaaaaaaaa

upvoted 1 times

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

Selected Answer: A

o ensure that Amazon S3 buckets do not have unauthorized configuration changes, a solutions architect should turn on AWS Config with the appropriate rules.

AWS Config is a service that provides you with a detailed view of the configuration of your AWS resources. It continuously records configuration changes to your resources and allows you to review, audit, and compare these changes over time. By turning on AWS Config and enabling the appropriate rules, you can monitor the configuration changes to your Amazon S3 buckets and receive notifications when unauthorized changes are made.

upvoted 1 times

Question #27

Topic 1

A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard. The company's product manager needs to access this dashboard periodically. The product manager does not have an AWS account. A solutions architect must provide access to the product manager by following the principle of least privilege.

Which solution will meet these requirements?

- A. Share the dashboard from the CloudWatch console. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.
- B. Create an IAM user specifically for the product manager. Attach the CloudWatchReadOnlyAccess AWS managed policy to the user. Share the new login credentials with the product manager. Share the browser URL of the correct dashboard with the product manager.
- C. Create an IAM user for the company's employees. Attach the ViewOnlyAccess AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.
- D. Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

Correct Answer: B

Community vote distribution

A (75%)

B (24%)

✉️  **masetromain**  1 year, 5 months ago

Selected Answer: A

Answer A : <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html>

Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard.

upvoted 74 times

✉️  **123jh10** 1 year, 5 months ago

Thanks for the link! No doubt A is the answer.

upvoted 6 times

✉️  **omoakin** 10 months, 1 week ago

nope! The principle of least privilege will contradict that B is the correct answer even Chat GPT says its B

upvoted 7 times

✉️  **Azure55** 4 months, 4 weeks ago

chatgpt chooses A

upvoted 2 times

✉️  **jaswantn** 1 month, 2 weeks ago

I opt for option (B); with CloudWatchReadOnlyAccess policy it is made sure that no other permission is granted, thus making it principle of least privilege. But with Option (A) , more permissions are granted by default and that too in sharable mode.

upvoted 1 times

✉️  **jaswantn** 1 month, 2 weeks ago

i change my option from B to A, after checking all the permissions that comes under CloudWatchReadOnlyAccess policy.

upvoted 1 times

✉️  **mn2013** 2 months ago

But this link also says All people who you share the dashboard with are granted these permissions for the account. If you share the dashboard publicly, then everyone who has the link to the dashboard has these permissions.

The cloudwatch:GetMetricData and ec2:DescribeTags permissions cannot be scoped down to specific metrics or EC2 instances, so the people with access to the dashboard can query all CloudWatch metrics and the names and tags of all EC2 instances in the account. If that is the case, how is the least privilege principle applicable?

upvoted 2 times

✉️  **Guru4Cloud**  8 months, 1 week ago

Selected Answer: B

Option B provides the product manager with specific access to the CloudWatch dashboard using an IAM user with the CloudWatchReadOnlyAccess policy attached. The IAM user has only read-only access to the required resources, which follows the principle of least privilege.

upvoted 12 times

 **emilyhu08** 5 months, 2 weeks ago

b has a problem for cloudwatchreadonlyacess policy, it's not only grant read access to dashboard, but other read permission for logs, insights, etc. so it does not follows the principle of least privilege. Option A only grants access to dashboard.

upvoted 11 times

 **LIORAGE** Most Recent 6 days, 20 hours ago

Answer B:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html>

When you share a dashboard, CloudWatch creates an IAM role in the account which gives the following permissions to the people who you share the dashboard with:

cloudwatch:GetInsightRuleReport
cloudwatch:GetMetricData
cloudwatch:DescribeAlarms
ec2:DescribeTags

A not provide principle of least privilege.

upvoted 1 times

 **Abhiiinav** 2 months, 1 week ago

Selected Answer: B

Option A suggests Sharing of dashboards with temporary credentials while the product manager needs to view it periodically. If your password expires, you need an extra overhead of resetting the password.

Thus option B is correct.

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html>

"Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard."

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: A

Answer-A

upvoted 1 times

 **ROBERTXLION** 2 months, 4 weeks ago

Selected Answer: B

<https://muhammadhassansaeed.medium.com/aws-certified-solutions-architect-associate-exam-dumps-with-complete-explanation-part3-5d649a3e850e>

upvoted 1 times

 **SVDK** 2 months, 3 weeks ago

His explanation is incorrect. The temporary password must be changed by the product manager and then does not expire. It's only the temp password that expires. Hence A is correct.

upvoted 1 times

 **tipopeso** 3 months ago

Selected Answer: A

This option allows the product manager to access the CloudWatch dashboard without needing an AWS account. The dashboard can be shared with the product manager via a link, which is generated by AWS and can be accessed securely. This method adheres to the principle of least privilege by granting access only to the specific dashboard required.

upvoted 2 times

 **smdrouiss** 3 months, 3 weeks ago

Selected Answer: A

I have tested it on my console, and it worked as well as I looked up into docs

upvoted 4 times

 **kt7** 4 months, 2 weeks ago

A is correct

upvoted 1 times

 **Ruffyit** 5 months ago

Answer A : <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html>

upvoted 1 times

 **danielpark99** 5 months, 2 weeks ago

Selected Answer: A

Clouwatch dashboards with people who do not have direct access to your aws account
upvoted 1 times

✉ **ABS_AWS** 5 months, 4 weeks ago

Answer is A
refer AWS doc ...

"To help manage this information access, Amazon CloudWatch has introduced CloudWatch dashboard sharing. This allows customers to easily and securely share their CloudWatch dashboards with people outside of their organization, in another business unit, or with those with no access AWS console access. This blog will demonstrate how a dashboard can be shared across the enterprise via a SAML provider in order to broker this secure access."

upvoted 3 times

✉ **David_Ang** 6 months ago

Selected Answer: B

"B" is the only correct answer because you always have to think which one is the more secure option, with "A" you are exposing the dashboard and everybody with the link can see it. is more secure and simple to give him an aws account with read only access to the dashboard.

upvoted 6 times

✉ **Examprep202324** 6 months, 3 weeks ago

When you share dashboards, you can designate who can view the dashboard in three ways:

One of which is following:--

1. Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard.

upvoted 1 times

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

New to the forum.....Just a question, has anyone gotten this exact question in the actual exam and whether or not the most voted answer was the correct one or not ?

upvoted 6 times

✉ **bojila** 7 months, 4 weeks ago

Selected Answer: A

Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard.

upvoted 1 times

Question #28

Topic 1

A company is migrating applications to AWS. The applications are deployed in different accounts. The company manages the accounts centrally by using AWS Organizations. The company's security team needs a single sign-on (SSO) solution across all the company's accounts. The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory.

Which solution will meet these requirements?

- A. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
- B. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
- C. Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.
- D. Deploy an identity provider (IdP) on premises. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

Correct Answer: A

Community vote distribution

B (77%)	A (17%)	3%
---------	---------	----

 **17Master**  1 year, 4 months ago

Selected Answer: B

Tricky question!!! forget one-way or two-way. In this scenario, AWS applications (Amazon Chime, Amazon Connect, Amazon QuickSight, AWS Single Sign-On, Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, AWS Client VPN, AWS Management Console, and AWS Transfer Family) need to be able to look up objects from the on-premises domain in order for them to function. This tells you that authentication needs to flow both ways. This scenario requires a two-way trust between the on-premises and AWS Managed Microsoft AD domains.

It is a requirement of the application

Scenario 2: <https://aws.amazon.com/es/blogs/security/everything-you-wanted-to-know-about-trusts-with-aws-managed-microsoft-ad/>
upvoted 64 times

 **pbpally** 10 months, 3 weeks ago

What I did find though was documentation that explicitly states that IAM Identity Center (successor to AWS SSO) requires a two-way trust: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_setup_trust.html

upvoted 8 times

 **pbpally** 10 months, 3 weeks ago

The problem with this is that nowhere in the question is it saying that the application needs to be able to flow back so two-way is not needed.
upvoted 3 times

 **mohamedsambo** 2 months, 2 weeks ago

AWS IAM Identity Center requires a two-way trust so that it has permissions to read user and group information from your domain to synchronize user and group metadata. IAM Identity Center uses this metadata when assigning access to permission sets or applications. User and group metadata is also used by applications for collaboration, like when you share a dashboard with another user or group. The trust from AWS Directory Service for Microsoft Active Directory to your domain permits IAM Identity Center to trust your domain for authentication. The trust in the opposite direction grants AWS permissions to read user and group metadata.

upvoted 2 times

 **KADSM**  1 year, 4 months ago

Answer B as we have AWS SSO which requires two way trust. As per documentation - A two-way trust is required for AWS Enterprise Apps such as Amazon Chime, Amazon Connect, Amazon QuickSight, AWS IAM Identity Center (successor to AWS Single Sign-On), Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, and the AWS Management Console. AWS Managed Microsoft AD must be able to query the users and groups in your self-managed AD.

Amazon EC2, Amazon RDS, and Amazon FSx will work with either a one-way or two-way trust.

upvoted 12 times

 **pbpally** 10 months, 3 weeks ago

I found the documentation that explicitly states that IAM Identity Center (successor to AWS SSO) requires a two-way trust: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_setup_trust.html

upvoted 3 times

 **awsgeek75**  2 months, 1 week ago

Selected Answer: B

I'll go for B as
A feels incomplete

C Can be done but company wants SSO, not a fill director service
D On prem already has a IDP so no.

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: B

Answer-B

upvoted 1 times

 **boooliyooo** 2 months, 3 weeks ago

Selected Answer: D

D is better and more applicable in real-world context where everyone chooses simplicity over a overhaul solution; Where Organizations may prefer to continue using their existing, trusted on-premises IdP solutions for authentication, especially if they have specific security policies or compliance requirements.

upvoted 1 times

 **Ruffyit** 5 months ago

Two-way trust or AD Connector. IAM Identity Center only works with those two.

"One-way trusts do not work with IAM Identity Center."

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

upvoted 2 times

 **rlamberti** 5 months, 1 week ago

Selected Answer: B

Two-way trust or AD Connector. IAM Identity Center only works with those two.

"One-way trusts do not work with IAM Identity Center."

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

upvoted 1 times

 **dhax12** 5 months, 2 weeks ago

From AWS Documentation:

A two-way trust is required for AWS Enterprise Apps such as Amazon Chime, Amazon Connect, Amazon QuickSight, AWS IAM Identity Center, Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, and the AWS Management Console. AWS Managed Microsoft AD must be able to query the users and groups in your self-managed AD.

Amazon EC2, Amazon RDS, and Amazon FSx will work with either a one-way or two-way trust.

upvoted 1 times

 **prabhjot** 5 months, 3 weeks ago

Option a- and why not option B -Option B, which suggests a two-way forest trust, is generally not recommended unless there are specific reasons for requiring a two-way trust, as it increases complexity and potential security risks.

upvoted 1 times

 **parrtn73** 5 months, 3 weeks ago

B

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

upvoted 1 times

 **Examprep202324** 6 months, 3 weeks ago

A two-way trust is required for AWS Enterprise Apps such as Amazon Chime, Amazon Connect, Amazon QuickSight, "AWS IAM Identity Center (successor to AWS Single Sign-On)", Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, and the AWS Management Console

upvoted 1 times

 **Yonimoni** 7 months, 1 week ago

Option B is the correct choice because it aligns with the AWS documentation, which states that a two-way trust relationship is needed between AWS Managed Microsoft AD and a self-managed AD for users to sign in with their corporate credentials to AWS services. This solution integrates AWS SSO, AWS Directory Service for Microsoft AD, and centralized account management through AWS Organizations.

Read until the end

"Create a two-way trust relationship – When two-way trust relationships are created between AWS Managed Microsoft AD and a self-managed directory in AD, users in your self-managed directory in AD can sign in with their corporate credentials to various AWS services and business applications. One-way trusts do not work with IAM Identity Center."

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

upvoted 1 times

 **Raggz** 7 months, 1 week ago

Selected Answer: C

Explanation:

To route users to the Region with the lowest latency, we can use Amazon Route 53 latency-based routing with health checks. We can deploy a Network Load Balancer (NLB) associated with the Auto Scaling group and create an Amazon Route 53 latency record that points to aliases for each NLB. To enable automated failover between Regions, we can configure Route 53 with failover routing policy. With failover routing policy, active-active or active-passive configurations can be configured between the Regions. Lastly, we can create an Amazon CloudFront distribution that uses the latency record as an origin which will improve the delivery performance of content to the end-users.

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option B is the right answer for this.

upvoted 1 times

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

Selected Answer: C

C. Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory. More information: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_use_cases.html
And yes, two-way trust can be created between AWS DS for MS-AD and the self-managed on-premises AD (https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_tutorial_setup_trust_create.html)

upvoted 1 times

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

This solution does not feature single-sign-on (SSO).

upvoted 3 times

✉️  **cookieMr** 9 months, 1 week ago

Selected Answer: A

The recommended solution is option A: Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console and create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO using AWS Directory Service for Microsoft Active Directory.

By implementing this solution, the company can achieve a single sign-on experience for their AWS accounts while maintaining central control over user and group management in their on-premises Active Directory. The one-way trust ensures that user and group information flows securely from the on-premises directory to AWS SSO, allowing for centralized access management and control across all AWS accounts.

upvoted 7 times

✉️  **DuboisNicolasDuclair** 9 months, 3 weeks ago

Selected Answer: D

Can we have a moderator ?

upvoted 1 times

Question #29

Topic 1

A company provides a Voice over Internet Protocol (VoIP) service that uses UDP connections. The service consists of Amazon EC2 instances that run in an Auto Scaling group. The company has deployments across multiple AWS Regions.

The company needs to route users to the Region with the lowest latency. The company also needs automated failover between Regions.

Which solution will meet these requirements?

- A. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Use the NLB as an AWS Global Accelerator endpoint in each Region.
- B. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Use the ALB as an AWS Global Accelerator endpoint in each Region.
- C. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 latency record that points to aliases for each NLB. Create an Amazon CloudFront distribution that uses the latency record as an origin.
- D. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 weighted record that points to aliases for each ALB. Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.

Correct Answer: C

Community vote distribution

A (78%) C (22%)

✉  **Six_Fingered_Jose**  1 year, 5 months ago

Selected Answer: A

agree with A,
Global Accelerator has automatic failover and is perfect for this scenario with VoIP
<https://aws.amazon.com/global-accelerator/faqs/>
upvoted 48 times

✉  **bnagaraja9099** 5 months ago

A - 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 5 times

✉  **TilTil** 1 week, 3 days ago

This is the best case for A to be an answer. Cloudfront is great but for HTTP use cases.
upvoted 1 times

✉  **BoboChow** 1 year, 4 months ago

Thank you for your link, it make me consolidate A.
upvoted 6 times

✉  **bullrem** 1 year, 2 months ago

This option does not meet the requirements because AWS Global Accelerator is only used to route traffic to the optimal AWS Region, it does not provide automatic failover between regions.
upvoted 2 times

✉  **sachin** 1 year ago

Instant regional failover: AWS Global Accelerator automatically checks the health of your applications and routes user traffic only to healthy application endpoints. If the health status changes or you make configuration updates, AWS Global Accelerator reacts instantaneously to route your users to the next available endpoint.
upvoted 8 times

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

Thank you, the link also helps me to know the differences between Global Acc and CloudFront.
upvoted 2 times

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

I also agree A after reading this link.
upvoted 1 times

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

Selected Answer: A

CloudFront uses Edge Locations to cache content while Global Accelerator uses Edge Locations to find an optimal pathway to the nearest regional endpoint. CloudFront is designed to handle HTTP protocol meanwhile Global Accelerator is best used for both HTTP and non-HTTP protocols such as TCP and UDP. so i think A is a better answer

upvoted 32 times

 **biggybear** Most Recent 9 hours, 5 minutes ago

Selected Answer: A

Correct as Global accelerator is most preferred for TCP and UDP

upvoted 1 times

 **biggybear** 9 hours, 6 minutes ago

A ia correct

upvoted 1 times

 **Kanagarajd** 3 weeks, 1 day ago

Selected Answer: A

A is right answer, key words VoIP, UDP connection, automatic failover between region.

upvoted 1 times

 **Naveena_Devanga** 1 month, 1 week ago

One of the major benefits of AWS Global Accelerator is

Instant regional failover: AWS Global Accelerator automatically checks the health of your applications and routes user traffic only to healthy application endpoints. If the health status changes or you make configuration updates, AWS Global Accelerator reacts instantaneously to route your users to the next available endpoint.

<https://aws.amazon.com/global-accelerator/faqs/>

upvoted 1 times

 **mn2013** 2 months ago

Agree with C. As i understand NLB cannot be used as AWS Global accelerator endpoint. It has to be ALB or ELB.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: A

Its UDP so ALB is not applicable here which means BD are wrong

C using CF that uses latency record as origin? Makes no sense

B NLB autoscaling and AWS GA is best used for lower latency and scaling.

Recommended read: <https://aws.amazon.com/blogs/networking-and-content-delivery/well-architecting-online-applications-with-cloudfront-and-aws-global-accelerator/>

upvoted 2 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: A

Answer-A

upvoted 1 times

 **mohamedsambo** 2 months, 2 weeks ago

Selected Answer: C

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

upvoted 1 times

 **hellomememe** 2 months, 3 weeks ago

Why ALB, not NLB?

upvoted 2 times

 **TheFivePips** 1 month ago

It IS NLB. You cannot trust the "official" answers. I am not even sure why they bother giving them

Application Load Balancer:

- Web applications with layer 7 routing (HTTP/HTTPS)
- Microservices architectures (e.g. Docker containers)
- Lambda targets

Network Load Balancer:

- TCP and UDP based applications
- Ultra low latency
- Static IP addresses
- VPC endpoint services

upvoted 3 times

 **pentium75** 3 months ago

"The company needs to route users to the Region with the lowest latency. The company also needs automated failover between Regions." IMO both A and C would meet both requirements. The main difference is that with A, the IP address stays the same - in case of failover, it would be routed to a different entry point. With C, the different endpoint have different IP addresses, and in case of failover, DNS would return the IP address of a different entry point. Thus failover might take longer with C, but again, the stem does not mention that failover must be fast ...

upvoted 2 times

 **ansagr** 3 months, 2 weeks ago

Selected Answer: C

Option A suggests using an NLB and associating it with an Auto Scaling group, then using the NLB as an AWS Global Accelerator endpoint in each Region. While this can provide low-latency access, AWS Global Accelerator primarily focuses on improving the availability and fault tolerance of applications. It directs traffic over the AWS global network to optimize the path to the application, but it may not necessarily route traffic based on the lowest latency.

In contrast, Option C involves using Amazon Route 53 for latency-based routing, which allows you to direct users to the Region with the lowest latency. This aligns more closely with the requirement of routing users to the Region with the lowest latency. Therefore, Option C is a better fit for the specified use case.

upvoted 10 times

 **yonwick** 2 months, 2 weeks ago

I agree with you, as a networking engineer, I would go with the R53 latency-based entries. I don't know why people are still choosing A, this is not an application based question, rather a networking based question.

I work with VoIP within my DataCenters as well, everyone of my network architect colleagues agreed with Option C.

upvoted 3 times

 **Ruffyit** 5 months ago

CloudFront uses Edge Locations to cache content while Global Accelerator uses Edge Locations to find an optimal pathway to the nearest regional endpoint. CloudFront is designed to handle HTTP protocol meanwhile Global Accelerator is best used for both HTTP and non-HTTP protocols such as TCP and UDP. so i think A is a better answer

upvoted 2 times

 **rlamberti** 5 months, 1 week ago

Selected Answer: A

Keywords: UDP, VoIP, low latency.
<https://aws.amazon.com/global-accelerator/faqs/>

upvoted 1 times

 **tavy** 4 months, 4 weeks ago

A does not mention the global accelerator service? It mention to make NLB act like one, not to use one. Kind of tricky I think
 ' Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Use the NLB as an AWS Global Accelerator endpoint in each Region.'

upvoted 2 times

 **pentium75** 3 months ago

It says that the NLB would act as a Global Accelerator ENDPOINT. This indicates that you'd also use Global Accelerator. And then it makes sense.

upvoted 1 times

 **awashenko** 5 months, 3 weeks ago

Selected Answer: A

<https://aws.amazon.com/global-accelerator/faqs/>
 upvoted 1 times

 **rainiverse** 5 months, 4 weeks ago

Selected Answer: C

To route users to the Region with the lowest latency and enable automated failover between Regions, the company should choose Option C. This option involves deploying a Network Load Balancer (NLB) and an associated target group, associating the target group with the Auto Scaling group, creating an Amazon Route 53 latency record that points to aliases for each NLB, and creating an Amazon CloudFront distribution that uses the latency record as an origin.

Option A is not the best choice because using an NLB as an AWS Global Accelerator endpoint in each Region does not provide automated failover between Regions.

Option B is also not ideal because using an Application Load Balancer (ALB) as an AWS Global Accelerator endpoint in each Region does not provide automated failover between Regions.

upvoted 1 times

 **smdrouiss** 3 months, 3 weeks ago

AWS Global Accelerator supports region failover. This means that if an endpoint in one AWS Region becomes unavailable, Global Accelerator will automatically route traffic to healthy endpoints in other Regions. This can help to improve the availability and performance of your applications.

upvoted 1 times

Question #30

Topic 1

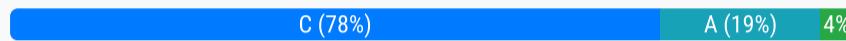
A development team runs monthly resource-intensive tests on its general purpose Amazon RDS for MySQL DB instance with Performance Insights enabled. The testing lasts for 48 hours once a month and is the only process that uses the database. The team wants to reduce the cost of running the tests without reducing the compute and memory attributes of the DB instance.

Which solution meets these requirements MOST cost-effectively?

- A. Stop the DB instance when tests are completed. Restart the DB instance when required.
- B. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.
- C. Create a snapshot when tests are completed. Terminate the DB instance and restore the snapshot when required.
- D. Modify the DB instance to a low-capacity instance when tests are completed. Modify the DB instance again when required.

Correct Answer: C

Community vote distribution



✉️ hanhdroid Highly Voted 1 year, 5 months ago

Selected Answer: C

Answer C, you still pay for storage when an RDS database is stopped
upvoted 32 times

✉️ KVK16 Highly Voted 1 year, 5 months ago

Selected Answer: C

C - Create a manual Snapshot of DB and shift to S3- Standard and Restore from Manual Snapshot when required.

Not A - By stopping the DB although you are not paying for DB hours you are still paying for Provisioned IOPs , the storage for Stopped DB is more than Snapshot of underlying EBS vol. and Automated Back ups .

Not D - Is possible but not MOST cost effective, no need to run the RDS when not needed.

upvoted 10 times

✉️ vi24 Most Recent 2 weeks, 4 days ago

My question is: isn't this DB collecting new data during the testing period (48 hrs.) ? after the snapshot is taken ? stop and restore db from the snapshot is the most cost effective but I think some data might be lost in between, so wouldn't be feasible !

upvoted 1 times

✉️ VanDacker 1 month ago

Selected Answer: A

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

upvoted 3 times

✉️ lsomas 1 month, 1 week ago

Answer C because,

You can stop a DB instance for up to seven days. If you don't manually start your DB instance after seven days, your DB instance is automatically started so that it doesn't fall behind any required maintenance updates.

So, the "auto starting" behaviour is expected.

If you rarely use the database, BEST option is to Snapshot and Delete the database. Then, when you need it again, you could launch a new database from the Snapshot.

Amazon RDS is not intended to be stopped for long periods.

upvoted 1 times

✉️ awsgeek75 2 months, 1 week ago

Selected Answer: C

DB is used one a month for 48 hours only so there is no point in keeping it up for rest of the month.

B: more cost

D: not allowed to reduce computing power

A: It will work but C is much cheaper as instance is not only stopped but terminated.

upvoted 1 times

✉️ A_jaa 2 months, 1 week ago

Selected Answer: C

Answer-C

upvoted 1 times

 **boooliyooo** 2 months, 3 weeks ago

Selected Answer: C

Option A (Stop and Restart) is less operationally complex and provides a quicker way to resume the database. It's suitable if the primary concern is operational simplicity and quick availability.

Option C (Snapshot, Terminate, and Restore) may offer higher cost savings, especially if the instance is large and expensive to run, as you're avoiding charges for the time the instance is down. However, it comes with higher operational complexity and longer lead times to bring the database back online.

In Amazon RDS, you do incur charges for a DB instance even when it's stopped. This is a key distinction from Amazon EC2, where you are not charged for instance hours while an EC2 instance is stopped. For RDS, the charges related to the instance's storage and backups continue to accrue even when the instance itself is not running.

upvoted 2 times

 **ignajtpolandstrong** 2 months, 4 weeks ago

It is C

Amazon RDS allows you to easily stop and start your database instances ONLY for up to seven days at a time. So Snapshot and Restore is proper solution.

upvoted 2 times

 **upliftinghut** 2 months, 4 weeks ago

Selected Answer: A

Database not used by any other applications/processes, only use 48 hours per month while still need the same compute and RAM for intense testing => stop and start the instance will be the most cost effective. Option C needs to pay for snapshot of DB and more complex for what purpose?

upvoted 1 times

 **upliftinghut** 2 months, 4 weeks ago

Sorry, should be C. Key word: Most cost-effective so C - which is taking snapshot is most cost-effective

upvoted 2 times

 **axayprabhu** 3 months, 3 weeks ago

Can you please clear my confusion, If the answer is C,

What is the use of DB here, when every time DB is terminated and restored from snapshots? Data will remain the same right? If DB is terminated how new data is stored when db is not present

upvoted 1 times

 **MiniYang** 4 months, 1 week ago

Selected Answer: A

The Answer is A.

Option A does reduce costs when RDS is not running, because RDS does not charge execution fees when it is not running. When an RDS instance is stopped, you only pay the associated storage charges. In Amazon RDS, storage and backup charges are based on the amount of storage you use. Therefore, when you stop an RDS execution instance, you will still pay the costs associated with storage, but not the execution fees.

In contrast, if you use option C, which is to take a snapshot and terminate the instance, there may be costs associated with storing the snapshot and Amazon Machine Image (AMI). Overall, option A minimizes costs because when you stop an RDS execution instance, you only have to pay a relatively low storage cost rather than an execution fee.

upvoted 2 times

 **roberto_rrt** 5 months, 1 week ago

Selected Answer: A

A. Stop the DB instance when tests are completed. Restart the DB instance when required.

Here's why option A is the most suitable choice:

Cost Reduction: Stopping the DB instance when not in use effectively reduces the cost to zero during the idle period. You only pay for storage when the instance is stopped. This is a cost-effective way to handle infrequent, resource-intensive tasks without incurring ongoing costs.

Performance Insights Enabled: This option allows you to keep Performance Insights enabled when the DB instance is stopped, which provides visibility into database performance. You can resume the instance and monitor performance during the testing period.

upvoted 2 times

 **hrushikeshrelekar** 5 months, 3 weeks ago

Selected Answer: D

A. Stop the DB instance when tests are completed. Restart the DB instance when required.

Explanation:

Stopping and starting a DB instance is the most cost-effective solution for scenarios where the database is not in use all the time. Amazon RDS allows you to stop and start the database instances, and you are not charged for the instance hours while the database is stopped.

upvoted 3 times

 **Chiquitabandita** 6 months, 3 weeks ago

chatgpt is saying one option is to start/stop db instance, so choice A even though the popular choice is C, otherwise use Aurora but that is not an option, nor would it probably be the most cost effective option

upvoted 1 times

 **Fresbie99** 7 months, 2 weeks ago

Selected Answer: C

As DB snapshots is cost efficient.
upvoted 1 times

 **miki111** 8 months, 1 week ago
Option C is the right answer for this.
upvoted 1 times

Question #31

Topic 1

A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check. What should a solutions architect do to accomplish this?

- A. Use AWS Config rules to define and detect resources that are not properly tagged.
- B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
- C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
- D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

Correct Answer: A*Community vote distribution*

A (98%)

 **kurinei021**  1 year, 3 months ago

Answer from ChatGPT:

Yes, you can use AWS Config to create tags for your resources. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. You can use AWS Config to create rules that automatically tag resources when they are created or when their configurations change.

To create tags for your resources using AWS Config, you will need to create an AWS Config rule that specifies the tag key and value you want to use and the resources you want to apply the tag to. You can then enable the rule and AWS Config will automatically apply the tag to the specified resources when they are created or when their configurations change.

upvoted 18 times

 **aaroncelestin** 7 months, 1 week ago

This is the first answer that I've seen ChatGPT get correct here on ExamTopics. You should all know that using ChatGPT for this is bound to give bad answers. It only parrots what it has seen written/copied/pasted by someone/something somewhere, picked up with absolutely zero context. ChatGPT doesn't "know" anything about AWS services. So, beware the "answers" it gives.

upvoted 10 times

 **kidomaruto** 4 months, 3 weeks ago

I tried it with Bing AI, and the answer was almost always the right one.

It depends a lot on the prompt quality

upvoted 2 times

 **cookieMr**  9 months, 1 week ago

Selected Answer: A

AWS Config provides a set of pre-built or customizable rules that can be used to check the configuration and compliance of AWS resources. By creating a custom rule or using the built-in rule for tagging, you can define the required tags for EC2, RDS DB and Redshift clusters. AWS Config continuously monitors the resources and generates configuration change events or evaluation results.

By leveraging AWS Config, the solution can automatically detect any resources that do not comply with the defined tagging requirements. This approach eliminates the need for manual checks or periodic code execution, reducing operational overhead. Additionally, AWS Config provides the ability to automatically remediate non-compliant resources by triggering Lambda or sending notifications, further streamlining the configuration management process.

Option B (using Cost Explorer) primarily focuses on cost analysis and does not provide direct enforcement of proper tagging. Option C and D (writing API calls and running them manually or through scheduled Lambda) require more manual effort and maintenance compared to using AWS Config rules.

upvoted 7 times

 **awsgeek75**  2 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/whitepapers/latest/tagging-best-practices/implementing-and-enforcing-tagging.html>

AWS Config (required_tag)

AWS Config is a service that allows you to assess, audit, and evaluate the configurations of your AWS resources (see Resource types supported by AWS Config). In the case of tagging, we can use it to identify resources that are lacking tags with specific keys, using the required_tags rule (refer to Resource types supported by required_tags). From the earlier example, we might test for the existence of the key on all Amazon EC2 instances.

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: A

Answer-A

upvoted 1 times

✉ **Ruffyit** 5 months ago

Has typos in the question, correct is "A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags." Keyword "are configured with tags", choose (A) "AWS Config rules".

upvoted 1 times

✉ **awashenko** 5 months, 3 weeks ago

Selected Answer: A

I originally thought D, but after reading through the discussion I agree that option A would require less effort. D would get the job done but would require more effort so I think A is correct.

upvoted 1 times

✉ **KawtarZ** 7 months, 1 week ago

Selected Answer: A

A without a doubt

upvoted 1 times

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

Selected Answer: A

AWS Config continually assesses, audits, and evaluates the configurations and relationships of your resources on AWS, on premises, and on other clouds.

upvoted 2 times

✉ **james2033** 8 months, 1 week ago

Selected Answer: A

Has typos in the question, correct is "A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags." Keyword "are configured with tags", choose (A) "AWS Config rules".

upvoted 1 times

✉ **miki111** 8 months, 1 week ago

Option A is the right answer for this.

upvoted 1 times

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

Selected Answer: A

The answer is A

upvoted 1 times

✉ **Bmarodi** 9 months, 3 weeks ago

Selected Answer: A

Option will accomplish the requirements

upvoted 1 times

✉ **beginnercloud** 10 months, 1 week ago

Selected Answer: A

AWS Config can track the configuration status of non-compliant resources :))

upvoted 1 times

✉ **caffee** 11 months, 2 weeks ago

Selected Answer: A

AWS Config can track the configuration status of non-compliant resources.

upvoted 2 times

✉ **gx2222** 11 months, 3 weeks ago

Selected Answer: A

Option A is the most appropriate solution to accomplish the given requirement because AWS Config Rules provide a way to evaluate the configuration of AWS resources against best practices and company policies. In this case, a custom AWS Config rule can be defined to check for proper tag allocation on Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters. The rule can be configured to run periodically and notify the responsible parties when a resource is not properly tagged.

upvoted 2 times

✉ **channn** 11 months, 4 weeks ago

Selected Answer: A

Key words: configured with tags

upvoted 1 times

✉ **linux_admin** 12 months ago

Selected Answer: A

AWS Config is a service that provides a detailed view of the configuration of AWS resources in an account. AWS Config rules can be used to define and detect resources that are not properly tagged. These rules can be customized to match specific requirements and automatically check all

resources for proper tag allocation. When resources are found without the proper tags, AWS Config can trigger an SNS notification or an AWS Lambda function to perform the required action.

upvoted 1 times

Question #32

Topic 1

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images.

Which method is the MOST cost-effective for hosting the website?

- A. Containerize the website and host it in AWS Fargate.
- B. Create an Amazon S3 bucket and host the website there.
- C. Deploy a web server on an Amazon EC2 instance to host the website.
- D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.

Correct Answer: B

Community vote distribution

B (100%)

✉️  **masetromain**  1 year, 5 months ago

Selected Answer: B

Good answer is B: client-side JavaScript. the website is static, so it must be S3.
upvoted 26 times

✉️  **BoboChow**  1 year, 5 months ago

Selected Answer: B

HTML, CSS, client-side JavaScript, and images are all static resources.
upvoted 10 times

✉️  **awsgeek75**  2 months, 1 week ago

Selected Answer: B

Cheapest Static site hosting = S3
upvoted 2 times

✉️  **A_jaa** 2 months, 1 week ago

Selected Answer: B

Answer-B
upvoted 1 times

✉️  **Ruffyit** 5 months ago

HTML, CSS, client-side JavaScript, and images are all static resources.
upvoted 1 times

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

The MOST cost-effective method for hosting a website is to:

Create an Amazon S3 bucket and host the website there.

Amazon S3 is a highly scalable and cost-effective object storage service. It is a good option for hosting static websites, such as the website in this scenario.

To host a static website on Amazon S3, you would first need to create an S3 bucket. Then, you would need to upload the website files to the bucket. Once the files are uploaded, you can configure the bucket to serve as a website.
upvoted 2 times

✉️  **hungpm** 6 months, 3 weeks ago

Selected Answer: B

Static website should work fine with S3
upvoted 1 times

✉️  **KawtarZ** 7 months, 1 week ago

Selected Answer: B

the website is static because the backend runs on client side.
upvoted 2 times

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

Selected Answer: B

all static resources.
upvoted 1 times

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

Selected Answer: B

static website, cost-effective = S3 web hosting
upvoted 3 times

 **james2033** 8 months, 1 week ago

Selected Answer: B

Just all static content HTML, CSS, client-side JavaScript, images. Amazon S3 is good enough.
upvoted 1 times

 **miki111** 8 months, 1 week ago
Option B is the right answer for this.

upvoted 1 times

 **Kaab_B** 8 months, 2 weeks ago

Selected Answer: B

S3 is amongst the cheapest services offered by AWS.
upvoted 1 times

 **karloscetina007** 8 months, 3 weeks ago

Selected Answer: B

B is the correct answer.
upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B

By using Amazon S3 to host the website, you can take advantage of its durability, scalability, and low-cost pricing model. You only pay for the storage and data transfer associated with your website, without the need for managing and maintaining web servers or containers. This reduces the operational overhead and infrastructure costs.

Containerizing the website and hosting it in AWS Fargate (option A) would involve additional complexity and costs associated with managing the container environment and scaling resources. Deploying a web server on an Amazon EC2 instance (option C) would require provisioning and managing the EC2 instance, which may not be cost-effective for a static website. Configuring an Application Load Balancer with an AWS Lambda target (option D) adds unnecessary complexity and may not be the most efficient solution for hosting a static website.

upvoted 5 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: B

Option B is the MOST cost-effective for hosting the website.
upvoted 1 times

 **beginnercloud** 10 months, 1 week ago

Selected Answer: B

static website = B
upvoted 1 times

Question #33

Topic 1

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval. What should a solutions architect recommend to meet these requirements?

- A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.
- B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.
- C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.
- D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.

Correct Answer: C

Community vote distribution

C (83%)

B (17%)

✉  **ArielSchivo**  1 year, 5 months ago

Selected Answer: C

I would go for C. The tricky phrase is "near-real-time solution", pointing to Firehouse, but it can't send data to DynamoDB, so it leaves us with C as best option.

Kinesis Data Firehose currently supports Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk, Datadog, NewRelic, Dynatrace, Sumologic, LogicMonitor, MongoDB, and HTTP End Point as destinations.

<https://aws.amazon.com/kinesis/data-firehose/faqs/#:~:text=Kinesis%20Data%20Firehose%20currently%20supports,HTTP%20End%20Point%20as%20destinations>.
upvoted 62 times

✉  **Lonojack** 1 year, 2 months ago

This was a really tough one. But you have the best explanation on here with reference point. Thanks. I'm going with answer C!
upvoted 3 times

✉  **SaraSundaram** 1 year ago

There are many questions having Firehose and Stream. Need to know them in detail to answer. Thanks for the explanation
upvoted 4 times

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

Stream is used if you want real time results , but with firehose , you generally use the data at a later point of time by storing it somewhere. Hence if you see "REAL TIME" the answer is most probably Kinesis Data Streams.
upvoted 14 times

✉  **lizzard812** 1 year, 1 month ago

Sorry but I still can't see how Kinesis Data Stream is 'scalable', since you have to provision the quantity of shards in advance?
upvoted 1 times

✉  **habibi03336** 1 year, 1 month ago

"easily stream data at any scale"
This is a description of Kinesis Data Stream. I think you can configure its quantity but still not provision and manage scalability by yourself.
upvoted 1 times

✉  **JesseeS**  1 year, 5 months ago

The answer is C, because Firehose does not support DynamoDB and another key word is "data" Kinesis Data Streams is the correct choice. Pay attention to key words. AWS likes to trick you up to make sure you know the services.
upvoted 29 times

✉  **vi24**  2 weeks, 3 days ago

I chose B. The "near real time" is very specific to Kinesis firehose which is a better option anyway. The rest of the answer makes sense too. C is wrong : "sensitive data removed by Lambda & then store transaction data in DynamoDB" , while it continues to say other applications are accessing the transaction data from kinesis Data stream !!

upvoted 1 times

 **Pics00094** 1 month ago

Selected Answer: C

need to know..

1) Lambda Integration

2) Difference between Real time(Kinesis Data Stream) vs Near Real time(Kinesis Fire House)

3) Firehouse can't target DynamoDB

upvoted 2 times

 **JulianWaksmann** 1 month, 2 weeks ago

i think c are bad too, because it isn't near real time.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: C

A: DynamoDB streams are logs, not fit for real-time sharing.

B: S3 is not document database, it's BLOB

D: S3 and files are not database

C: Kinesis + Lambda + DynamoDB is high performance, low latency scalable solution.

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: C

Answer-C

upvoted 1 times

 **bujuman** 3 months ago

Selected Answer: C

Data Stream can handle near-real-time and is able to store to DynamoDB

upvoted 1 times

 **djgodzilla** 3 months, 1 week ago

Selected Answer: C

Kinesis Data Streams stores data for later processing by applications , key difference with Firehose which delivers data directly to AWS services.

upvoted 1 times

 **wabosi** 4 months, 2 weeks ago

Selected Answer: C

Correct answer is C.

As some commented already, 'near-real-time' could make you think about Firehose but its consumers are 3rd-party partners destinations, Amazon S3, Amazon Redshift, Amazon OpenSearch and HTTP endpoint so DynamoDB can't be used in this scenario.

upvoted 1 times

 **Ruffyit** 5 months ago

C is the best solution for the following reasons:

1. Real-time Data Stream: To share millions of financial transactions with other apps, you need to be able to ingest data in real-time, which is made possible by Amazon Kinesis Data Streams.

2. Data Transformation: You can cleanse and eliminate sensitive data from transactions before storing them in Amazon DynamoDB by utilizing AWS Lambda with Kinesis Data Streams. This takes care of the requirement to handle sensitive data with care.

3. Scalability: DynamoDB and Amazon Kinesis are both extremely scalable technologies that can manage enormous data volumes and adjust to the workload.

upvoted 1 times

 **AWSStudyBuddy** 5 months, 1 week ago

C is the best solution for the following reasons:

1. Real-time Data Stream: To share millions of financial transactions with other apps, you need to be able to ingest data in real-time, which is made possible by Amazon Kinesis Data Streams.

2. Data Transformation: You can cleanse and eliminate sensitive data from transactions before storing them in Amazon DynamoDB by utilizing AWS Lambda with Kinesis Data Streams. This takes care of the requirement to handle sensitive data with care.

3. Scalability: DynamoDB and Amazon Kinesis are both extremely scalable technologies that can manage enormous data volumes and adjust to the workload.

4. Low-Latency retrieval: Applications requiring real-time data can benefit from low-latency retrieval, which is ensured by storing the processed data in DynamoDB.

upvoted 2 times

 **AWSStudyBuddy** 5 months, 1 week ago

Choices A, B, and D are limited in certain ways:

• Real-time data streaming is not provided by Option A (DynamoDB with Streams); additional components would need to be implemented in order to handle data in real-time.

• Kinesis Data Firehose, Option B, lacks the real-time processing capabilities of Kinesis Data Streams and is primarily used for data distribution to

destinations like as S3.

- For near-real-time use cases, Option D (Batch processing with S3) is not the best choice. It adds latency and overhead associated with batch processing, which is incompatible with the need for real-time data sharing.

Using the advantages of Lambda, DynamoDB, and Kinesis Data Streams, Option C offers a scalable, real-time, and effective solution for the given use case.

upvoted 1 times

✉ **Ak9kumar** 6 months ago

I picked B. We need to understand how Kinesis Data Warehouse works to answer this question right.

upvoted 1 times

✉ **spw7** 5 months ago

firehose can not send data to dynamoDB

upvoted 1 times

✉ **sohailn** 7 months, 2 weeks ago

kinesis Data Firhouse optionally support lambda for transformation

upvoted 1 times

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

Selected Answer: C

Scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications = Amazon Kinesis Data Streams.

Remove sensitive data from transactions = AWS Lambda.

Store transaction data in a document database for low-latency retrieval = Amazon DynamoDB.

upvoted 9 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: C

To meet the requirements of sharing financial transaction details with several other internal applications, and processing and storing the transactions data in a scalable and near-real-time manner, a solutions architect should recommend option C: Stream the transactions data into Amazon Kinesis Data Streams, use AWS Lambda integration to remove sensitive data, and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.

Option A (storing transactions data in DynamoDB and using DynamoDB Streams) may not provide the same level of scalability and real-time data sharing as Kinesis Data Streams. Option B (using Kinesis Data Firehose to store data in DynamoDB and S3) adds unnecessary complexity and additional storage costs. Option D (storing batched transactions data in S3 and processing with Lambda) may not provide the required near-real-time data sharing and low-latency retrieval compared to the streaming-based solution.

upvoted 3 times

✉ **oiccic99** 9 months, 2 weeks ago

Selected Answer: C

its c because yes

upvoted 1 times

Question #34

Topic 1

A company hosts its multi-tier applications on AWS. For compliance, governance, auditing, and security, the company must track configuration changes on its AWS resources and record a history of API calls made to these resources.

What should a solutions architect do to meet these requirements?

- A. Use AWS CloudTrail to track configuration changes and AWS Config to record API calls.
- B. Use AWS Config to track configuration changes and AWS CloudTrail to record API calls.
- C. Use AWS Config to track configuration changes and Amazon CloudWatch to record API calls.
- D. Use AWS CloudTrail to track configuration changes and Amazon CloudWatch to record API calls.

Correct Answer: B

Community vote distribution

B (98%)

✉️  **airraid2010**  1 year, 5 months ago

Selected Answer: B

CloudTrail - Track user activity and API call history.
Config - Assess, audits, and evaluates the configuration and relationships of tag resources.

Therefore, the answer is B
upvoted 30 times

✉️  **awsgeek75**  2 months, 1 week ago

Selected Answer: B

Config = Governance, auditing of AWS resource
CloudTrail = API call tracking
B is correct
upvoted 1 times

✉️  **A_jaa** 2 months, 1 week ago

Selected Answer: B

Answer-B
upvoted 1 times

✉️  **Ruffyit** 5 months ago

Correct Answer- Option B. Here's why

AWS Config for Configuration Changes: AWS Config is a service that tracks changes to resource configurations over time. It provides a history of configuration changes to your AWS resources and helps with compliance and auditing by allowing you to assess how resource configurations have changed over time.

AWS CloudTrail for API Calls: AWS CloudTrail is designed specifically for recording API calls made to AWS resources. It captures detailed information about who made each API call, the actions taken, and the resources affected. This is essential for auditing and security purposes.
upvoted 1 times

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

Correct Answer- Option B. Here's why

AWS Config for Configuration Changes: AWS Config is a service that tracks changes to resource configurations over time. It provides a history of configuration changes to your AWS resources and helps with compliance and auditing by allowing you to assess how resource configurations have changed over time.

AWS CloudTrail for API Calls: AWS CloudTrail is designed specifically for recording API calls made to AWS resources. It captures detailed information about who made each API call, the actions taken, and the resources affected. This is essential for auditing and security purposes.

While Amazon CloudWatch can be used to monitor and gather metrics, it is not designed for recording API calls or tracking configuration changes. AWS Config and AWS CloudTrail are purpose-built for these specific tasks and are the best services to use for the described requirements.
upvoted 1 times

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

Selected Answer: B

Although tracking configuration changes and recording API calls are not intended uses for Amazon CloudWatch, it can be utilized for monitoring and collecting data. AWS CloudTrail and AWS Config are purpose-built for these specific tasks and are the best services to use for the described requirements.

upvoted 1 times

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

Selected Answer: B

CloudWatch is a monitoring service for AWS resources and applications. CloudTrail is a web service that records API activity in your AWS account.
upvoted 2 times

✉  **Bogs123456711** 7 months, 4 weeks ago

Selected Answer: B

CONFIG - AWS CONFIG
RECORD API CALLS - CLOUDTRAIL
upvoted 1 times

✉  **hsinchang** 8 months ago

Selected Answer: B

CloudWatch is mainly used to monitor AWS services with metrics, not recording actions inside the AWS environments. It can also monitor CloudTrail logged events.
For recording API calls it requires CloudTrail.
upvoted 1 times

✉  **james2033** 8 months, 1 week ago

Selected Answer: B

Keyword "Amazon CloudWatch" is not for this case, remove C and D.

Use AWS Config first to track configuration changes, Second is AWS CloudTrail to record API calls. (Answer B, and correct answer). Answer A is reversed order of B, and not accepted.

upvoted 2 times

✉  **miki111** 8 months, 1 week ago

Option B is the right answer for this.

upvoted 1 times

✉  **karloscetina007** 8 months, 3 weeks ago

Selected Answer: B

B is the answer with no doubts
upvoted 1 times

✉  **minhpn** 9 months, 1 week ago

Selected Answer: B

config => AWS config
record API calls => AWS CloudTrail
upvoted 1 times

✉  **cookieMr** 9 months, 1 week ago

Selected Answer: B

To meet the requirement of tracking configuration changes on AWS resources and recording a history of API calls, a solutions architect should recommend option B: Use AWS Config to track configuration changes and AWS CloudTrail to record API calls.

Option A (using CloudTrail to track configuration changes and Config to record API calls) is incorrect because CloudTrail is specifically designed to capture API call history, while Config is designed for tracking configuration changes.

Option C (using Config to track configuration changes and CloudWatch to record API calls) is not the recommended approach. While CloudWatch can be used for monitoring and logging, it does not provide the same level of detail and compliance tracking as CloudTrail for recording API calls.

Option D (using CloudTrail to track configuration changes and CloudWatch to record API calls) is not the optimal choice because CloudTrail is the appropriate service for tracking configuration changes, while CloudWatch is not specifically designed for recording API call history.
upvoted 2 times

✉  **Bmarodi** 9 months, 3 weeks ago

Selected Answer: B

Option B meets requirements.
upvoted 1 times

✉  **linux_admin** 12 months ago

Selected Answer: B

AWS Config is a fully managed service that allows the company to assess, audit, and evaluate the configurations of its AWS resources. It provides a detailed inventory of the resources in use and tracks changes to resource configurations. AWS Config can detect configuration changes and alert the company when changes occur. It also provides a historical view of changes, which is essential for compliance and governance purposes.

AWS CloudTrail is a fully managed service that provides a detailed history of API calls made to the company's AWS resources. It records all API activity in the AWS account, including who made the API call, when the call was made, and what resources were affected by the call. This information is critical for security and auditing purposes, as it allows the company to investigate any suspicious activity that might occur on its AWS resources.
upvoted 3 times

✉  **bilel500** 1 year ago

Selected Answer: B

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It provides a history of configuration changes made to your resources and can be used to track changes made to your resources over time.

AWS CloudTrail is a service that enables you to record API calls made to your AWS resources. It provides a history of API calls made to your resources, including the identity of the caller, the time of the call, the source of the call, and the response element returned by the service.
upvoted 1 times

Question #35

Topic 1

A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third-party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.

Which solution meets these requirements?

- A. Enable Amazon GuardDuty on the account.
- B. Enable Amazon Inspector on the EC2 instances.
- C. Enable AWS Shield and assign Amazon Route 53 to it.
- D. Enable AWS Shield Advanced and assign the ELB to it.

Correct Answer: D

Community vote distribution

D (100%)

✉  **ninjawrz**  1 year, 5 months ago

Selected Answer: D

Answer is D
C is incorrect because question says Third party DNS and route 53 is AWS proprietary
upvoted 37 times

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

Right answer, wrong explanation.
You can use Route 53 with a custom domain.. it's all about the "large-scale DDOS attack".
upvoted 8 times

✉  **BoboChow**  1 year, 5 months ago

Selected Answer: D

AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator standard accelerators.
upvoted 26 times

✉  **leonardh** 10 months, 3 weeks ago

I'd agree as Shield Advanced is the only tier that can protect EC2 which is not possible in Standard.
upvoted 7 times

✉  **awsgeek75**  2 months, 1 week ago

Selected Answer: D

A: GuardDuty is not for this, mostly for account monitoring for suspicious activity
B: Inspector is for OS vulnerabilities
C: Shield with R53 is not going to protect against DDoS
D: Shield Advanced is build for DDoS protection
upvoted 2 times

✉  **awsgeek75** 2 months, 1 week ago

Forgot to mention, C won't work because a 3rd party DNS is used and R53 is not part of the setup
upvoted 2 times

✉  **awsgeek75** 2 months, 1 week ago

Prevent large scale DDOS attack = AWS Shield Advanced
upvoted 1 times

✉  **A_jaa** 2 months, 1 week ago

Selected Answer: D

Answer-D
upvoted 1 times

✉  **djgodzilla** 3 months, 1 week ago

Selected Answer: D

- In addition to the network and transport layer protections that come with Standard, Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall.
<https://aws.amazon.com/shield/features/#:~:text=In%20addition%20to%20the%20network,WAF%2C%20a%20web%20application%20firewall.>
upvoted 1 times

✉  **OmegaLambda7XL9** 4 months, 1 week ago

This one got me to be honest
upvoted 2 times

✉  **Ruffyit** 5 months ago

Option A is incorrect because Amazon GuardDuty is a threat detection service that focuses on identifying malicious activity and unauthorized behavior within AWS accounts. While it is useful for detecting various security threats, it does not specifically address large-scale DDoS attacks.

Option B is also incorrect because Amazon Inspector is a vulnerability assessment service that helps identify security issues and vulnerabilities within EC2. It does not directly protect against DDoS attacks.

Option C is not the optimal choice because AWS Shield provides basic DDoS protection for resources such as Elastic IP addresses, CloudFront, and Route53 hosted zones. However, it

upvoted 2 times

✉  **Ruffyit** 5 months ago

does not provide the advanced capabilities and assistance offered by AWS Shield Advanced, which is better suited for protecting against large-scale DDoS attacks.

Therefore, option D with AWS Shield Advanced and assigning the ELB to it is the recommended solution to detect and protect against large-scale DDoS attacks in the architecture described.

upvoted 2 times

✉  **Abitek007** 5 months, 3 weeks ago

D, but can be tricky, the third party negates Route53
upvoted 1 times

✉  **Ak9kumar** 6 months ago

Answer D. Learn section on AWS Advanced Shield on aws.amazon.com to help you understand this. It helped me.
upvoted 1 times

✉  **ishant101** 7 months ago

answer is D
upvoted 1 times

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

Selected Answer: D
DDoS = AWS Shield
upvoted 2 times

✉  **hsinchang** 8 months ago

Selected Answer: D
large-scale DDoS leads to advanced instead of standard AWS Shield.
upvoted 1 times

✉  **james2033** 8 months, 1 week ago

Selected Answer: D
Keyword "large-scale DDoS attacks", "Amazon EC2", "VPC", "ELB", "3rd service used for DNS".
Amazon GuardDuty <https://aws.amazon.com/guardduty/> Intelligent threat detection.

AWS Shield <https://aws.amazon.com/shield/> Automatically detect and mitigate sophisticated network-level DDoS.

AWS Shield Advanced with ELB <https://aws.amazon.com/about-aws/whats-new/2022/04/aws-shield-application-balancer-automatic-ddos-mitigation/>. Choose D.

upvoted 2 times

✉  **miki111** 8 months, 1 week ago

Option D is the right answer for this.
upvoted 1 times

✉  **Kaab_B** 8 months, 2 weeks ago

Selected Answer: D
DDoS extended is AWS Shield Advanced without a doubt.
upvoted 1 times

✉  **karloscetina007** 8 months, 3 weeks ago

A third-party service
D is the answer with no doubts
upvoted 1 times

Question #36

Topic 1

A company is building an application in the AWS Cloud. The application will store data in Amazon S3 buckets in two AWS Regions. The company must use an AWS Key Management Service (AWS KMS) customer managed key to encrypt all data that is stored in the S3 buckets. The data in both S3 buckets must be encrypted and decrypted with the same KMS key. The data and the key must be stored in each of the two Regions. Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure replication between the S3 buckets.
- B. Create a customer managed multi-Region KMS key. Create an S3 bucket in each Region. Configure replication between the S3 buckets. Configure the application to use the KMS key with client-side encryption.
- C. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure replication between the S3 buckets.
- D. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with AWS KMS keys (SSE-KMS). Configure replication between the S3 buckets.

Correct Answer: C

Community vote distribution

B (57%)

D (41%)

 **pooppants**  1 year, 5 months ago

Selected Answer: B

KMS Multi-region keys are required <https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>
upvoted 59 times

 **Instantqueue** 5 months, 2 weeks ago

It's not correct because the question asks for server side encryption, not client side (before the objects reach the bucket).
upvoted 5 times

 **sohailn** 7 months, 2 weeks ago

Absolutely D is the right one because s3 kms multi region as an individual key so you must first decrypt in source bucket and then re-encrypt in target bucket
upvoted 4 times

 **sakurali** 5 months, 1 week ago

Each set of related multi-Region keys has the same key material and key ID, so you can encrypt data in one AWS Region and decrypt it in a different AWS Region without re-encrypting or making a cross-Region call to AWS KMS.
upvoted 4 times

 **Johan_jelly** 3 months, 1 week ago

KMS multi-region keys are typically used when you need to enable cross-Region replication of encrypted data
upvoted 1 times

 **magazz** 1 year, 4 months ago

Amazon S3 cross-region replication decrypts and re-encrypts data under a KMS key in the destination Region, even when replicating objects protected by a multi-Region key. So stating that Amazon S3 cross-region replication decrypts and re-encrypts data under a KMS key in the destination Region, even when replicating objects protected by a multi-Region key is required is incorrect
upvoted 3 times

 **thanhvx1** 11 months, 3 weeks ago

Option B involves configuring the application to use client-side encryption, which can increase the operational overhead of managing and securing the keys.
upvoted 2 times

 **TuLe** 1 year, 3 months ago

@magazz: it's not true then. Based on the document from AWS <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html>, we will need to setup the replication rule with destination KMS. In order to have the key available in more than 2, then multi-region key should be required. But I'm still not favor option B - we can use server-side when why wasting effort to do client side encryption.
upvoted 2 times

 **TuLe** 1 year, 3 months ago

I would say it's true... Not sure the previous one say "not true" :D.
upvoted 1 times

 **JayBee65** 1 year, 3 months ago

It's not clear what you are saying. Are you saying that B is correct or D is correct?
upvoted 2 times

 **karbob** 1 year, 2 months ago

:D => is smile i thought
upvoted 2 times

 **KJa**  1 year, 5 months ago

Selected Answer: D

Cannot be A - question says customer managed key
Cannot B - client side encryption is operational overhead
Cannot C - as it says SSE-S3 instead of customer managed
so the answer is D though it required one time setup of keys

upvoted 53 times

 **mattlai** 1 year, 5 months ago

fun joke, if u dont do encryption on client side, where else could it be?
upvoted 1 times

 **Newptone** 1 year, 4 months ago

It could be server side. For client side, the application need to finish the encryption and decryption by itself. So S3 object encryption on the server side is less operational overhead. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingClientSideEncryption.html>

But for option B, the major issue is if you create KMS keys in 2 regions, they can not be the same.
upvoted 5 times

 **Newptone** 1 year, 4 months ago

Sorry for the typo, I mean option D.
upvoted 2 times

 **Clouddon** 7 months, 2 weeks ago

Kindly point at where server-side encryption support multi-region. It is only mention on the aws blog that client-side support multi-region.
upvoted 1 times

 **th3cookie** 1 year, 4 months ago

How does client side encryption increase OPERATIONAL overhead? Do you think every connected client is sitting there with gpg cli, decrypting/encrypting every packet that comes in/out? No, it's done via SDK -> <https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/introduction.html>

The correct answer is B because that's the only way to actually get the same key across multiple regions with minimal operational overhead
upvoted 12 times

 **kakka22** 11 months, 3 weeks ago

"The data in both S3 buckets must be encrypted and decrypted with the same KMS key"
Client side encryption means that key is generated in from the client without storing that in the KMS...
upvoted 5 times

 **BoboChow** 1 year, 5 months ago

The data in both S3 buckets must be encrypted and decrypted with the same KMS key.
AWS KMS supports multi-Region keys, which are AWS KMS keys in different AWS Regions that can be used interchangeably – as though you had the same key in multiple Regions.
"as though" means it's different.
So I agree with B
upvoted 13 times

 **BoboChow** 1 year, 5 months ago

key change across regions unless you use multi-Region keys
upvoted 2 times

 **pentium75** 3 months ago

B includes replicating the data in the S3 buckets, which is not mentioned anywhere in the stem. It says that you need to store data in two buckets, not that you need to replicate content between buckets.
upvoted 1 times

 **Drew3000** 2 weeks, 1 day ago

All the choices involve replication between the buckets.
upvoted 1 times

 **ml1190**  2 days, 7 hours ago

SSE encryption is not required and multi-region keys support client side encryption, so the correct answer is B
upvoted 1 times

 **hro** 2 days, 23 hours ago

C - The question implies that the Data AND Key must be in EACH of the two Regions

upvoted 1 times

 **MoAboDaif** 2 weeks, 1 day ago

Selected Answer: D

he sayed "The company must use an Key Management Service (AWS KMS) customer managed key"

B. is using client side encryption not even aws key

Right... ??

upvoted 1 times

 **NishantM** 3 weeks, 1 day ago

Selected Answer: D

It is mentioning server side encryption using KMS.

upvoted 1 times

 **jhakas_bijoy** 1 month ago

Selected Answer: B

this is clear case of multi region key

upvoted 1 times

 **TheFivePips** 1 month ago

Selected Answer: B

"A single-Region KMS key generated by AWS KMS is stored and used only in the Region in which it was created. With AWS KMS multi-Region keys you can choose to replicate a multi-Region primary key into multiple Regions within the same AWS partition."

<https://aws.amazon.com/kms/faqs/>

upvoted 1 times

 **Mohammed_Kamal** 1 month, 1 week ago

Selected Answer: B

i found the answer guys. acually i never found resource state that normal keys (not multi regions key) can be replicated across region.

also i found this "A single-Region KMS key generated by AWS KMS is stored and used only in the Region in which it was created. With AWS KMS multi-Region keys you can choose to replicate a multi-Region primary key into multiple Regions within the same AWS partition." which mean option D can't never be correct since key can't be used in another region which seem logically otherwise they wouldn't make multi region keys if we can simply copy keys

upvoted 2 times

 **modehqudah** 1 month, 3 weeks ago

Selected Answer: B

The data in both S3 buckets must be encrypted and decrypted with the same KMS key.

upvoted 1 times

 **klimaxk666** 1 month, 3 weeks ago

Selected Answer: B

By creating a customer managed multi-Region KMS key, you can have a single key that works across both AWS Regions.

Creating an S3 bucket in each Region allows you to store data in both Regions.

Configuring replication between the S3 buckets ensures that the data is replicated between the Regions.

Using client-side encryption with the KMS key ensures that the data is encrypted and decrypted with the same KMS key

upvoted 1 times

 **yonwick** 2 months ago

I say D.

B is not the right one because it uses client-side key.

upvoted 1 times

 **mn2013** 2 months ago

Selected Answer: B

Going with B as that is the only option that allows to use the same key in multiple regions which is reqd for the cross-region replication. They key used is AWS KMS key and for multi-region. But the encryption and decryption will be done by the client.

upvoted 1 times

 **upliftinghut** 2 months ago

Selected Answer: B

B is correct. If server side and customer managed key, must be SSE-C => D not correct. Link:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html>

upvoted 1 times

 **upliftinghut** 2 months ago

SSE-S3 and SSE-KMS are both server side and managed by AWS

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: B

A: Not customer managed

C: SSE-S3 cannot use customer provided keys, you have to use SSE-C

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/specifying-s3-encryption.html>

If you want to specify a different encryption type in your PUT requests, you can use server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS), dual-layer server-side encryption with AWS KMS keys (DSSE-KMS), or server-side encryption with customer-provided keys (SSE-C). If you want to set a different default encryption configuration in the destination bucket, you can use SSE-KMS or DSSE-KMS.

D: Creates 2 separate keys in 2 regions so it's wrong

B: is correct

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: B

Answer-B

upvoted 1 times

 **rt_7777** 3 months ago

While answer D is make more sense in aligned with these points:

- data in both S3 buckets must be encrypted and decrypted with the same KMS keys
- The "data" and the "key" must be stored in in each of the two regions
- LEAST operational overhead

Why exam answer given is C where not using KMS to perform server-side encryption?

upvoted 1 times

Question #37

Topic 1

A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework.

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

- A. Use the EC2 serial console to directly access the terminal interface of each instance for administration.
- B. Attach the appropriate IAM role to each existing instance and new instance. Use AWS Systems Manager Session Manager to establish a remote SSH session.
- C. Create an administrative SSH key pair. Load the public key into each EC2 instance. Deploy a bastion host in a public subnet to provide a tunnel for administration of each instance.
- D. Establish an AWS Site-to-Site VPN connection. Instruct administrators to use their local on-premises machines to connect directly to the instances by using SSH keys across the VPN tunnel.

Correct Answer: B

Community vote distribution



✉️ **BoboChow** Highly Voted 1 year, 4 months ago

Selected Answer: B

How can Session Manager benefit my organization?

Ans: No open inbound ports and no need to manage bastion hosts or SSH keys

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

upvoted 19 times

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

Do you know what from the question is it Windows or Linux EC2. I think not so how you want to do SSH session for Windows?

Answer is C

upvoted 2 times

✉️ **JayBee65** 1 year, 3 months ago

Session Manager provides support for Windows, Linux, and macOS from a single tool

upvoted 5 times

✉️ **sohailn** 7 months, 2 weeks ago

session manager works with linux, windows, and mac too

upvoted 3 times

✉️ **TienHuyhn** 9 months ago

"Cross-platform support for Windows, Linux, and macOS"

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

upvoted 2 times

✉️ **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: B

A: Serial console is for device direct connection to peripherals and monitor boot etc.

C: Workable solution but a lot of overhead

D: Too much overhead for everyone

B: Managed product for this purpose so least overhead.

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

upvoted 1 times

✉️ **A_jaa** 2 months, 1 week ago

Selected Answer: B

Answer-B

upvoted 1 times

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

I go with option B. Here's why--- IAM Roles: Without SSH keys or shared passwords, securely provide access to EC2 instances and AWS services.
upvoted 4 times

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

Without requiring direct SSH connection, securely access and control EC2 instances with AWS Systems Manager Session Manager.

Least Operational Overhead: An effective and fully managed method of managing instances.

Well-Architected Framework: Complies with performance, security, and reliability best practices from AWS.

Cons of alternative options:

Option A: The automation and flexibility required for secure administration at scale are not provided by using the EC2 serial terminal directly.

Option C: There is more operational overhead and complexity when a bastion host is deployed.

Option D: For secure instance administration, setting up an AWS Site-to-Site VPN connection is too difficult and not the optimal approach.

In conclusion, Option B is suggested as the best option given the given circumstances.

upvoted 4 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: B

This solution meets all of the requirements with the LEAST operational overhead. It is repeatable, uses native AWS services, and follows the AWS Well-Architected Framework.

Repeatable: The process of attaching an IAM role to an EC2 instance and using Systems Manager Session Manager to establish a remote SSH session is repeatable. This can be easily automated, so that new instances can be provisioned and administrators can connect to them securely without any manual intervention.

upvoted 2 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected Answer: B

With AWS Systems Manager Session Manager, you can manage your Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, on-premises servers, and virtual machines (VMs). You can use either an interactive one-click browser-based shell or the AWS Command Line Interface (AWS CLI). It provides secure and auditable node management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html#:~:text=RSS-,Session%20Manager,-is%20a%20fully>
upvoted 2 times

 **james2033** 8 months, 1 week ago

Selected Answer: B

Keyword "access and administer the instances remotely and securely" See "AWS Systems Manager Session Manager at "
<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html>.

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option B is the right answer for this.

upvoted 1 times

 **TienHuynh** 9 months ago

Selected Answer: B

- +Centralized access control to managed nodes using IAM policies
- +No open inbound ports and no need to manage bastion hosts or SSH keys
- +Cross-platform support for Windows, Linux, and macOS

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B

Option A provides direct access to the terminal interface of each instance, but it may not be practical for administration purposes and can be cumbersome to manage, especially for multiple instances.

Option C adds operational overhead and introduces additional infrastructure that needs to be managed, monitored, and secured. It also requires SSH key management and maintenance.

Option D is complex and may not be necessary for remote administration. It also requires administrators to connect from their local on-premises machines, which adds complexity and potential security risks.

Therefore, option B is the recommended solution as it provides secure, auditable, and repeatable remote access using IAM roles and AWS Systems Manager Session Manager, with minimal operational overhead.

upvoted 4 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: B

The choice for me is the option B.

upvoted 1 times

 **cheese929** 11 months, 3 weeks ago

Selected Answer: B

B is correct and has the least overhead.

upvoted 1 times

✉️ **linux_admin** 12 months ago

Selected Answer: B

AWS Systems Manager Session Manager is a fully managed service that provides secure and auditable instance management without the need for bastion hosts, VPNs, or SSH keys. It provides secure and auditable access to EC2 instances and eliminates the need for managing and securing SSH keys.

upvoted 1 times

✉️ **PaoloRoma** 1 year ago

Selected Answer: B

I selected B) as "open inbound ports, maintain bastion hosts, or manage SSH keys" <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html> However Session Manager comes with pretty robust list of prerequisites to put in place (SSM Agent and connectivity to SSM endpoints). On the other side A) come with basically no prerequisites, but it is only for Linux and we do not have info about OSs, so we should assume Windows as well.

upvoted 1 times

✉️ **nour** 1 year ago

Selected Answer: B

The keyword that makes option B follows the AWS Well-Architected Framework is "IAM role." IAM roles provide fine-grained access control and are a recommended best practice in the AWS Well-Architected Framework. By attaching the appropriate IAM role to each instance and using AWS Systems Manager Session Manager to establish a remote SSH session, the solution is using IAM roles to control access and follows a recommended best practice.

upvoted 2 times

✉️ **Shaw605** 1 year, 1 month ago

Answer is B ~ Chat GPT

To meet the requirements with the least operational overhead, the company can use the AWS Systems Manager Session Manager. It is a native AWS service that enables secure and auditable access to instances without the need for remote public IP addresses, inbound security group rules, or Bastion hosts. With AWS Systems Manager Session Manager, the company can establish a secure and auditable session to the EC2 instances and perform administrative tasks without the need for additional operational overhead.

upvoted 1 times

✉️ **Shaw605** 1 year, 1 month ago

Answer is B ~ (Chat GPT)

A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework.

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

upvoted 1 times

Question #38

Topic 1

A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website.

Which solution meets these requirements MOST cost-effectively?

- A. Replicate the S3 bucket that contains the website to all AWS Regions. Add Route 53 geolocation routing entries.
- B. Provision accelerators in AWS Global Accelerator. Associate the supplied IP addresses with the S3 bucket. Edit the Route 53 entries to point to the IP addresses of the accelerators.
- C. Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.
- D. Enable S3 Transfer Acceleration on the bucket. Edit the Route 53 entries to point to the new endpoint.

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

Option A (replicating the S3 bucket to all AWS Regions) can be costly and complex, requiring replication of data across multiple Regions and managing synchronization. It may not provide a significant latency improvement compared to the CloudFront solution.

Option B (provisioning accelerators in AWS Global Accelerator) can be more expensive as it adds an extra layer of infrastructure (accelerators) and requires associating IP addresses with the S3 bucket. CloudFront already includes global edge locations and provides similar acceleration capabilities.

Option D (enabling S3 Transfer Acceleration) can help improve upload speed to the S3 bucket but may not have a significant impact on reducing latency for website visitors.

Therefore, option C is the most cost-effective solution as it leverages CloudFront's caching and global distribution capabilities to decrease latency and improve website performance.

upvoted 25 times

✉️  **TilTil**  1 week ago

Cloudfront is a lovely and affordable CDN for static content.

upvoted 1 times

✉️  **awsgeek75** 2 months, 1 week ago

Selected Answer: C

S3 static website so CloudFront is the best CDN solution for low cost and low latency

- A: Very expensive way of doing this
- B: Makes no sense
- D: Transfer Acc is for upload boosting
- C: CloudFront literally solves this problem

upvoted 1 times

✉️  **A_jaa** 2 months, 1 week ago

Selected Answer: C

Answer-C

upvoted 1 times

✉️  **Ruffyit** 5 months ago

Option A (replicating the S3 bucket to all AWS Regions) can be costly and complex, requiring replication of data across multiple Regions and managing synchronization. It may not provide a significant latency improvement compared to the CloudFront solution.

Option B (provisioning accelerators in AWS Global Accelerator) can be more expensive as it adds an extra layer of infrastructure (accelerators) and requires associating IP addresses with the S3 bucket. CloudFront already includes global edge locations and provides similar acceleration capabilities.

Option D (enabling S3 Transfer Acceleration) can help improve upload speed to the S3 bucket but may not have a significant impact on reducing latency for website visitors.

Therefore, option C is the most cost-effective solution as it leverages CloudFront's caching and global distribution capabilities to decrease latency and improve website performance.

upvoted 1 times

✉️  **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

Amazon CloudFront is a content delivery network (CDN) service that distributes content globally to reduce latency. By setting up a CloudFront distribution in front of the S3 bucket hosting the static website, you can take advantage of its edge locations around the world to deliver content from the nearest location to the users, reducing the latency they experience.

CloudFront automatically caches and replicates content to its edge locations, resulting in faster delivery and lower latency for users worldwide. This solution is highly effective in optimizing performance while keeping costs under control because CloudFront charges are based on actual data transfer and requests, and the pay-as-you-go pricing model ensures that you only pay for what you use.

upvoted 4 times

 **TariqKipkemei** 7 months, 3 weeks ago

Keywords:
Global, Reduce latency, S3, Static Website, Cost effective = Amazon CloudFront

upvoted 4 times

 **james2033** 8 months, 1 week ago

Selected Answer: C
Keyword "Amazon CloudFront" (C).

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option C is the right answer for this.
upvoted 1 times

 **miki111** 8 months, 1 week ago

Option C is the right answer for this.
upvoted 1 times

 **TienHuynh** 9 months ago

Selected Answer: C
key words:
-around the world
-decrease latency
-most cost-effective

answer is C
upvoted 1 times

 **cheese929** 11 months, 3 weeks ago

Selected Answer: C
C is the most cost effective.
upvoted 1 times

 **linux_admin** 12 months ago

Selected Answer: C
Amazon CloudFront is a content delivery network (CDN) that caches content at edge locations around the world, providing low latency and high transfer speeds to users accessing the content. Adding a CloudFront distribution in front of the S3 bucket will cache the static website's content at edge locations around the world, decreasing latency for users accessing the website.

This solution is also cost-effective as it only charges for the data transfer and requests made by users accessing the content from the CloudFront edge locations. Additionally, this solution provides scalability and reliability benefits as CloudFront can automatically scale to handle increased demand and provide high availability for the website.

upvoted 1 times

 **test_devops_aws** 1 year ago

Selected Answer: C
Cloud front
upvoted 1 times

 **bilel500** 1 year ago

Selected Answer: C
Amazon CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as HTML, CSS, JavaScript, and images. It does this by placing cache servers in locations around the world, which store copies of the content and serve it to users from the location that is nearest to them.
upvoted 1 times

 **Bhawesh** 1 year, 1 month ago

My vote is: option B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3. This question has 2 requirements:

1. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications.
2. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

upvoted 1 times

 **Ello2023** 1 year, 1 month ago

Selected Answer: C

C. S3 accelerator is best for uploads to S3, whereas Cloudfront is for content delivery. S3 static website can be the origin which is distributed to Cloudfront and routed by Route 53.

upvoted 3 times

Question #39

Topic 1

A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains more than 10 million rows. The database has 2 TB of General Purpose SSD storage. There are millions of updates against this data every day through the company's website.

The company has noticed that some insert operations are taking 10 seconds or longer. The company has determined that the database storage performance is the problem.

Which solution addresses this performance issue?

- A. Change the storage type to Provisioned IOPS SSD.
- B. Change the DB instance to a memory optimized instance class.
- C. Change the DB instance to a burstable performance instance class.
- D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Correct Answer: B*Community vote distribution*

pazabal Highly Voted 1 year, 3 months ago

Selected Answer: A

- A: Made for high levels of I/O opps for consistent, predictable performance.
 B: Can improve performance of insert opps, but it's a storage performance rather than processing power problem
 C: for moderate CPU usage
 D: for scale read-only replicas and doesn't improve performance of insert opps on the primary DB instance
 upvoted 27 times

cookieMr Highly Voted 9 months, 1 week ago

Selected Answer: A

Option B (changing the DB instance to a memory optimized instance class) focuses on improving memory capacity but may not directly address the storage performance issue.

Option C (changing the DB instance to a burstable performance instance class) is suitable for workloads with varying usage patterns and burstable performance needs, but it may not provide consistent and predictable performance for heavy write workloads.

Option D (enabling Multi-AZ RDS read replicas with MySQL native asynchronous replication) is a solution for high availability and read scaling but does not directly address the storage performance issue.

Therefore, option A is the most appropriate solution to address the performance issue by leveraging Provisioned IOPS SSD storage type, which provides consistent and predictable I/O performance for the Amazon RDS for MySQL database.

upvoted 18 times

TilTil Most Recent 1 week ago

Selected Answer: B

- A. IOPS is about increasing the number of input connections so you can handle more requests. Which may not be the issue.
 B. Having a memory optimized class provides more RAM to execute the queries which take upto 10 secs to complete. More RAM means they can execute faster.
 C and D are distractors. They deal with high availability and timely scalability which are not issues here.
 upvoted 1 times

awsgeek75 2 months, 1 week ago

Selected Answer: A

- Database storage is issue so
 BD is irrelevant
 C is for performance boost (CPU) which won't help with storage issues
 A Fix the storage issue
 upvoted 1 times

A_jaa 2 months, 1 week ago

Selected Answer: A

- Answer-A
 upvoted 1 times

bujuman 3 months ago

Selected Answer: B

Do not misconsider "database storage performance is the problem". I believe the correct answer is B Due to the fact that Memory Optimized EC2 instance family is designed for DB servers perf.

upvoted 1 times

 **pentium75** 3 months ago

But the stem clearly says that storage performance, NOT memory performance, is the problem. More memory won't increase storage performance.

upvoted 2 times

 **aptx4869** 4 months, 4 weeks ago

Selected Answer: A

A is correct answer because it is talking about storage and transaction speed is slow due to it, should change to iops storage instead.

upvoted 1 times

 **Ruffyit** 5 months ago

A: Made for high levels of I/O opps for consistent, predictable performance.

B: Can improve performance of insert opps, but it's a storage performance rather than processing power problem

C: for moderate CPU usage

D: for scale read-only replicas and doesn't improve performance of insert opps on the primary DB instance

upvoted 1 times

 **AWSStudyBuddy** 5 months, 1 week ago

I go with option A. Using Amazon Provisioned IOPS (PIOPS) SSD storage is the best way to solve the performance issue of insert operations taking 10 seconds or longer on an Amazon RDS for MySQL database table with more than 10 million rows and 2 TB of General Purpose SSD storage.

A high-performance storage solution with reliable throughput and minimal latency is PIOPS SSD storage. Workloads like insert operations, which demand high I/O performance, are ideally suited for it.

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: A

Key: database storage performance is the problem.

upvoted 1 times

 **awsleffe** 5 months, 3 weeks ago

Selected Answer: A

Option A is answer - A. Change the storage type to Provisioned IOPS SSD.

The company's issue is related to storage performance, specifically with insert operations. This suggests that the I/O operations are the bottleneck.

Provisioned IOPS SSD storage type is designed to handle the kind of workload the company is experiencing and should help improve the performance of insert operations.

upvoted 2 times

 **awashenko** 5 months, 3 weeks ago

Selected Answer: A

"The company has determined that the database storage performance is the problem."

This is the key statement in the question. Otherwise I would have selected B but this statement here makes A correct.

upvoted 1 times

 **David_Ang** 6 months ago

Selected Answer: A

yeah "A" is correct is the most suitable option for this scenario, because you need to improve the speed of the reading and writing of the storage system.

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: A

The best solution would be to change the storage type to Provisioned IOPS SSD. This allows you to specify a higher level of IOPS provisioned for your workload's needs. Therefore, switching to Provisioned IOPS SSD storage is the most direct way to resolve the storage performance bottleneck causing the slow insert times. The ability to provision high IOPS makes it the best solution for high throughput transactional workloads like this one.

upvoted 4 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected Answer: A

Provisioned IOPS SSD it is.

upvoted 1 times

 **Suvam90** 8 months, 1 week ago

Option A is correct

upvoted 1 times

 **james2033** 8 months, 1 week ago

Selected Answer: A

Keyword "Provisioned IOPS SSD" <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/provisioned-iops.html>
upvoted 2 times

Question #40

Topic 1

A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis. The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days. What is the MOST operationally efficient solution that meets these requirements?

- A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
- B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts. Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
- C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Set up the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days.
- D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts, and set the message retention period to 14 days. Configure consumers to poll the SQS queue, check the age of the message, and analyze the message data as needed. If the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.

Correct Answer: A*Community vote distribution*

Sinaneos Highly Voted 1 year, 5 months ago

Selected Answer: A

Definitely A, it's the most operationally efficient compared to D, which requires a lot of code and infrastructure to maintain. A is mostly managed (firehose is fully managed and S3 lifecycles are also managed)

upvoted 36 times

Kelvin_ke 1 year, 3 months ago

what about the 30 days minimum requirement to transition to S3 glacier?

upvoted 8 times

Abrar2022 10 months, 2 weeks ago

GLACIER IS 7 DAYS REQUIREMENT NOT 30

upvoted 3 times

studis 1 year, 3 months ago

You can directly migrate from S3 standard to glacier without waiting

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

upvoted 4 times

ErnShm 10 months ago

the current article doesn't enable the current option, minimum days are 30

upvoted 1 times

Suvam90 7 months, 1 week ago

No , It's not correct , We can change the storage class in day 0 also using lifecycle policy , I implemented in my project, 30 days is just an example.

upvoted 3 times

caffee 11 months, 2 weeks ago

This constraint is related to moving from Standard to IA/IA-One Zone only. Nothing to do with Glacier

upvoted 3 times

123jh10 Highly Voted 1 year, 5 months ago

Selected Answer: A

Only A makes sense operationally.

If you think D, just consider what is needed to move the message from SQS to S3... you are polling daily 14 TB to take out 1 TB... that's no operationally efficient at all.

upvoted 17 times

Parul25 Most Recent 2 months ago

I understand A is the most operationally efficient option of all but I can't wrap my head around the fact that objects must have a minimum of 30 days before they can transition or expire from Amazon S3. This means that for the first 30 days after an item is created, you cannot transition or remove it. So, how option A can be the best fit?

upvoted 1 times

 **cheroh_tots** 1 month, 1 week ago

The same 30-day minimum applies when you specify a transition from S3 Standard-IA storage to S3 One Zone-IA.
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: A

BCD: Additional infra which company doesn't want

A: Firehose for ingestion and delivery to S3. Lifecycle for managing archive. Fully managed and operationally easy solution

upvoted 1 times

 **A_jaa** 2 months, 1 week ago

Selected Answer: A

Answer-A

upvoted 1 times

 **jjcode** 3 months, 2 weeks ago

so many words...

upvoted 4 times

 **OmegaLambda7XL9** 4 months, 1 week ago

That was an easy A. Kinesis Firehose can load data directly to S3 which makes it the most operationally efficient

upvoted 1 times

 **Ruffyit** 5 months ago

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: A

Key: MOST operationally efficient solution

upvoted 1 times

 **David_Ang** 6 months ago

Selected Answer: A

"A" is simply correct because kinesis firehouse is made for this, SQS standard is not going to support 500 million alerts 2KB each (1 TB) this service is made for requests that are lighter.

upvoted 1 times

 **Ak9kumar** 6 months ago

I picked A. Appeared to be right answer.

upvoted 1 times

 **chandu7024** 6 months, 1 week ago

Should be A

upvoted 1 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected Answer: A

The MOST operationally efficient option is A.

upvoted 1 times

 **james2033** 8 months, 1 week ago

Selected Answer: A

Keyword "Amazon S3 Glacier" (A).

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option A is the right answer for this.

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: A

B suggests launching EC2 instances to ingest and store the alerts, which introduces additional infrastructure management overhead and may not be as cost-effective and scalable as using managed services like Kinesis Data Firehose and S3.

C involves delivering the alerts to an Amazon OpenSearch Service cluster and manually managing snapshots and data deletion. This introduces additional complexity and manual overhead compared to the simpler solution of using Kinesis Data Firehose and S3.

D suggests using SQS to ingest the alerts, but it does not provide the same level of data persistence and durability as storing the alerts directly in S3. Additionally, it requires manual processing and copying of messages to S3, which adds operational complexity.

Therefore, A provides the most operationally efficient solution that meets the company's requirements by leveraging Kinesis Data Firehose to ingest the alerts, storing them in an S3 bucket, and using an S3 Lifecycle configuration to transition data to S3 Glacier for long-term archival, all without the need for managing additional infrastructure.

upvoted 7 times

 **Abrar2022** 10 months, 2 weeks ago

Focus on keywords: Amazon Kinesis Data Firehose delivery stream to ingest the alerts. S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.

upvoted 3 times

Question #41

Topic 1

A company's application integrates with multiple software-as-a-service (SaaS) sources for data collection. The company runs Amazon EC2 instances to receive the data and to upload the data to an Amazon S3 bucket for analysis. The same EC2 instance that receives and uploads the data also sends a notification to the user when an upload is complete. The company has noticed slow application performance and wants to improve the performance as much as possible.

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

- A. Create an Auto Scaling group so that EC2 instances can scale out. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
- B. Create an Amazon AppFlow flow to transfer data between each SaaS source and the S3 bucket. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data. Configure the S3 bucket as the rule's target. Create a second EventBridge (Cloud Watch Events) rule to send events when the upload to the S3 bucket is complete. Configure an Amazon Simple Notification Service (Amazon SNS) topic as the second rule's target.
- D. Create a Docker container to use instead of an EC2 instance. Host the containerized application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon CloudWatch Container Insights to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

Correct Answer: B

Community vote distribution

B (69%)

A (31%)

✉  Six_Fingered_Jose  1 year, 5 months ago

Selected Answer: B

This question just screams AppFlow (SaaS integration)
<https://aws.amazon.com/appflow/>

upvoted 32 times

✉  Six_Fingered_Jose 1 year, 5 months ago

configuring Auto-Scaling also takes time when compared to AppFlow,
 in AWS's words "in just a few clicks"

> Amazon AppFlow is a fully managed integration service that enables you to securely transfer data between Software-as-a-Service (SaaS) applications like Salesforce, SAP, Zendesk, Slack, and ServiceNow, and AWS services like Amazon S3 and Amazon Redshift, in just a few clicks

upvoted 19 times

✉  jdr75  11 months, 4 weeks ago

Selected Answer: A

It says "LEAST operational overhead" (ie do it in a way it's the less work for me).

If you know a little Amazon AppFlow (see some videos) you'll see you'll need time to configure and test it, and at the end cope with the errors during the extraction and load the info to the target.

The customer in the example ALREADY has some EC2 that do the work, the only problem is the performance, that WILL be improved scaling out and adding a queue (SNS) to decouple the work of notify the user.

The operational load of doing this is LESS than configuring AppFlow.

upvoted 29 times

✉  pentium75 3 months ago

"Operational overhead" refers to operation of the solution once it's deployed, it's not about setting it up. EC2 instances that retrieve data from A and write it to B are nonsense, that's what cloud services are meant for.

upvoted 4 times

✉  awsgeek75 2 months, 1 week ago

With AWS, a managed service is "less operational overhead" regardless of the complexity of the setup. AppFlow management is less of a headache when compared to EC2 management so A cannot be correct. EC2 has a setup overhead of OS/Application/Code hooks, security etc. continuous patching/upgrading seems like more than what you'll need to do with SaaS.

B is the correct answer.

upvoted 3 times

✉  SMALLE  1 month, 2 weeks ago

Selected Answer: B

Amazon AppFlow is a fully managed integration service that helps you securely transfer data between software as a service (SaaS) applications such as Salesforce, SAP, Google Analytics, Facebook Ads, and ServiceNow, and AWS services such as Amazon Simple Storage Service (S3) and Amazon Redshift in just a few clicks.

<https://aws.amazon.com/appflow/>

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/appflow/>

"With Amazon AppFlow automate bi-directional data flows between SaaS applications and AWS services in just a few clicks."

If you want to pass the exam, choose B, regardless of your personal experience! Always use AWS managed services for "least operational overhead"

upvoted 4 times

✉ **MoshirGCP** 4 months ago

SaaS - AppFlow

upvoted 2 times

✉ **OmegaLambda7XL9** 4 months, 1 week ago

Yea , I think this question is looking for Amazon Appflow.I also feel like it would be easier to set up Autoscaling for the already existing EC2 instances in the short term but then the fact that this software integrates with a lot of SAAS services means using Amazon Appflow will work reduce operational overhead in the long term

upvoted 4 times

✉ **Ruffyit** 5 months ago

<https://docs.aws.amazon.com/appflow/latest/userguide/what-is-appflow.html>

upvoted 1 times

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

Selected Answer: B

<https://aws.amazon.com/appflow/>

upvoted 1 times

✉ **ACloud_Guru15** 5 months, 1 week ago

Selected Answer: B

B suits the requirement

upvoted 1 times

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

Selected Answer: A

The problem with A is you need to add ALB or ELB in front of ASG, and update DNS for your application, so B seems like a better choice.

upvoted 1 times

✉ **awashenko** 5 months, 3 weeks ago

This is a tough one. If they were not already using EC2 the answer would for sure be AppFlow (B). The question says "least operational overhead" so I feel like it takes more work to configure AppFlow than it does to create auto scaling in EC2.

If I had this question on the test, I would likely go with AppFlow so B

upvoted 2 times

✉ **Techi47** 6 months ago

Selected Answer: A

While option B utilizes managed services and can be a valid approach, it's important to note that Amazon AppFlow is primarily designed for data integration and synchronization between various SaaS applications and AWS services. It may introduce an additional layer of complexity compared to directly handling the uploads with EC2 instances.

Ultimately, the choice between Option A and Option B depends on specific factors such as the existing architecture, the nature of data transfers, and any potential advantages offered by using Amazon AppFlow for data integration.

If the primary concern is to improve performance for data uploads and user notifications without introducing new services, Option A (Auto Scaling group with S3 event notifications) would likely be the simpler and more operationally efficient choice. However, if data integration between SaaS sources and the S3 bucket is a critical aspect of the application, Option B might be a more suitable approach.

upvoted 2 times

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

Selected Answer: B

SaaS Integration = Amazon AppFlow

upvoted 2 times

✉ **hsinchang** 8 months ago

Selected Answer: B

SaaS -> AppFlow

upvoted 1 times

✉ **miki111** 8 months, 1 week ago

Option B is the right answer.

upvoted 1 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: B

Option A suggests using an Auto Scaling group to scale out EC2 instances, but it does not address the potential bottleneck of slow application performance and the notification process.

Option C involves using Amazon EventBridge (CloudWatch Events) rules for data output and S3 uploads, but it introduces additional complexity with separate rules and does not specifically address the slow application performance.

Option D suggests containerizing the application and using Amazon Elastic Container Service (Amazon ECS) with CloudWatch Container Insights, which may involve more operational overhead and setup compared to the simpler solution provided by Amazon AppFlow.

Therefore, option B offers the most streamlined solution with the least operational overhead by utilizing Amazon AppFlow for data transfer, configuring S3 event notifications for upload completion, and leveraging Amazon SNS for notifications without requiring additional infrastructure management.

upvoted 7 times

 **Abrar2022** 10 months, 1 week ago

So true, This question just screams AppFlow (SaaS integration)

upvoted 1 times

Question #42

Topic 1

A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC. The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other. However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway. The company is concerned about data transfer charges. What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

- A. Launch the NAT gateway in each Availability Zone.
- B. Replace the NAT gateway with a NAT instance.
- C. Deploy a gateway VPC endpoint for Amazon S3.
- D. Provision an EC2 Dedicated Host to run the EC2 instances.

Correct Answer: C

Community vote distribution

C (99%)

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

Selected Answer: C

Deploying a gateway VPC endpoint for Amazon S3 is the most cost-effective way for the company to avoid Regional data transfer charges. A gateway VPC endpoint is a network gateway that allows communication between instances in a VPC and a service, such as Amazon S3, without requiring an Internet gateway or a NAT device. Data transfer between the VPC and the service through a gateway VPC endpoint is free of charge, while data transfer between the VPC and the Internet through an Internet gateway or NAT device is subject to data transfer charges. By using a gateway VPC endpoint, the company can reduce its data transfer costs by eliminating the need to transfer data through the NAT gateway to access Amazon S3. This option would provide the required connectivity to Amazon S3 and minimize data transfer charges.

upvoted 63 times

✉  **Bmarodi** 9 months, 3 weeks ago

Very good explanation!

upvoted 7 times

✉  **johne42** 7 months ago

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 5 times

✉  **OmegaLambda7XL9** 4 months, 1 week ago

Precisely

upvoted 3 times

✉  **awsgeek75**  2 months, 1 week ago

Selected Answer: C

Gateway VPC allows direct access to S3 without going through public internet. This is the de-facto way to save cost for S3 to VPC traffic. Correct answer is C

upvoted 1 times

✉  **MoshiurGCP** 4 months ago

Avoid regional data transfer charge - VPC endpoint

upvoted 2 times

✉  **Ruffyit** 5 months ago

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 1 times

✉  **ACloud_Guru15** 5 months, 1 week ago

Selected Answer: C

Gateway Endpoint bests suits the requirement

upvoted 1 times

✉  **srinivasmn** 6 months, 1 week ago

Answer is C: An S3 VPC endpoint provides a way for an S3 request to be routed through to the Amazon S3 service, without having to connect a subnet to an internet gateway. The S3 VPC endpoint is what's known as a gateway endpoint.

upvoted 1 times

✉  **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

the EC2 instances are downloading and uploading images to S3, configuring a gateway VPC endpoint will allow them to access S3 without crossing Availability Zones or regions, eliminating regional data transfer charges

upvoted 1 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected Answer: C

Gateway VPC endpoints provide reliable connectivity to Amazon S3 without requiring an internet gateway or a NAT device for your VPC.
upvoted 2 times

 **miki111** 8 months, 1 week ago

Option C is the right answer.

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

By deploying a gateway VPC endpoint for S3, the company can establish a direct connection between their VPC and S3 without going through the internet gateway or NAT gateway. This enables traffic between the EC2 and S3 to stay within the Amazon network, avoiding Regional data transfer charges.

A suggests launching the NAT gateway in each AZ. While this can help with availability and redundancy, it does not address the issue of data transfer charges, as the traffic would still traverse the NAT gateways and incur data transfer fees.

B suggests replacing the NAT gateway with a NAT instance. However, this solution still involves transferring data between the instances and S3 through the NAT instance, which would result in data transfer charges.

D suggests provisioning an EC2 Dedicated Host to run the EC2. While this can provide dedicated hardware for the instances, it does not directly address the issue of data transfer charges.

upvoted 4 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: C

Option C is the answer.

upvoted 1 times

 **linux_admin** 12 months ago

Selected Answer: C

A gateway VPC endpoint is a fully managed service that allows connectivity from a VPC to AWS services such as S3 without the need for a NAT gateway or a public internet gateway. By deploying a Gateway VPC endpoint for Amazon S3, the company can ensure that all S3 traffic remains within the VPC and does not cross the regional boundary. This eliminates regional data transfer charges and provides a more cost-effective solution for the company.

upvoted 1 times

 **AndyMartinez** 1 year, 1 month ago

Selected Answer: C

C - gateway VPC endpoint.

upvoted 1 times

 **secdaddy** 1 year, 2 months ago

'Regional' data transfer isn't clear but I think we have to assume this means the traffic stays in the region.

The two options that seem possible are NAT gateway per AZ vs privatelink gateway endpoints per AZ.

privatelink/endpoints do have costs (url below)

privatelink endpoint / LB costs look lower than NAT gateway costs

privatelink doesn't incur inter-AZ data transfer charges (if in the same region) as NAT gateways do which goes towards the key requirement stated

good writeup here : <https://www.vantage.sh/blog/nat-gateway-vpc-endpoint-savings>

<https://aws.amazon.com/privatelink/pricing/>

<https://aws.amazon.com/vpc/pricing/>

<https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-costs/>

upvoted 2 times

 **pazabal** 1 year, 3 months ago

Selected Answer: C

C, privately connects vpc to aws services via privatelink. Doesn't require nat gateway, vpn or direct connect. Data doesn't leave amazon network so there are no data transfer charges

A, used to enable instances in private subnets to connect to internet or aws services, data transferred is charged

B, similar to nat gateway

D, not related to data transfer

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: C

Option C (correct). Deploy a gateway VPC endpoint for Amazon S3.

A VPC endpoint for Amazon S3 allows you to access Amazon S3 resources within your VPC without using the Internet or a NAT gateway. This means that data transfer between your EC2 instances and S3 will not incur Regional data transfer charges.

Option A (wrong), launching a NAT gateway in each Availability Zone, would not avoid data transfer charges because the NAT gateway would still be used to access S3.

Option B (wrong), replacing the NAT gateway with a NAT instance, would also not avoid data transfer charges as it would still require using the Internet or a NAT gateway to access S3.

Option D (wrong), provisioning an EC2 Dedicated Host, would not affect data transfer charges as it only pertains to the physical host that the EC2 instances are running on and not the data transfer charges for accessing.

upvoted 3 times

 **Morinator** 1 year, 3 months ago

Selected Answer: C

VPC endpoint

upvoted 1 times

Question #43

Topic 1

A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal impact on internet connectivity for internal users.

Which solution meets these requirements?

- A. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint.
- B. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.
- C. Order daily AWS Snowball devices. Load the data onto the Snowball devices and return the devices to AWS each day.
- D. Submit a support ticket through the AWS Management Console. Request the removal of S3 service limits from the account.

Correct Answer: B

Community vote distribution

B (99%)

✉  **Sinaneos**  1 year, 5 months ago

Selected Answer: B

- A: VPN also goes through the internet and uses the bandwidth
 C: daily Snowball transfer is not really a long-term solution when it comes to cost and efficiency
 D: S3 limits don't change anything here

So the answer is B
 upvoted 33 times

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

Selected Answer: B

Option B (correct). Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.

AWS Direct Connect is a network service that allows you to establish a dedicated network connection from your on-premises data center to AWS. This connection bypasses the public Internet and can provide more reliable, lower-latency communication between your on-premises application and Amazon S3. By directing backup traffic through the AWS Direct Connect connection, you can minimize the impact on your internet bandwidth and ensure timely backups to S3.

upvoted 27 times

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

Option A (wrong), establishing AWS VPN connections and proxying all traffic through a VPC gateway endpoint, would not necessarily minimize the impact on internet bandwidth as it would still utilize the public Internet to access S3.

Option C (wrong), using AWS Snowball devices, would not address the issue of internet bandwidth limitations as the data would still need to be transferred over the Internet to and from the Snowball devices.

Option D (wrong), submitting a support ticket to request the removal of S3 service limits, would not address the issue of internet bandwidth limitations and would not ensure timely backups to S3.

upvoted 8 times

✉  **OmegaLambda7XL9** 4 months, 1 week ago

Snowball isn't timely since it takes days after ordering to receive the Snowball devices and days to have it shipped and backed up
 upvoted 2 times

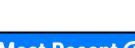
✉  **Bofi** 1 year, 1 month ago

Option C is wrong so is your reason. you do not need internet to load data into Snowball Devices. if you are using snow cone for example, u will connect it to your on-premises device directly for loading and Aws will load it in the cloud. However, it not effective to do that everyday, hence option B is the better choice.

upvoted 3 times

✉  **Buruguduystunstugudunstuy** 1 year ago

You're right Option B is the correct answer. I answered Option B as the correct answer above.
 upvoted 1 times

✉  **awsgeek75**  2 months, 1 week ago

Selected Answer: B

Direct Connect is the only working solution.

- A: VPN uses same bandwidth so doesn't solve anything
 C: Snowball devices are physical devices requiring physical shipment so wrong solution
 D: There are no S3 service limitations in the account related to this problem

upvoted 1 times

 **NicolasB** 3 months ago

Option B.

AWS Direct Connect link your on-premise instance with VPC, and all traffic will bypass your Internet Service Provider.

[upvoted 1 times](https://docs.aws.amazon.com/directconnect/latest/UserGuide>Welcome.html</p></div><div data-bbox=)

 **MoshiurGCP** 4 months ago

Resolve Internet connection problem - Direct Connect

upvoted 1 times

 **Ruffyit** 5 months ago

AWS Direct Connect is a network service that allows you to establish a dedicated network connection from your on-premises data center to AWS. This connection bypasses the public Internet and can provide more reliable, lower-latency communication between your on-premises application and Amazon S3. By directing backup traffic through the AWS Direct Connect connection, you can minimize the impact on your internet bandwidth and ensure timely backups to S3.

upvoted 1 times

 **AWSStudyBuddy** 5 months, 1 week ago

Selected Answer: B

I picked option B, because AWS Direct Connect offers a dedicated, secure, high-performance connection that may circumvent bandwidth restrictions and minimize the impact on internet access, AWS Direct Connect is the ideal choice for backing up data to Amazon S3. Some solutions are not as good because they are not as scalable, reliable, or secure as VPN connections, Snowball devices, or reducing S3 service constraints.

upvoted 2 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: B

Key: time sensitive. So snowball does not apply here.

upvoted 1 times

 **srinivasmn** 6 months, 1 week ago

Right option is C,, In AWS Direct Connect, the network is not fluctuating and provides a consistent experience, while in AWS VPN the VPN is connected with shared and public networks, so the bandwidth and latency fluctuate. Hence direct connect is better choice than virtual connect.

upvoted 1 times

 **srinivasmn** 6 months, 1 week ago

Typo correction to my my above comment. The right option is B.

upvoted 1 times

 **chandu7024** 6 months, 1 week ago

Option B Correct. Reason is that, Direct connect will not use internet. But it will take good amount of time to establish the connectivity.

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: B

AWS Direct Connect is a dedicated network connection between your on-premises network and AWS. This provides a private, high-bandwidth connection that is not subject to the same internet bandwidth limitations as traditional internet connections. This will allow for timely backups to Amazon S3 without impacting internet connectivity for internal users.

upvoted 2 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected Answer: B

AWS Direct Connect cloud service is the shortest path to your AWS resources. While in transit, your network traffic remains on the AWS global network and never touches the public internet. This reduces the chance of hitting bottlenecks or unexpected increases in latency.

<https://aws.amazon.com/directconnect/#:~:text=The-AWS%20Direct%20Connect,-cloud%20service%20is>

upvoted 2 times

 **miki111** 8 months, 1 week ago

Option B is the right answer.

upvoted 1 times

 **Kaab_B** 8 months, 2 weeks ago

Selected Answer: B

This is long-term and provides solution for internet speed as well

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B

AWS Direct Connect provides a dedicated network connection between on-premises and AWS, bypassing public internet. By establishing this connection for backup traffic, company can ensure fast and reliable transfers between their on-premises and S3 without impacting their internet connectivity for internal users. This provides a dedicated and high-speed connection that is well-suited for data transfers and minimizes impact on internet bandwidth limitations.

While option A can provide a secure connection, it still utilizes internet bandwidth for data transfer and may not effectively address issue of limited

bandwidth.

While option C can work for occasional large data transfers, it may not be suitable for frequent backups and can introduce additional operational overhead.

D, submitting a support ticket to request removal of S3 service limits, does not address issue of internet bandwidth limitations and is not a relevant solution for given requirements.

upvoted 3 times

 **emanuelmelis** 9 months, 1 week ago

Galleta siempre veo tus comentarios! sos crack!

upvoted 1 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: B

Option B meets these requirements.

upvoted 1 times

 **Abrar2022** 10 months, 1 week ago

This question can confuse you as it mentions internet and Direct Connect bypasses internet and uses dedicated network connections. So don't be fooled - keyword in the question is "minimize the impact internet bandwidth for internal users"

upvoted 1 times

Question #44

Topic 1

A company has an Amazon S3 bucket that contains critical data. The company must protect the data from accidental deletion.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.
- C. Create a bucket policy on the S3 bucket.
- D. Enable default encryption on the S3 bucket.
- E. Create a lifecycle policy for the objects in the S3 bucket.

Correct Answer: BD

Community vote distribution

AB (98%)

✉  **Uhrien**  1 year, 5 months ago

Selected Answer: AB

The correct solution is AB, as you can see here:

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-audit-deleted-missing-objects/>

It states the following:

To prevent or mitigate future accidental deletions, consider the following features:

Enable versioning to keep historical versions of an object.

Enable Cross-Region Replication of objects.

Enable MFA delete to require multi-factor authentication (MFA) when deleting an object version.

upvoted 56 times

✉  **cookieMr**  9 months, 1 week ago

Selected Answer: AB

Enabling versioning on S3 ensures multiple versions of object are stored in bucket. When object is updated or deleted, new version is created, preserving previous version.

Enabling MFA Delete adds additional layer of protection by requiring MFA device to be present when attempting to delete objects. This helps prevent accidental or unauthorized deletions by requiring extra level of authentication.

C. Creating a bucket policy on S3 is more focused on defining access control and permissions for bucket and its objects, rather than protecting against accidental deletion.

D. Enabling default encryption on S3 ensures that any new objects uploaded to bucket are automatically encrypted. While encryption is important for data security, it does not directly address accidental deletion.

E. Creating lifecycle policy for objects in S3 allows for automated management of objects based on predefined rules. While this can help with data retention and storage cost optimization, it does not directly protect against accidental deletion.

upvoted 10 times

✉  **mmrakib**  2 weeks, 6 days ago

Selected Answer: AB

AB will be the correct answer.

upvoted 1 times

✉  **sidharthwader** 4 weeks ago

This could be done if we enable MFA delete on the bucket but in order to enable this bucket versioning must be done. Hence A and B would be the answer.

upvoted 1 times

✉  **Conster** 1 month, 1 week ago

I am getting so confused about what answers I should study. The answers don't match here or in ChatGPT. Can anyone who just took the exam, and passed, point me in the right direction? TIA!

upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

Selected Answer: AB

B: MFA to put an extra step to verify deletion and stop from accidental deletion

A: Versioning for recovery of objects that were deleted accidentally even with MFA

Remember, the solution is not required to STOP from deletion. It just wants to STOP ACCIDENTAL deletion.

CDE offer nothing related to accidental deletion
upvoted 1 times

 **rt_7777** 3 months ago

Not sure why Answer is BD. I am trying to rationalize it. What I guess could be to address keyword "critical data" where set default encryption is just enhance the security of stored data but does not prevent from deletion. This will have 2 options A, B for that. B is make sense to ensure user know what to delete on second layer. For option A, it just help you to audit and recovered what was accidentally deleted but does not "prevent" accidentally delete.

upvoted 1 times

 **fb4afde** 3 months, 2 weeks ago

Selected Answer: AB

Agree, s3 encryption does not prevent deletion
upvoted 2 times

 **jjcode** 3 months, 2 weeks ago

Yeah so.. encryption is enabled by default on S3, sooooo why is the answer D.

Starting today, Amazon Simple Storage Service (Amazon S3) encrypts all new objects by default. Now, S3 automatically applies server-side encryption (SSE-S3) for each new object, unless you specify a different encryption option.

upvoted 1 times

 **Leo1688** 3 months, 3 weeks ago

What's the correct answers?
upvoted 1 times

 **MoshiurGCP** 4 months ago

Prevent accidental deletion - MFA, Versioning
upvoted 1 times

 **Marco_St** 4 months, 2 weeks ago

Selected Answer: AB

MFA will add extra security of deleting item from s3

Versioning will make the data recovering

upvoted 1 times

 **JustEugen** 4 months, 3 weeks ago

Selected Answer: AB

A) <https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>

Versioning-enabled buckets can help you recover objects from accidental deletion or overwrite. For example, if you delete an object, Amazon S3 inserts a delete marker instead of removing the object permanently. The delete marker becomes the current object version. If you overwrite an object, it results in a new object version in the bucket. You can always restore the previous version

B) <https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiFactorAuthenticationDelete.html>

upvoted 1 times

 **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: AC

A - object must be versioned, so multiple uploads won't cause data loss

C - even though objects are versioned you have to specify deny policy for delete actions on bucket level to ensure they can't be deleted

B - MFA helps with authentication, doesn't protect if user has permission to delete

upvoted 1 times

 **pentium75** 3 months ago

You're asked to prevent ACCIDENTAL deletion, not deletion.

upvoted 3 times

 **Ruffyit** 5 months ago

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-audit-deleted-missing-objects/>

upvoted 1 times

 **AWSStudyBuddy** 5 months, 1 week ago

Selected Answer: AB

The two most effective steps a solutions architect can take to protect an Amazon S3 bucket from accidental deletion are:

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.

Versioning keeps multiple versions of objects in the S3 bucket, even when they are overwritten or deleted. This allows you to recover objects that have been accidentally deleted.

MFA Delete requires you to enter a one-time password from a multi-factor authentication (MFA) device before you can delete an object in the S3 bucket. This helps to prevent accidental deletions.

upvoted 1 times

 **kagitala** 5 months, 2 weeks ago

A+B is the correct answer

upvoted 1 times

Question #45

A company has a data ingestion workflow that consists of the following:

- An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries
- An AWS Lambda function to process the data and record metadata

The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job.

Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Choose two.)

- A. Deploy the Lambda function in multiple Availability Zones.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic.
- C. Increase the CPU and memory that are allocated to the Lambda function.
- D. Increase provisioned throughput for the Lambda function.
- E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue.

Correct Answer: BE

Community vote distribution

BE (98%)

✉️ **Incognito013** Highly Voted 1 year, 5 months ago

A, C, D options are out, since Lambda is fully managed service which provides high availability and scalability by its own

Answers are B and E

upvoted 25 times

✉️ **Oluseun** 1 year ago

There are times you do have to increase lambda memory for improved performance though. But not in this case.

upvoted 4 times

✉️ **Sinaneos** Highly Voted 1 year, 5 months ago

Selected Answer: BE

BE so that the lambda function reads the SQS queue and nothing gets lost

upvoted 10 times

✉️ **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: BE

BE is correct as SQS ensures the messages are stored in a queue for processing.

A: No issue with Lambda availability so this solution is wrong

C: No issues with CPU or memory so no value added by this step also

D: This is not a provisioning issue so provisioning more Lambda won't solve the re-execution issues. The missed messages will still be lost
upvoted 3 times

✉️ **OmegaLambda7XL9** 4 months, 1 week ago

Since network timeout is the issue here, introduce SQS and read from it , that way when network goes down, data still remains in the queue and when connectivity is back, the lambda function can continue from the last data in the queue

upvoted 2 times

✉️ **Ruffyit** 5 months ago

the correct combination of actions to ensure that the Lambda function ingests all data in the future is to create an SQS queue and subscribe it to the SNS topic (option B) and modify the Lambda function to read from the SQS queue (option E).

upvoted 1 times

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

Selected Answer: BE

Key: network connectivity issues

upvoted 1 times

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

Selected Answer: BE

This one told you the answer in the answer choices. Just add the word THEN between B and E and there ya go.

upvoted 1 times

✉️ **Abdou1604** 7 months, 2 weeks ago

B and E , the FAN out model , SQS will help to retrieve the work and delayed processing

upvoted 1 times

Guru4Cloud 7 months, 2 weeks ago

Selected Answer: BE

B) Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic.

E) Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue.

upvoted 1 times

TariqKipkemei 7 months, 3 weeks ago

Selected Answer: BE

BE is most logical answer.

upvoted 1 times

miki111 8 months, 1 week ago

Option BE is the right answer.

upvoted 1 times

cookieMr 9 months, 1 week ago

Selected Answer: BE

A. Deploying the Lambda function in multiple Availability Zones improves availability and fault tolerance but does not guarantee ingestion of all data.

C. Increasing CPU and memory allocated to the Lambda function may improve its performance but does not address the issue of connectivity failures.

D. Increasing provisioned throughput for the Lambda function is not applicable as Lambda functions are automatically scaled by AWS and provisioned throughput is not configurable.

Therefore, the correct combination of actions to ensure that the Lambda function ingests all data in the future is to create an SQS queue and subscribe it to the SNS topic (option B) and modify the Lambda function to read from the SQS queue (option E).

upvoted 7 times

Bmarodi 9 months, 3 weeks ago

Selected Answer: BE

The combination of actions a solutions architect take to ensure that the Lambda function ingests all data in the future, are by Creating an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic, and Modifying the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue

upvoted 1 times

linux_admin 12 months ago

Selected Answer: BE

B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic. This will decouple the ingestion workflow and provide a buffer to temporarily store the data in case of network connectivity issues.

E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue. This will allow the Lambda function to process the data from the SQS queue at its own pace, decoupling the data ingestion from the data delivery and providing more flexibility and fault tolerance.

upvoted 3 times

Ello2023 1 year, 1 month ago

Help

Can SQS Queue have multiple consumers so SNS and Lambda can consume at the same time?

upvoted 1 times

Lonojack 1 year, 1 month ago

How come no one's acknowledged the connection issue? Obviously we know we need SQS as a buffer for messages when the system fails. But shouldn't we consider provisioned iops to handle the connectivity so maybe it will be less likely to lose connectivity and fail in the first place?

upvoted 2 times

ProfXsamson 1 year, 1 month ago

What does connectivity have to do with Provisioned IOPS which is supposed to enhance I/O rate?

upvoted 2 times

SilentMilli 1 year, 2 months ago

Selected Answer: BE

To ensure that the Lambda function ingests all data in the future, the solutions architect can create an Amazon Simple Queue Service (Amazon SQS) queue and subscribe it to the SNS topic. This will allow the data notifications to be queued in the event of a network connectivity issue, rather than being lost. The solutions architect can then modify the Lambda function to read from the SQS queue, rather than from the SNS topic directly. This will allow the Lambda function to process any queued data as soon as the network connectivity issue is resolved, without the need for manual intervention.

By using an SQS queue as a buffer between the SNS topic and the Lambda function, the company can improve the reliability and resilience of the ingestion workflow. This approach will help ensure that the Lambda function ingests all data in the future, even when there are network connectivity issues.

upvoted 3 times

Question #46

Topic 1

A company has an application that provides marketing services to stores. The services are based on previous purchases by store customers. The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers. Some of the files can exceed 200 GB in size.

Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included. The company wants administrators to be alerted if PII is shared again. The company also wants to automate remediation.

What should a solutions architect do to meet these requirements with the LEAST development effort?

- A. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Inspector to scan the objects in the bucket. If objects contain PII, trigger an S3 Lifecycle policy to remove the objects that contain PII.
- B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
- C. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
- D. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Email Service (Amazon SES) to trigger a notification to the administrators and trigger an S3 Lifecycle policy to remove the objects that contain PII.

Correct Answer: B*Community vote distribution*

Gatt Highly Voted 1 year, 4 months ago

I have a problem with answer B. The question says: "automate remediation". B says that you inform the administrator and he removes the data manually, that's not automating remediation. Very weird, that would mean that D is correct - but it's so much harder to implement.

upvoted 30 times

Joxtat 1 year, 2 months ago

Pay attention to the entire question as in What should a solutions architect do to meet these requirements with the LEAST development effort? That is why Macie is used. Answer is B

upvoted 7 times

Maxpayne009 11 months ago

Macie has file size limit and clearly question mentions 200GB filesizes are possible. Lambda is the way to go ..

upvoted 5 times

pentium75 3 months ago

You're confusing "files to retrieve samples from" with "files to analyze". Macie can analyze 20 GB files.

upvoted 2 times

ronaldchow 1 year, 3 months ago

By "automate remediation", I thought it meant to use Amazon Macie to automate discovery on personally identifiable information. <https://aws.amazon.com/macie/>

- Discover sensitive data across your S3 environment to increase visibility and automated remediation of data security risks.

upvoted 2 times

Horaii 1 year, 3 months ago

That is correct, "Automate remediation" is not possible if you chose the B

upvoted 2 times

karbob 1 year, 2 months ago

what about LEAST development effort on
custom scanning algorithms and If objects contain PII
upvoted 3 times

grzeev Highly Voted 1 year, 4 months ago

Selected Answer: B

Amazon Macie is a data security and data privacy service that uses machine learning (ML) and pattern matching to discover and protect your sensitive data

upvoted 18 times

grzeev 1 year, 4 months ago

Macie automatically detects a large and growing list of sensitive data types, including personally identifiable information (PII) such as names, addresses, and credit card numbers. It also gives you constant visibility of the data security and data privacy of your data stored in Amazon S3
upvoted 10 times

 **JavierEF** Most Recent 3 days, 14 hours ago

Selected Answer: D

I'm going to with D. A is not the answer because Amazon Inspector does not detect PII. B could be except for the "automate remediation". C does not automate remediation. Even with the extra development effort, D is the answer that suits better the question.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: B

Always prefer AWS managed solution, especially when they have a SaaS over custom solution when the ask for "with the LEAST development effort". Anything else doesn't really matter.

B is the only choice as Macie is PII detection and SNS is for alerting.

upvoted 2 times

 **JTruong** 2 months, 3 weeks ago

Auto remediation is a Macie's feature so B is CORRECT

<https://aws.amazon.com/macie/#:~:text=Discover%20sensitive%20data%20across%20your,remediation%20of%20data%20security%20risks>.

upvoted 3 times

 **NicolasB** 2 months, 4 weeks ago

Selected Answer: B

Each time the question asks about PII and security posture of your organization in S3, the option with Macie should be considered.

<https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html>

upvoted 1 times

 **rt_7777** 3 months ago

I am in the consideration B and D. Based on the requirement, it need to detect and notify administrator when PII data uploaded. And with LEAST development effort - option B definite an answer. However, it does not meet the automate remediation which need some extra configuration. I opt for D for the reason meeting 3 points, but development (on coding) could be extra/ also subject to the skillset and experience.

Any thought?

upvoted 1 times

 **SaurabhTiwari1** 3 months, 1 week ago

Selected Answer: B

Keywords-

Sensitive data, Alert, PII = Macie

upvoted 1 times

 **anikolov** 3 months, 1 week ago

Selected Answer: D

Amazon Macie quotas: <https://docs.aws.amazon.com/macie/latest/user/macie-quotas.html>

upvoted 1 times

 **pentium75** 3 months ago

The size limits are about SAMPLE files, not files to analyze.

upvoted 1 times

 **anikolov** 1 month, 4 weeks ago

On the same link above:

Size of an individual file to analyze:

Adobe Portable Document Format (.pdf) file: 1,024 MB

Apache Avro object container (.avro) file: 8 GB

Apache Parquet (.parquet) file: 8 GB

Email message (.eml) file: 20 GB

GNU Zip compressed archive (.gz or .gzip) file: 8 GB

Microsoft Excel workbook (.xls or .xlsx) file: 512 MB

Microsoft Word document (.doc or .docx) file: 512 MB

Non-binary text file: 20 GB

TAR archive (.tar) file: 20 GB

ZIP compressed archive (.zip) file: 8 GB

If a file is larger than the applicable quota, Macie doesn't analyze any data in the file.

and we have mention that "Some of the files can exceed 200 GB in size."

upvoted 1 times

 **MoshiurGCP** 4 months ago

Amazon Macie to scan the object

upvoted 1 times

 **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: D

B is incorrect because macie can't process such big files

upvoted 1 times

✉ **Eneiss** 4 months, 4 weeks ago

I would have picked B but D must actually be the correct answer for 2 reasons:

- B does not automate remediation
- Macie does not support 200GB files:

Size of an Amazon S3 object to retrieve and reveal sensitive data samples from:

Apache Avro object container (.avro) file: 70 MB

Apache Parquet (.parquet) file: 100 MB

CSV (.csv) file: 255 MB

GNU Zip compressed archive (.gz or .gzip) file: 90 MB

JSON or JSON Lines (.json or .jsonl) file: 25 MB

Microsoft Excel workbook (.xlsx) file: 20 MB

Non-binary text (text/plain) file: 100 MB

TSV (.tsv) file: 75 MB

ZIP compressed archive (.zip) file: 355 MB

(source: <https://docs.aws.amazon.com/macie/latest/user/macie-quotas.html>)

So weird question because usually PII => Macie, but not this time because of specific constraints...

upvoted 3 times

✉ **baku98** 3 months, 3 weeks ago

Some quotas can be increased, while others cannot. To request an increase to a quota, use the Service Quotas console. To learn how to request an increase, see Requesting a quota increase in the Service Quotas User Guide. If a quota isn't available on the Service Quotas console, use the service limit increase form on the AWS Support Center Console to request an increase to the quota.

upvoted 1 times

✉ **Ruffyit** 5 months ago

Amazon Macie is a data security and data privacy service that uses machine learning (ML) and pattern matching to discover and protect your sensitive data

upvoted 1 times

✉ **sweetheatmn** 5 months ago

Selected Answer: B

Despite that B does not look to automate remediation and requires admin interaction, it is the best fit as Macie is the designated service for scanning S3 and finding PII

can not be D because how can a lambda trigger a life cycle policy to remove PII, this is not practical and life cycle policies does not remove files by an invocation

upvoted 1 times

✉ **GB_12345** 5 months, 2 weeks ago

Selected Answer: D

The Key words are PII, 200 GB, and automate remediation

A) Amazon Inspector is about software & network vulnerability detection

B) Amazon Macie is for PII detection, but it has severe quota limitations, i.e. it will only retrieve and analyze a 25MB JSON file or 100MB text file (wonder if people save JSON as text to analyze bigger files)

Also it's not automatically remediating the problem files

C) won't automatically remediate the problem files

D) While more development effort required than using Macie, it will actually (once developed) analyze and automatically remove the bad file

This is a horrible question, and the real answer would be to break down the data into smaller chunks and use Macie on that

upvoted 4 times

✉ **baku98** 3 months, 3 weeks ago

B: Some quotas can be increased, while others cannot. To request an increase to a quota, use the Service Quotas console. To learn how to request an increase, see Requesting a quota increase in the Service Quotas User Guide. If a quota isn't available on the Service Quotas console, use the service limit increase form on the AWS Support Center Console to request an increase to the quota.

upvoted 1 times

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

Selected Answer: D

What a horrible question...it wants to automate remediation but with LEAST development effort, and then with that 200GB size...

upvoted 2 times

✉ **baku98** 3 months, 3 weeks ago

B: Some quotas can be increased, while others cannot. To request an increase to a quota, use the Service Quotas console. To learn how to request an increase, see Requesting a quota increase in the Service Quotas User Guide. If a quota isn't available on the Service Quotas console, use the service limit increase form on the AWS Support Center Console to request an increase to the quota.

upvoted 1 times

✉ **RSavio** 5 months, 3 weeks ago

Option A, while using Amazon S3 and Amazon inspector, doesn't provide as specialized PII detection capabilities as Amazon Macie.

Option C and D suggest implementing custom scanning algorithms in AWS Lambda, which would require more development effort and ongoing

maintenance compared to leverage a purpose-built service like Amazon Macie.

So Option B provides an efficient and effective solution while minimizing development effort.

upvoted 1 times

Question #47

Topic 1

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

- A. Purchase Reserved Instances that specify the Region needed.
- B. Create an On-Demand Capacity Reservation that specifies the Region needed.
- C. Purchase Reserved Instances that specify the Region and three Availability Zones needed.
- D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

Correct Answer: D

Community vote distribution

D (100%)

✉  **Incognito013**  1 year, 5 months ago

Reserved instances are for long term so on-demand will be the right choice - Answer D
upvoted 27 times

✉  **simoneric88** 2 months, 1 week ago

Confirmed! Reserved instances require a fixed one-year or three-year commitment. See
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html#capacity-reservations-differences>
upvoted 3 times

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

Selected Answer: D

CORRECT

Option D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

An On-Demand Capacity Reservation is a type of Amazon EC2 reservation that enables you to create and manage reserved capacity on Amazon EC2. With an On-Demand Capacity Reservation, you can specify the Region and Availability Zones where you want to reserve capacity, and the number of EC2 instances you want to reserve. This allows you to guarantee capacity in specific Availability Zones in a specific Region.

WRONG

Option A, purchasing Reserved Instances that specify the Region needed, would not guarantee capacity in specific Availability Zones.

Option B, creating an On-Demand Capacity Reservation that specifies the Region needed, would not guarantee capacity in specific Availability Zones.

Option C, purchasing Reserved Instances that specify the Region and three Availability Zones needed, would not guarantee capacity in specific Availability Zones as Reserved Instances do not provide capacity reservations.

upvoted 22 times

✉  **BlueVolcano1** 1 year, 2 months ago

Another reason as to why Reserved Instances aren't the solution here is that you have to commit to either a 1 year or 3 year term, not 1 week.
upvoted 21 times

✉  **TilTil**  1 week ago

Selected Answer: D

Picked C for this one and failed. Reserved Instances are reserved for 1-3 years so On-Demand Reservation makes more sense.

upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

Selected Answer: D

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>

"On-Demand Capacity Reservations enable you to reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone for any duration"

upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

Just to avoid any confusion, Reserved Instance also guarantee capacity reservation. However, the reason why we don't need Reserved Instances is because they are reserved for a duration of 1 to 3 years with a lock-in contract (no refunds!). The company is only interested in reserved capacity for a week so D is the best solution.

<https://aws.amazon.com/compare/the-difference-between-on-demand-instances-and-reserved-instances/>

upvoted 1 times

✉  **MoshiurGCP** 4 months ago

Guarantee capacity on 3 AZ - on demand reservation, specify region & Availability Zone

upvoted 1 times

 **Ruffyit** 5 months ago

CORRECT

Option D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

An On-Demand Capacity Reservation is a type of Amazon EC2 reservation that enables you to create and manage reserved capacity on Amazon EC2. With an On-Demand Capacity Reservation, you can specify the Region and Availability Zones where you want to reserve capacity, and the number of EC2 instances you want to reserve. This allows you to guarantee capacity in specific Availability Zones in a specific Region.

upvoted 1 times

 **awashenko** 5 months, 3 weeks ago

Selected Answer: D

Reserved Instances have a commitment over a year so those are out. Option B only allows you to specify the Region and not the AZ. Therefore, D is the only solution.

upvoted 1 times

 **Abdou1604** 7 months, 2 weeks ago

its B , On-Demand Capacity Reservation allows you to reserve capacity for Amazon EC2 instances in a specific AWS Region, without specifying specific Availability Zones

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: D

D is the correct option to guarantee EC2 capacity in specific Availability Zones for a set timeframe.

On-Demand Capacity Reservations allow you to reserve EC2 capacity across specific Availability Zones for any duration. This guarantees you will have access to those resources.

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option D is the right answer.

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: D

The most appropriate option to guarantee EC2 capacity in three specific Availability Zones in the desired AWS Region for the 1-week event is to create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones (option D).

A. Purchasing Reserved Instances that specify the Region needed does not guarantee capacity in specific Availability Zones.

B. Creating an On-Demand Capacity Reservation without specifying the Availability Zones would not guarantee capacity in the desired zones.

C. Purchasing Reserved Instances that specify the Region and three Availability Zones is not necessary for a short-term event and involves longer-term commitments.

upvoted 4 times

 **Abrar2022** 10 months, 1 week ago

Reserved instances is for long term

On-demand Capacity reservation enables you to choose specific AZ for any duration

upvoted 1 times

 **Eden** 1 year ago

Just for 1 week so D on demand

upvoted 1 times

 **killbots** 1 year ago

Selected Answer: D

I agree that the answer is D because its only needed for a 1 week event. C would be right if it was a re-occurring event for 1 or more years as reserved instances have to be purchased on long term commitments but would satisfy the capacity requirements.

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

upvoted 1 times

 **Ello2023** 1 year, 1 month ago

D. Reservations are used for long term. A minimum of 1 - 3 years making it cheaper. Whereas, on demand reservation is where you will always get access to CAPACITY it either be 1 week in advance or 1 month in an AZ but you pay On-Demand price meaning there is no discount.

upvoted 1 times

 **BlueVolcano1** 1 year, 2 months ago

Selected Answer: D

Correct answer is On-Demand Capacity Reservation: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>

upvoted 1 times

 **SilentMilli** 1 year, 2 months ago

Selected Answer: D

To guarantee EC2 capacity in specific Availability Zones, the company should create an On-Demand Capacity Reservation. On-Demand Capacity Reservations are a type of EC2 resource that allows the company to reserve capacity for On-Demand instances in a specific Availability Zone or set

of Availability Zones. By creating an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed, the company can guarantee that it will have the EC2 capacity it needs for the upcoming event. The reservation will last for the duration of the event (1 week) and will ensure that the company has the capacity it needs to run its workloads.

upvoted 2 times

Question #48

Topic 1

A company's website uses an Amazon EC2 instance store for its catalog of items. The company wants to make sure that the catalog is highly available and that the catalog is stored in a durable location.

What should a solutions architect do to meet these requirements?

- A. Move the catalog to Amazon ElastiCache for Redis.
- B. Deploy a larger EC2 instance with a larger instance store.
- C. Move the catalog from the instance store to Amazon S3 Glacier Deep Archive.
- D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.

Correct Answer: A

Community vote distribution



✉️ **Six_Fingered_Jose** Highly Voted 1 year, 5 months ago

Selected Answer: D
keyword is "durable" location
A and B is ephemeral storage
C takes forever so is not HA,
that leaves D
upvoted 40 times

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

Yes, if you open EFS home page (<https://aws.amazon.com/efs/>), Amazon state, "Securely and reliably access your files with a fully managed file system designed for 99.99999999 percent (11 9s) durability and up to 99.99 percent (4 9s) of availability."
upvoted 9 times

✉️ **rajendradba** Highly Voted 1 year, 5 months ago

Selected Answer: D
ElastiCache is in Memory, EFS is for durability
upvoted 18 times

✉️ **sirasdf** 1 month ago

That's wrong. EFS is highly available.
upvoted 2 times

✉️ **TilTil** Most Recent 1 week ago

Selected Answer: D
A and B are distractors.
D is durable and HA.
upvoted 1 times

✉️ **modehqudah** 1 month, 3 weeks ago

Selected Answer: D
durable location
upvoted 1 times

✉️ **arslantobe** 2 months ago

Option C, which suggests moving the catalog to Amazon S3 Glacier Deep Archive, is not a suitable choice for an active catalog that requires high availability and quick access. Glacier Deep Archive is designed for long-term archival and may not provide the low-latency access required for a catalog used in a website.

Therefore, option D is the most appropriate choice for achieving both high availability and durability for the catalog.

upvoted 1 times

✉️ **vip2** 2 months, 2 weeks ago

Selected Answer: A
SEE <https://aws.amazon.com/elasticsearch/faqs/#Redis>
upvoted 1 times

✉️ **Hams0** 2 months, 3 weeks ago

Redis can be made durable, supports failover and multi-AZ deployment, it's effective in catalog use cases. EFS is effective when a shared storage is needed
upvoted 2 times

✉️  **rt_7777** 3 months ago

A and D, who win?
upvoted 1 times

✉️  **fb4afde** 3 months, 2 weeks ago

Selected Answer: D

EC for Redis: Durability is a consideration, but the primary use case is caching
EFS: Durability is a core feature for file-based data
upvoted 1 times

✉️  **Ruffyit** 5 months ago

Amazon EFS (Option D) provides the necessary combination of high availability, durability. See question states that high availability with durable location
upvoted 2 times

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

Selected Answer: D

Everyone else pretty much covered it but yes the answer is D.
EFS- Securely and reliably access your files with a fully managed file system designed for 99.99999999 percent (11 9s) durability and up to 99.99 percent (4 9s) of availability
upvoted 3 times

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

Selected Answer: D

EFS is most durable solution
upvoted 1 times

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

Selected Answer: D

The keyword is "durability" and "accessibility". If you open EFS home page (<https://aws.amazon.com/efs/>), Amazon state, "Securely and reliably access your files with a fully managed file system designed for 99.99999999 percent (11 9s) durability and up to 99.99 percent (4 9s) of availability."

upvoted 1 times

✉️  **Hassao0** 6 months, 4 weeks ago

Amazon EFS (Option D) provides the necessary combination of high availability, durability. See question states that high availability with durable location
upvoted 1 times

✉️  **nafeez7950** 7 months, 1 week ago

Selected Answer: A

If i'm not mistaken, Option is A is the right answer because of its Redis technology. Redis can manage its durability using its AOF persistence which allows logging changes of the catalog data and can be replayed, even in the event of failure. As for the availability, Redis also allows replication, so if one fails, another is still working. Considering this question isn't about sharing file systems between instances and rather a customer wants to access a catalog, option A seems to be more suitable option here.

upvoted 4 times

✉️  **pentium75** 3 months ago

Stem doesn't mention configuring Redis replication. Thus "single-node Amazon ElastiCache Redis clusters are in-memory entities with limited data protection services (AOF). If your cluster fails for any reason, you lose all the cluster's data."
upvoted 1 times

✉️  **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: D

D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.

The instance store on an EC2 instance is ephemeral storage that does not provide the durability or availability needed for the catalog.

Amazon EFS provides a scalable, high-performance file system that can be shared between EC2 instances. Data on EFS is stored redundantly across multiple Availability Zones, providing high durability and availability.

EFS is a better solution for the catalog storage than ElastiCache, S3 Glacier, or a larger EC2 instance store. Moving the catalog to EFS would meet the requirements for high availability and durable storage.

upvoted 2 times

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

Selected Answer: D

Highly available and durable = Elastic File System (Amazon EFS)
upvoted 1 times

Question #49

Topic 1

A company stores call transcript files on a monthly basis. Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year. The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-year-old as quickly as possible. A delay in retrieving older files is acceptable.

Which solution will meet these requirements MOST cost-effectively?

- A. Store individual files with tags in Amazon S3 Glacier Instant Retrieval. Query the tags to retrieve the files from S3 Glacier Instant Retrieval.
- B. Store individual files in Amazon S3 Intelligent-Tiering. Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year. Query and retrieve the files that are in Amazon S3 by using Amazon Athena. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.
- C. Store individual files with tags in Amazon S3 Standard storage. Store search metadata for each archive in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.
- D. Store individual files in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year. Store search metadata in Amazon RDS. Query the files from Amazon RDS. Retrieve the files from S3 Glacier Deep Archive.

Correct Answer: C*Community vote distribution*

masetromain 1 year, 5 months ago

Selected Answer: B

I think the answer is B:

Users access the files randomly

S3 Intelligent-Tiering is the ideal storage class for data with unknown, changing, or unpredictable access patterns, independent of object size or retention period. You can use S3 Intelligent-Tiering as the default storage class for virtually any workload, especially data lakes, data analytics, new applications, and user-generated content.

<https://aws.amazon.com/fr/s3/storage-classes/intelligent-tiering/>
upvoted 39 times

sachin 1 year ago

What about if the file you have not accessed 360 days and intelligent tier moved the file to Glacier and on 364 day you want to access the file instantly ?

I think C is right choice

upvoted 3 times

habibi03336 1 year, 1 month ago

It says "S3 Intelligent-Tiering is the ideal storage class for data with unknown, changing, or unpredictable access patterns". However, the statement says access pattern is predictable. It says there is frequent access about 1year.

upvoted 1 times

killbots 1 year ago

it doesnt say predictable, it says files are accessed random. Random = Unpredictable. Answer is B
upvoted 8 times

MutiverseAgent 8 months, 3 weeks ago

Agree, S3 Intelligent-Tiering meets all the requirements. The very important/crucial consideration here to satisfy that all files within a year are instantly accessible is that the two options "Archive Access" and "Deep Archive Access" are not enabled in the "Archive rule actions" section present in the "Intelligent-Tiering Archive configurations" of the bucket. Those options are not enabled by default so this answer will work.

upvoted 2 times

ssoffline 10 months, 1 week ago

Answer is C, why not intelligent Tiering

If the Intelligent-Tiering data transitions to Glacier after 180 days instead of 1 year, it would still be a cost-effective solution that meets the requirements.

With files stored in Amazon S3 Intelligent-Tiering, the data is automatically moved to the appropriate storage class based on its access patterns. In this case, if the data transitions to Glacier after 180 days, it means that files that are infrequently accessed beyond the initial 180 days will be stored in Glacier, which is a lower-cost storage option compared to S3 Standard.

upvoted 6 times

 **RupeC** 8 months, 2 weeks ago

With S3 Intelligent-Tiering, you can define rules that determine when objects should be moved from the frequent access tier to the infrequent access tier, or vice versa, within S3 Standard storage classes.

upvoted 1 times

 **IngenieriaEGlobal** 5 months, 2 weeks ago

The Answer is B. S3 Intelligent-Tiering stores objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the infrequent access tier. There are no retrieval fees in S3 Intelligent-Tiering. If an object in the infrequent access tier is accessed later, it is automatically moved back to the frequent access tier. No additional tiering fees apply when objects are moved between access tiers within the S3 Intelligent-Tiering storage class. S3 Intelligent-Tiering is designed for 99.9% availability and 99.999999999% durability, and offers the same low latency and high throughput performance of S3 Standard

upvoted 4 times

Are you not going to pay for Athena usage?

upvoted 1 times

 **pentium75** 3 months ago

C involves moving "the files to S3 Glacier Instant Retrieval" which is not cost-effective since "a delay in retrieving older files is acceptable."

upvoted 3 times

 **Lilibell**  1 year, 5 months ago

The answer is B

upvoted 12 times

 **LIORAGE**  5 days, 12 hours ago

Selected Answer: B

B is good answer: Athena is good option to query data in S3. And before 1 year data are randomly used, for this, intelligent tiering is good option.

upvoted 1 times

 **chickenmf** 3 weeks ago

Selected Answer: C

The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-year-old as quickly as possible" -- What if S3 Intelligent-Tiering transitioned the data that's under 1 year old into a storage class that takes a long time to access?

upvoted 1 times

 **dsshahu01** 1 month ago

Selected Answer: C

The answer is C

S3 standard for first part (intelligent tiering is much better and cost-effective)
glacier instant retrieval because of the statement after a year needs to be retrieved as soon as possible)

Also why ruling out B is because of Athena - it becomes expensive if data is retrieved using it after scanning all the data in glacier per request.
upvoted 1 times

 **awsgEEK75** 2 months, 1 week ago

Selected Answer: B

A: It does not account for random pattern of first year

C: "Store search metadata for each archive in Amazon S3 Standard storage"... this part is wrong for me. Storing metadata forever in S3 so that it can be queried? This is why I won't select it.

D: RDS is costly for storage and query just to know where your S3 object is.

B is correct as Intelligent Tiering takes care of random frequency in first year in most cost effective way. Older object will end up in S3 glacier with flexible retrieval so cost effective. Athena doesn't care where your object is (S3 standard, IA or Glacier) and queries work.

upvoted 1 times

 **bujuman** 2 months, 3 weeks ago

Selected Answer: B

According to the fact that S3 Std, Std-IA and One Zone-IA are Higher cost, frequent access storage classes and the fact that S3 Intelligent-Tiering is an additional storage class that provides flexibility for data with unknown or changing access patterns. It automates the movement of your objects between storage classes to optimize cost. Plus the requirement for MOST cost-effective solution, Answer B seems to be the right solution

upvoted 1 times

 **JTruong** 2 months, 3 weeks ago

If you watch Stephen Mareek's Udemy SSA video - anything after 1 year has to go with Amazon Athena

upvoted 1 times

 **upliftinghut** 2 months, 4 weeks ago

Selected Answer: C

C is the most cost-effective given no Athena and the archive files don't need instant access. A delay is acceptable

upvoted 1 times

 **upliftinghut** 2 months, 4 weeks ago

quite tricky because B has better cost with flexible retrieval for files after 1 year. If counting in operation overhead then C is better. For cost-optimized, B can probably be better. Tricky question then

upvoted 1 times

 **fb4afde** 3 months, 2 weeks ago

Selected Answer: C

I picked "B" first, then switched to "C" because it asks for MORE cost-effective = Athena might be pricey: however:

Access Patterns:

If your data access patterns are predictable and consistent, and you do not require automatic tiering based on access frequency, S3 Standard might be a straightforward and cost-effective choice.

Variable Access Patterns:

If your data access patterns are variable or unpredictable, and you want automatic cost optimization based on access frequency, S3 Intelligent-Tiering might provide cost savings.

upvoted 1 times

 **wantu** 3 months, 4 weeks ago

Selected Answer: B

los usuarios acceden a los archivos de forma aleatoria. S3 Intelligent-Tiering es la clase de almacenamiento ideal para datos con patrones de acceso desconocidos, cambiantes o impredecibles, independientemente del tamaño del objeto o el período de retención. Puede utilizar S3 Intelligent-Tiering como clase de almacenamiento predeterminada para prácticamente cualquier carga de trabajo, especialmente lagos de datos, análisis de datos, nuevas aplicaciones y contenido generado por el usuario.

upvoted 2 times

 **xogete** 4 months, 1 week ago

Selected Answer: C

i think B would be for least operation overhead, but C only uses S3 which would make it most cost effective, no?

upvoted 1 times

 **wabosi** 4 months, 2 weeks ago

Selected Answer: B

I vote for B, key points to me are:

"randomly within 1 year" my mind goes to intelligent-tiering

"A delay in retrieving older files is acceptable" my mind goes to Glacier Flexible Retrieval after 1 year because they don't need it immediately
"MOST cost-effectively" there are no retrieval charges in S3 intelligent-tiering storage, on top of this Glacier Flexible Retrieval is cheaper than Glacier Instant Retrieval, if they accept retrieval time in 5 – 12 hours, bulk is free

upvoted 2 times

 **SAA463** 4 months, 3 weeks ago

I think the answer is C is cost effective

upvoted 1 times

 **ACloud_Guru15** 5 months, 1 week ago

Selected Answer: C

Considering the cost-effective solution that meets the requirements, option B (Store individual files in Amazon S3 Intelligent-Tiering, use S3 Lifecycle policies to move the files to S3 Glacier after 1 year, query and retrieve the files that are in Amazon S3 by using Amazon Athena, and query and retrieve the files that are in S3 Glacier by using S3 Glacier Select) seems to be the most appropriate. It ensures efficient access to recent and infrequently accessed files, while also managing costs effectively.

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: B

I think the reason C is the correct answer is because it is cheaper than B; and the question is asking the MOST cost effective solution.

upvoted 1 times

 **Wayne23Fang** 5 months, 2 weeks ago

Selected Answer: C

I m on "C" camp. It is hard to beat S3 solution for Cost-effective. C) uses only S3 not other cost like Athena or RDB. The other comment below to support (C) are reasonable like ssoffline's.

upvoted 1 times

Question #50

Topic 1

A company has a production workload that runs on 1,000 Amazon EC2 Linux instances. The workload is powered by third-party software. The company needs to patch the third-party software on all EC2 instances as quickly as possible to remediate a critical security vulnerability. What should a solutions architect do to meet these requirements?

- A. Create an AWS Lambda function to apply the patch to all EC2 instances.
- B. Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances.
- C. Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.
- D. Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.

Correct Answer: D*Community vote distribution*

D (72%)

B (28%)

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

The primary focus of Patch Manager, a capability of AWS Systems Manager, is on installing operating systems security-related updates on managed nodes. By default, Patch Manager doesn't install all available patches, but rather a smaller set of patches focused on security. (Ref <https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-how-it-works-selection.html>)

Run Command allows you to automate common administrative tasks and perform one-time configuration changes at scale. (Ref <https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html>)

Seems like patch manager is meant for OS level patches and not 3rd party applications. And this falls under run command wheelhouse to carry out one-time configuration changes (update of 3rd part application) at scale.

upvoted 55 times

 **Fakhrudin** 6 months, 3 weeks ago

3rd party applications are also supported by Patch Manager (<https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager.html>).

You can use Patch Manager to apply patches for both operating systems and applications. (On Windows Server, application support is limited to updates for applications released by Microsoft.) You can use Patch Manager to install Service Packs on Windows nodes and perform minor version upgrades on Linux nodes. You can patch fleets of Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, on-premises servers, and virtual machines (VMs) by operating system type. This includes supported versions of several operating systems, as listed in Patch Manager prerequisites.

upvoted 5 times

 **Shasha1** Highly Voted 1 year, 3 months ago

D

AWS Systems Manager Run Command allows the company to run commands or scripts on multiple EC2 instances. By using Run Command, the company can quickly and easily apply the patch to all 1,000 EC2 instances to remediate the security vulnerability.

Creating an AWS Lambda function to apply the patch to all EC2 instances would not be a suitable solution, as Lambda functions are not designed to run on EC2 instances. Configuring AWS Systems Manager Patch Manager to apply the patch to all EC2 instances would not be a suitable solution, as Patch Manager is not designed to apply third-party software patches. Scheduling an AWS Systems Manager maintenance window to apply the patch to all EC2 instances would not be a suitable solution, as maintenance windows are not designed to apply patches to third-party software

upvoted 20 times

 **RafikTAAMMA** Most Recent 4 days, 23 hours ago

Selected Answer: D

AWS Systems Manager Patch Manager primarily focuses on operating system patches and does not directly support third-party software patching on Linux instances

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: D

Critical means immediate. Just run the patch command with AWS SM run command to get it done. D is best choice.

A: Too convoluted

B: Can work but have to setup a lot of things to get this done. would be a good choice if D wasn't an option

C: It's a critical patch so not time for maintenance window

upvoted 1 times

 **rt_7777** 3 months ago

By practice, isn't schedule planned downtime is common sense before patching done?

upvoted 1 times

 **youssefrm** 3 months ago

maintenance window will trigger the run command or the patch manager in the right time (as quickly as possible)
upvoted 1 times

 **SaurabhTiwari1** 3 months, 1 week ago

Selected Answer: D

keyword - as quickly as possible
Option B - efficient and reliable
Option D - speed and immediate execution
hence D is correct

upvoted 1 times

 **MoshiurGCP** 4 months ago

Third party software - Custom command.
upvoted 2 times

 **bnagaraja9099** 4 months, 3 weeks ago

D - Patch manager does not understand severity for third party software .
Patch Manager doesn't derive severity levels from third-party sources, such as the Common Vulnerability Scoring System (CVSS), or from metrics released by the National Vulnerability Database (NVD).

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

upvoted 2 times

 **AWSStudyBuddy** 5 months, 1 week ago

Selected Answer: B

I go with option B. To quickly patch third-party software on 1,000 EC2 instances, use AWS Systems Manager Patch Manager. It automates the patching process, from scanning for missing patches to applying the patch to all targeted instances. Patch Manager is designed for managing and automating the patching process for EC2 instances at scale.

upvoted 2 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: D

Key: third-party software and run custom command
upvoted 3 times

 **poponpo** 5 months, 3 weeks ago

Selected Answer: D

Hey dudes. Patch Manager needs the agent. You have to install the agent on all of instances. Can you install the agent over a thousand? Maybe you need SSM Run Command.
<https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-prerequisites.html>

upvoted 4 times

 **gsax** 6 months, 2 weeks ago

Selected Answer: B

Make note of this requirement, "as quickly as possible to remediate a critical security vulnerability." Patch Manager would save time and effort.
upvoted 3 times

 **[Removed]** 6 months, 2 weeks ago

Selected Answer: D

Patching support for applications on Windows Server managed nodes is limited to applications released by Microsoft.
<https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-patching-windows-applications.html>

upvoted 1 times

 **Instantqueue** 5 months, 2 weeks ago

Not true it patches Linux too

upvoted 1 times

 **Abdou1604** 7 months, 2 weeks ago

AWS Systems Manager Patch Manager is designed to apply patches not only to the operating system but also to third-party software running on Amazon EC2 instances, on-premises servers, and virtual machines. It allows you to manage and automate the process of patching both operating systems and applications, including third-party applications so using the patch manager and scheduling a maintenance window, you can ensure controlled and coordinated patching of the EC2 instances. This helps in minimizing disruptions and managing the process effectively so the answer is C :)

upvoted 2 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: D

Patch Manager is designed to patch the underlying OS and select AWS software like Amazon Linux, Windows, etc. It may not work well for patching third-party software.

Run Command allows you to run arbitrary commands or scripts across your fleet of instances. So you can use it to run a command/script that applies the specific patch or update for the third-party software.

Run Command can target the instances very quickly to apply the patch in an urgent scenario.

Since this is a critical vulnerability, the company likely needs more control over how the patch is applied versus relying on Patch Manager's automated patching process.

Run Command allows checking the output/return code to verify if the patch was applied properly on each instance.

upvoted 4 times

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

Selected Answer: B

Technically both 'Patch Manager' and 'Run Command' would work. But the patch manager was build specifically to apply patches for both operating systems and applications.

upvoted 2 times

✉ **johne42** 7 months ago

Some folk think the answer is D... but the Run Command is 'instance' level meaning it is connecting to one.
<https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager.html>

upvoted 1 times

✉ **TheFivePips** 1 month ago

"Using Run Command, a capability of AWS Systems Manager, you can remotely and securely manage the configuration of your managed nodes. A managed node is any Amazon Elastic Compute Cloud (Amazon EC2) instance or non-EC2 machine in your hybrid and multicloud environment that has been configured for Systems Manager. Run Command allows you to automate common administrative tasks and perform one-time configuration changes at scale."

this sure sounds like a one-time configuration change done at scale

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

upvoted 1 times

Question #51

Topic 1

A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Configure the application to send the data to Amazon Kinesis Data Firehose.
- B. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Glue job to query the application's API for the data.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.
- E. Store the application data in Amazon S3. Create an Amazon Simple Notification Service (Amazon SNS) topic as an S3 event destination to send the report by email.

Correct Answer: DE

Community vote distribution



✉️ **whosawsome** Highly Voted 1 year, 5 months ago

Selected Answer: BD

You can use SES to format the report in HTML.

<https://docs.aws.amazon.com/ses/latest/dg/send-email-formatted.html>

upvoted 30 times

✉️ **apchandana** 11 months, 4 weeks ago

this document is talking about the SES API. not ses. SES does not format data. just sending emails.

<https://aws.amazon.com/ses/>

upvoted 4 times

✉️ **Clouddon** 7 months, 2 weeks ago

When you send an email with Amazon SES, the email information you need to provide depends on how you call Amazon SES. You can provide a minimal amount of information and have Amazon SES take care of all of the formatting for you. Or, if you want to do something more advanced like send an attachment, you can provide the raw message yourself. <https://docs.aws.amazon.com/ses/latest/dg/send-email-concepts-email-format.html>

upvoted 2 times

✉️ **backbencher2022** Highly Voted 1 year, 4 months ago

Selected Answer: BD

B&D are the only 2 correct options. If you are choosing option E then you missed the daily morning schedule requirement mentioned in the question which cant be achieved with S3 events for SNS. Event Bridge can used to configure scheduled events (every morning in this case). Option B fulfills the email in HTML format requirement (by SES) and D fulfills every morning schedule event requirement (by EventBridge)

upvoted 24 times

✉️ **RupeC** 8 months, 2 weeks ago

I don't believe you are correct when you say that E cannot meet the scheduling requirement. If the glue action is scheduled and outputs to S3, then as the S3 event destination is SNS, in effect you have a way of getting SNS to have a scheduled release.

upvoted 2 times

✉️ **pentium75** 2 months, 2 weeks ago

But E does not include a glue action. We need either C or D for the scheduling, plus B or E for the email sending.

upvoted 1 times

✉️ **slimen** 4 months, 3 weeks ago

the daily schedule can be achieve with event bridge

- schedule and event bridge to trigger daily
- the event briodige will trigger a lambda function that will collect data and save it in s3
- once data in s3 the event noitification will trigger SNS to send emails

upvoted 1 times

✉️ **Monster07** Most Recent 1 day, 5 hours ago

Selected Answer: BD

Chat GPT says :

With Amazon SES, you can send rich, formatted email content, including text, HTML, attachments, and embedded images, suitable for email

communication.

Amazon SNS is primarily used for sending plain-text or JSON-formatted messages, suitable for notifications and alerts across different channels.

This can suggest that we need to use SES if we want to use HTML content.

upvoted 1 times

 **wyejay** 2 months, 1 week ago

Answer: B and D

Other options

A. Amazon Kinesis Data Firehose: This service is typically used for real-time streaming data processing rather than for scheduled tasks like generating a morning report.

C. Amazon EventBridge to invoke an AWS Glue job: AWS Glue is a data integration service that's more focused on ETL (extract, transform, load) operations, often involving large datasets and complex transformations, which might be more than needed for this scenario.

E. Amazon S3 with SNS topic: Storing data in S3 and using SNS for notification is viable, but this doesn't directly address the need to format the data into HTML and send it as an email report. SNS is better suited for sending notifications rather than formatted reports.

upvoted 5 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: BD

Very detailed question so let's break it down:

"send the report to several email addresses at the same time every morning" this locks B as nothing else can do it.

A: Firehose to collect data from API will work but it cannot generate a report

C: Glue is ETL, it cannot extract data from an API

E: Store data in S3. No idea what this will help with

The API provides order shipping data so you can query it. Lambda can be used to query the API easily so D is good choice that works with B.

BD is correct combination

upvoted 1 times

 **pentium75** 2 months, 2 weeks ago

Selected Answer: BD

"At the same time every morning" requires scheduling, which is only mentioned in C and D. AWS Glue has no native functionality to query REST APIs, thus we need a Lambda function -> D.

For email we need SES or SNS, but as we want "an easy-to-read HTML format", SNS is out. SNS can send notifications, not formatted emails. Thus B.

upvoted 4 times

 **MoshiurGCP** 4 months ago

Key: Send email every morning same time - 1. Simple email 2. AWS Event Bridge with lambda

upvoted 1 times

 **wearrexdzw3123** 4 months, 2 weeks ago

Selected Answer: B

I think there is a problem with the answer. It should be that ses sends the email processed by lambda.

upvoted 1 times

 **tom_cruise** 5 months ago

Selected Answer: BD

Key: retrieval by a REST API, that's why use lambda

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: DE

Both SES and SNS can format html, but there is a disconnection between B and D. Where do you store the data between the steps?

upvoted 4 times

 **pentium75** 3 months ago

Why would I need to "store the data"? Wouldn't the Lambda function just call the SES API?

upvoted 1 times

 **David_Ang** 5 months, 4 weeks ago

Selected Answer: BD

the reason why "B" is more correct than "E" is because is more simple and you don't have to store data is not what they want, also SES is a service that is meant for sending the data through email, and is exactly what the company wants. is not the first time the admin is wrong with the answer

upvoted 2 times

 **hieulam** 6 months, 1 week ago

Selected Answer: DE

E should be correct:

<https://saturncloud.io/blog/how-to-send-html-mails-using-amazon-sns/>

upvoted 1 times

✉  **h_sahu** 6 months ago

I believe BD are the answers. E can't be used, because, in E can't help with email formatting. E won't be the best choice even for scheduling.
upvoted 2 times

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

Selected Answer: BD

Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data. Then use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.

upvoted 2 times

✉  **miki111** 8 months, 1 week ago

Option BD is the correct answer
upvoted 1 times

✉  **miki111** 8 months, 1 week ago

Option BD is the right answer.
upvoted 1 times

✉  **RupeC** 8 months, 2 weeks ago

Selected Answer: CE

Glue - is scheduled to prep the docs using its ETL functionality. Then E. puts the data into S3 and uses sns to send it out by email.

upvoted 2 times

✉  **RupeC** 8 months, 1 week ago

On review, I think DE. D is better than C and glue is ETL but actually, the data needs to be queried, so Lambda is better. The eventbridge is scheduled so S3 and SNS will also by default be run immediately after the eventbridge rule has run.

upvoted 2 times

✉  **Mia2009687** 8 months, 2 weeks ago

Selected Answer: DE

B- Neither Lambda or SEM could hold the data. After the data being handled by Lambda, needs to store it in S3 before publishing to the end users.

upvoted 2 times

✉  **pentium75** 3 months ago

Why? Wouldn't the Lambda function just call the SES API?

upvoted 1 times

Question #52

A company wants to migrate its on-premises application to AWS. The application produces output files that vary in size from tens of gigabytes to hundreds of terabytes. The application data must be stored in a standard file system structure. The company wants a solution that scales automatically, is highly available, and requires minimum operational overhead.

Which solution will meet these requirements?

- A. Migrate the application to run as containers on Amazon Elastic Container Service (Amazon ECS). Use Amazon S3 for storage.
- B. Migrate the application to run as containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon Elastic Block Store (Amazon EBS) for storage.
- C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.
- D. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic Block Store (Amazon EBS) for storage.

Correct Answer: C

Community vote distribution

C (100%)

✉  **ArielSchivo**  1 year, 5 months ago

Selected Answer: C

EFS is a standard file system, it scales automatically and is highly available.
upvoted 28 times

✉  **masetromain**  1 year, 5 months ago

I have absolutely no idea...

Output files that vary in size from tens of gigabytes to hundreds of terabytes

Simit size for a single object:

S3 5To TiB
<https://aws.amazon.com/fr/blogs/aws/amazon-s3-object-size-limit/>

EBS 64 Tib
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/volume_constraints.html

EFS 47.9 TiB
<https://docs.aws.amazon.com/efs/latest/ug/limits.html>

upvoted 9 times

✉  **Help2023** 1 year, 1 month ago

The answer to that is

Limit size for a single object:

S3, 5TiB is per object but you can have more than one object in a bucket, meaning infinity
<https://aws.amazon.com/fr/blogs/aws/amazon-s3-object-size-limit/>

EBS 64 Tib is per block of storage
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/volume_constraints.html
EFS 47.9 TiB per file and in the questions its says Files the 's'
<https://docs.aws.amazon.com/efs/latest/ug/limits.html>

upvoted 2 times

✉  **RBSK** 1 year, 3 months ago

None meets 100s of TB / file. Bit confusing / misleading

upvoted 4 times

✉  **JayBee65** 1 year, 3 months ago

S3 and EBS are block storage but you are looking to store files, so EFS is the correct option.

upvoted 4 times

✉  **Ello2023** 1 year, 2 months ago

S3 is object storage.

upvoted 13 times

✉  **OmegaLambda7XL9** 4 months, 1 week ago

A lil correction,S3 is Object storage not Block Storage

upvoted 3 times

✉  **sidharthwader**  4 weeks ago

C is the only option which supports standard file system when we talk about high availability. EBS scope is within a availability zone but EFS has scope of a region.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: C

Standard file system that is highly available: EFS

Autoscaling highly available system: EC2 or ECS or EKS can work

A: Not suitable due to S3 which is BLOB not file system

B: EKS is ok but EBS is not HA

D: EBS is not HA

So by elimination, C is best option.

upvoted 1 times

 **pentium75** 3 months ago

Selected Answer: C

"File system structure" = EFS, which also meets all the other requirements.

upvoted 2 times

 **Mikado211** 3 months, 3 weeks ago

Selected Answer: C

Technically the A could work, ECS is often recommended by AWS in case of minimum operational overhead, and S3 is durable and highly scalable BUT it is not a "traditional" file system structure. In an S3 bucket, there is no real file structure, only files and prefixes that simulate a structure.

B is wrong because of EKS which require more management

EFS is recommended for minimum operational overhead instead of EBS.

So C (EC2 + EFS) is recommended here over D (EC2 + EBS).

upvoted 3 times

 **wantu** 3 months, 4 weeks ago

Selected Answer: C

Palabras clave: autoescalamiento y archivos

upvoted 1 times

 **leosmal** 4 months ago

The key is Multi-AZ ,EBS does not support it.

upvoted 2 times

 **TariqKipkemei** 7 months, 3 weeks ago

Selected Answer: C

Standard file system structure, scales automatically, requires minimum operational overhead = Amazon Elastic File System (Amazon EFS)

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option C is the correct answer

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

EFS provides a scalable and fully managed file system that can be easily mounted to multiple EC2. It allows you to store and access files using the standard file system structure, which aligns with the company's requirement for a standard file system. EFS automatically scales with the size of your data.

A suggests using ECS for container orchestration and S3 for storage. ECS doesn't offer a native file system storage solution. S3 is an object storage service and may not be the most suitable option for a standard file system structure.

B suggests using EKS for container orchestration and EBS for storage. Similar to A, EBS is block storage and not optimized for file system access. While EKS can manage containers, it doesn't specifically address the file storage requirements.

D suggests using EC2 with EBS for storage. While EBS can provide block storage for EC2, it doesn't inherently offer a scalable file system solution like EFS. You would need to manage and provision EBS volumes manually, which may introduce operational overhead.

upvoted 6 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: C

Option C meets the requirements.

upvoted 1 times

 **joshnort** 11 months ago

Selected Answer: C

Keywords: file system structure, scales automatically, highly available, and minimal operational overhead

upvoted 1 times

 **harirkmusa** 1 year, 1 month ago

standard file system structure is the KEYWORD here, the S3 and EBS are not file based storage. EFS is. so the automatic answer is C
upvoted 1 times

 **NitiATOS** 1 year, 1 month ago

Selected Answer: C

I will go with C as If the app is deployed in MultiAZ, computes are different but the Storage needs to be common.
EFS is easiest way to configure shared storage as compared to SHARED EBS.
Hence C Suits the best.

upvoted 1 times

 **Strk18** 1 year, 2 months ago

Selected Answer: C

C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.
upvoted 2 times

 **SilentMilli** 1 year, 2 months ago

Selected Answer: C

Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.
upvoted 1 times

Question #53

Topic 1

A company needs to store its accounting records in Amazon S3. The records must be immediately accessible for 1 year and then must be archived for an additional 9 years. No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period. The records must be stored with maximum resiliency.

Which solution will meet these requirements?

- A. Store the records in S3 Glacier for the entire 10-year period. Use an access control policy to deny deletion of the records for a period of 10 years.
- B. Store the records by using S3 Intelligent-Tiering. Use an IAM policy to deny deletion of the records. After 10 years, change the IAM policy to allow deletion.
- C. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.
- D. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.

Correct Answer: C

Community vote distribution

C (100%)

 **awsgeek75**  2 months, 1 week ago

Selected Answer: C

Only CD provides Object Lock options which is required for stopping admin/root users from deleting.
D is governance mode which is like government, pay enough money and you can do anything. This is not what we want so compliance is the option.
C is right choice.

For future, remember

S3 Lock Governance = corrupt government official
S3 Lock Compliance = honest solution architect!

upvoted 6 times

 **Guru4Cloud**  7 months, 2 weeks ago

Selected Answer: C

The key reasons are:

The S3 Lifecycle policy transitions the data to Glacier Deep Archive after 1 year for long-term archival.
S3 Object Lock in compliance mode prevents any user from deleting or overwriting objects for the specified retention period.
Glacier Deep Archive provides very high durability and the lowest storage cost for long-term archival.
Compliance mode ensures no one can override or change the retention settings even if policies change.
This meets all the requirements - immediate access for 1 year, archived for 9 years, unable to delete for 10 years, maximum resiliency

upvoted 5 times

 **Ruffyit**  5 months ago

No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period = Compliance Mode

upvoted 4 times

 **axelrodb** 6 months, 2 weeks ago

Selected Answer: C

To meet the requirements of immediately accessible records for 1 year and then archived for an additional 9 years with maximum resiliency, we can use S3 Lifecycle policy to transition records from S3 Standard to S3 Glacier Deep Archive after 1 year. And to ensure that the records cannot be deleted by anyone, including administrative and root users, we can use S3 Object Lock in compliance mode for a period of 10 years. Therefore, the correct answer is option C.

Reference: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.htmls>

upvoted 3 times

 **TariqKipkemei** 7 months, 2 weeks ago

Selected Answer: C

No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period = Compliance Mode

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option C is the correct answer

upvoted 2 times

 **MutiverseAgent** 8 months, 3 weeks ago

Why not A? Move all files to S3 Glacier instant retrieval (Cheaper than S3) and then move files older than a year to S3 Deep archive.

upvoted 1 times

 **dhax12** 5 months, 2 weeks ago

Put entire 10 years to Glacier means it's not accessible for the 1 year window. Hence wrong answer.

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

To prevent deletion of records during the entire 10-year period, you can utilize S3 Object Lock feature. By enabling it in compliance mode, you can set a retention period on the objects, preventing any user, including administrative and root users, from deleting records.

A: S3 Glacier is suitable for long-term archival, it may not provide immediate accessibility for the first year as required.

B: Intelligent-Tiering may not offer the most cost-effective archival storage option for extended 9-year period. Changing the IAM policy after 10 years to allow deletion also introduces manual steps and potential human error.

D: While S3 One Zone-IA can provide cost savings, it doesn't offer the same level of resiliency as S3 Glacier Deep Archive for long-term archival.

upvoted 3 times

 **11pantheman11** 11 months ago

Selected Answer: C

In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

upvoted 3 times

 **athiha** 1 year ago

Selected Answer: C

Retention Period: A period is specified by Days & Years.

With Retention Compliance Mode, you can't change/adjust (even by the account root user) the retention mode during the retention period while all objects within the bucket are Locked.

With Retention Governance mode, a less restrictive mode, you can grant special permission to a group of users to adjust the Lock settings by using S3:BypassGovernanceRetention.

Legal Hold: It's On/Off setting on an object version. There is no retention period. If you enable Legal Hold on specific object version, you will not be able to delete or override that specific object version. It needs S:PutObjectLegalHold as a permission.

upvoted 3 times

 **Wheretostart** 1 year ago

Selected Answer: C

S3 Glacier Deep Archive all day....

upvoted 1 times

 **SilentMilli** 1 year, 2 months ago

Selected Answer: C

Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.

upvoted 1 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: C

Use S3 Object Lock in compliance mode

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

upvoted 3 times

 **pazabal** 1 year, 3 months ago

Selected Answer: C

C, A lifecycle set to transition from standard to Glacier deep archive and use lock for the delete requirement

A, B and D don't meet the requirements

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: C

C. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.

To meet the requirements, the company could use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. S3 Glacier Deep Archive is Amazon's lowest-cost storage class, specifically designed for long-term retention of data that is accessed rarely. This would allow the company to store the records with maximum resiliency and at the lowest possible cost.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

To ensure that the records are not deleted during the entire 10-year period, the company could use S3 Object Lock in compliance mode. S3 Object Lock allows the company to apply a retention period to objects in S3, preventing the objects from being deleted until the retention period expires. By using S3 Object Lock in compliance mode, the company can ensure that the records are not deleted by anyone, including administrative users and root users, during the entire 10-year period.

upvoted 1 times

 **Nandan747** 1 year, 3 months ago

Selected Answer: C

A and B are ruled out as you need them to be accessible for 1 year and using control policy or IAM policies, the administrator or root still has the ability to delete them.

D is ruled out as it uses One Zone-IA, but requirement says max- resiliency.

SO- C should be the right answer.

upvoted 4 times

 **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

Question #54

Topic 1

A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a highly available and durable storage solution that preserves how users currently access the files.

What should a solutions architect do to meet these requirements?

- A. Migrate all the data to Amazon S3. Set up IAM authentication for users to access files.
- B. Set up an Amazon S3 File Gateway. Mount the S3 File Gateway on the existing EC2 instances.
- C. Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.
- D. Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.

Correct Answer: C

Community vote distribution

C (98%)

✉️ **k1kavi1** Highly Voted 1 year, 3 months ago

Selected Answer: C

EFS is not supported on Windows instances

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEFS.html>

Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system.

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>

upvoted 14 times

✉️ **Buruguduystunstugudunstuy** Highly Voted 1 year, 4 months ago

Selected Answer: C

Windows file shares = Amazon FSx for Windows File Server

Hence, the correct answer is C

upvoted 7 times

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

Taking back this answer. As explained in the latest update.

CORRECT

D: Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.

upvoted 1 times

✉️ **pentium75** 3 months ago

No, users should continue using SMB, which EFS doesn't support

upvoted 1 times

✉️ **SMALLE** Most Recent 1 month, 2 weeks ago

Selected Answer: C

FSx=Windows

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>

upvoted 2 times

✉️ **awsgeek75** 2 months, 1 week ago

Selected Answer: C

Windows workload rules out S3 and EFS as they cannot be mounted directly on Windows. S3 File Gateway is mainly for on-prem to AWS which is not a requirement here as company is already in AWS.

C meets all the requirements.

upvoted 2 times

✉️ **jitlathi** 2 months, 4 weeks ago

Selected Answer: C

With Amazon FSx for Windows File Server, you can enjoy a native Windows file server experience with a fully managed, scalable, and highly dependable file storage solution

upvoted 2 times

✉️ **Ruffyit** 5 months ago

<https://aws.amazon.com/fsx/windows/faqs/>

Thousands of compute instances and devices can access a file system concurrently.

upvoted 1 times

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

Selected Answer: C

With Amazon FSx for Windows File Server, you can enjoy a native Windows file server experience with a fully managed, scalable, and highly dependable file storage solution. Rich administrative features including end-user file recovery, user quotas, and Microsoft Active Directory integration are all provided by this Windows Server-based system.

upvoted 1 times

✉ **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

The key reasons are:

FSx for Windows provides fully managed Windows-native SMB file shares that are accessible from Windows clients.

It allows seamlessly migrating the existing Windows file shares to FSx shares without disrupting users.

The Multi-AZ configuration provides high availability and durability for file storage.

Users can continue to access files the same way over SMB without any changes.

It is optimized for Windows workloads and provides features like user quotas, ACLs, AD integration.

Data is stored on SSDs with automatic backups for resilience.

upvoted 1 times

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

Selected Answer: C

The company wants a highly available and durable storage solution that preserves how users currently access the files = Amazon FSx for Windows File Server

upvoted 1 times

✉ **miki111** 8 months, 1 week ago

Option C is the correct answer

upvoted 1 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: C

Migrating all the data to FSx for Windows File Server allows you to preserve existing user access method and maintain compatibility with Windows file shares. Users can continue accessing files using the same method as before, without any disruptions.

A: S3 is a highly durable object storage service, it is not designed to directly host Windows file shares. Implementing IAM authentication for file access would require significant changes to existing user access method.

B: S3 File Gateway can provide access to Amazon S3 objects through standard file protocols, it may not be ideal solution for preserving existing user access method and maintaining Windows file shares.

D: Although Amazon EFS provides highly available and durable file storage, it may not directly support the existing Windows file shares and their access method.

upvoted 4 times

✉ **11pantheman11** 11 months ago

Selected Answer: C

<https://aws.amazon.com/fsx/windows/faqs/>

Thousands of compute instances and devices can access a file system concurrently.

EFS does not support Windows

upvoted 2 times

✉ **cheese929** 11 months, 1 week ago

Selected Answer: C

C is correct. Amazon FSx for Windows File Server.

upvoted 3 times

✉ **satosi** 11 months, 1 week ago

Selected Answer: C

EFS is not supported on Windows instances

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEFS.html>

Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system.

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>

upvoted 3 times

✉ **cheese929** 11 months, 2 weeks ago

Selected Answer: C

C is correct. Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers.

upvoted 2 times

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

Selected Answer: C

Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.
upvoted 2 times

 **dan80** 1 year, 2 months ago

Selected Answer: C

<https://aws.amazon.com/blogs/aws/amazon-fsx-for-windows-file-server-update-new-enterprise-ready-features/>
upvoted 3 times

Question #55

Topic 1

A solutions architect is developing a VPC architecture that includes multiple subnets. The architecture will host applications that use Amazon EC2 instances and Amazon RDS instances. The architecture consists of six subnets in two Availability Zones. Each Availability Zone includes a public subnet, a private subnet, and a dedicated subnet for databases. Only EC2 instances that run in the private subnets can have access to the RDS databases.

Which solution will meet these requirements?

- A. Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table with the database subnets.
- B. Create a security group that denies inbound traffic from the security group that is assigned to instances in the public subnets. Attach the security group to the DB instances.
- C. Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.
- D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

Correct Answer: C

Community vote distribution

C (100%)

✉️  **Sinaneos**  1 year, 5 months ago

Selected Answer: C

- A: doesn't fully configure the traffic flow
 B: security groups don't have deny rules
 D: peering is mostly between VPCs, doesn't really help here

answer is C, most mainstream way

upvoted 46 times

✉️  **Gary_Phillips_2007**  1 year ago

Just took the exam today and EVERY ONE of the questions came from this dump. Memorize it all. Good luck.

upvoted 26 times

✉️  **orhan64** 8 months ago

Hey bro, did you buy premium access?

upvoted 5 times

✉️  **awsgeek75**  2 months, 1 week ago

Selected Answer: C

- A: route table that connect... no idea what this option is trying to do but won't work for RDS
 B: SG are deny by default
 D: Peering connection between subnets? No idea what this is but happy to learn if such a thing exists.

C: SG to allow input to private subnet means everything else will be blocked. Attaching this SG to DB instance means it will block everything except the private subnet instances which is where the required EC2 instances are.

upvoted 2 times

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

Selected Answer: C

RDS databases can only be accessed by EC2 instances located in private subnets: From the security group given to instances in the private subnets, the DB instances' security group will permit incoming traffic. Because of this, the RDS databases will only be accessible by EC2 instances located on the private subnets.

Because of its safe architecture, Every other source of incoming traffic will be blocked by the security group that is linked to the database instances. The RDS databases will be better shielded from unwanted access thanks to this.

upvoted 1 times

✉️  **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

The key reasons are:

Using security groups to control access between resources is a standard practice in VPCs.

The security group attached to the RDS DB instances can allow inbound traffic from the security group for the EC2 instances in the private subnets. This allows only those EC2 instances in the private subnets to connect to the databases, meeting the requirements.

Route tables, peering connections, and denying public subnet access would not achieve the needed selectivity of allowing only the private subnet

EC2 instances.

Security groups provide stateful filtering at the instance level for precise access control.

upvoted 2 times

 **TariqKipkemei** 7 months, 2 weeks ago

Selected Answer: C

Security groups only have allow rules

upvoted 1 times

 **praveenvky83** 7 months, 3 weeks ago

Selected Answer: C

option C

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option C is the correct answer

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

Creating security group that allows inbound traffic from security group assigned to instances in private subnets ensures that only EC2 running in private subnets can access the RDS databases. By associating security group with DB, you restrict access to only instances that belong to designated security group.

A: This approach may help control routing within VPC, it does not address the specific access requirement between EC2 instances and RDS databases.

B: Using a deny rule in a security group can lead to complexities and potential misconfigurations. It is generally recommended to use allow rules to explicitly define access permissions.

D: Peering connections enable communication between different VPCs or VPCs in different regions, and they are not necessary for restricting access between subnets within the same VPC.

upvoted 3 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: C

Option C meets the requirements.

upvoted 1 times

 **Abrar2022** 10 months, 1 week ago

By default, a security group is set up with rules that deny all inbound traffic and permit all outbound traffic.

upvoted 1 times

 **water314** 10 months, 4 weeks ago

Selected Answer: C

CCCCCCCCCC

upvoted 1 times

 **SilentMilli** 1 year, 2 months ago

Selected Answer: C

Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances. This will allow the EC2 instances in the private subnets to have access to the RDS databases while denying access to the EC2 instances in the public subnets.

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: C

The solution that meets the requirements described in the question is option C: Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.

In this solution, the security group applied to the DB instances allows inbound traffic from the security group assigned to instances in the private subnets. This ensures that only EC2 instances running in the private subnets can have access to the RDS databases.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option A, creating a new route table that excludes the route to the public subnets' CIDR blocks and associating it with the database subnets, would not meet the requirements because it would block all traffic to the database subnets, not just traffic from the public subnets.

Option B, creating a security group that denies inbound traffic from the security group assigned to instances in the public subnets and attaching it to the DB instances, would not meet the requirements because it would allow all traffic from the private subnets to reach the DB instances, not just traffic from the security group assigned to instances in the private subnets.

Option D, creating a new peering connection between the public subnets and the private subnets and a different peering connection between the private subnets and the database subnets, would not meet the requirements because it would allow all traffic from the private subnets to reach the DB instances, not just traffic from the security group assigned to instances in the private subnets.

upvoted 1 times

 **Nandan747** 1 year, 3 months ago

Selected Answer: C

The real trick is between B and C. A and D are ruled out for obvious reasons.
B is wrong as you cannot have deny type rules in Security groups.
So- C is the right answer.

upvoted 4 times

 **ashish_t** 1 year, 4 months ago

Selected Answer: C

The key is "Only EC2 instances that run in the private subnets can have access to the RDS databases"
The answer is C.

upvoted 2 times

 **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

Question #56

Topic 1

A company has registered its domain name with Amazon Route 53. The company uses Amazon API Gateway in the ca-central-1 Region as a public interface for its backend microservice APIs. Third-party services consume the APIs securely. The company wants to design its API Gateway URL with the company's domain name and corresponding certificate so that the third-party services can use HTTPS.

Which solution will meet these requirements?

- A. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default URL. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).
- B. Create Route 53 DNS records with the company's domain name. Point the alias record to the Regional API Gateway stage endpoint. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.
- C. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint. Configure Route 53 to route traffic to the API Gateway endpoint.
- D. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region. Attach the certificate to the API Gateway APIs. Create Route 53 DNS records with the company's domain name. Point an A record to the company's domain name.

Correct Answer: D

Community vote distribution

C (94%) 6%

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

Selected Answer: C

The correct solution to meet these requirements is option C.

To design the API Gateway URL with the company's domain name and corresponding certificate, the company needs to do the following:

1. Create a Regional API Gateway endpoint: This will allow the company to create an endpoint that is specific to a region.
2. Associate the API Gateway endpoint with the company's domain name: This will allow the company to use its own domain name for the API Gateway URL.
3. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region: This will allow the company to use HTTPS for secure communication with its APIs.
4. Attach the certificate to the API Gateway endpoint: This will allow the company to use the certificate for securing the API Gateway URL.
5. Configure Route 53 to route traffic to the API Gateway endpoint: This will allow the company to use Route 53 to route traffic to the API Gateway URL using the company's domain name.

upvoted 45 times

 **t0nx** 4 months ago

Why the "reveal solution" most of the time gives the wrong answer ?

upvoted 10 times

 **wharfargo** 1 month, 3 weeks ago

i read this before that they can't give 100% of the right answers legally or something

upvoted 6 times

 **aadityaravi8** 9 months ago

google bard reply..

upvoted 4 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option C includes all the necessary steps to meet the requirements, hence it is the correct solution.

Options A and D do not include the necessary steps to associate the API Gateway endpoint with the company's domain name and attach the certificate to the endpoint.

Option B includes the necessary steps to associate the API Gateway endpoint with the company's domain name and attach the certificate, but it imports the certificate into the us-east-1 Region instead of the ca-central-1 Region where the API Gateway is located.

upvoted 9 times

 **masetromain** Highly Voted  1 year, 5 months ago

Selected Answer: C

I think the answer is C. we don't need to attach a certificate in us-east-1, if is not for cloudfront. In our case the target is ca-central-1.
upvoted 30 times

Valero_ 1 year, 5 months ago

I think that is C too, the target would be the same Region.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-regional-api-custom-domain-create.html>
upvoted 8 times

MutiverseAgent 8 months, 3 weeks ago

Agree, C is correct by using the API Gateway option "Custom domain names"

<https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-custom-domains.html>
upvoted 1 times

awsgeek75 **Most Recent** 2 months, 1 week ago

Selected Answer: C

BD are wrong because they are in wrong regions.

A. Does not help with R53 routing to API Gateway and not sure what it's trying to do here
C is correct
upvoted 1 times

bujuman 2 months, 3 weeks ago

Selected Answer: C

Important

For an API Gateway Regional custom domain name, you must request or import the certificate in the same Region as your API.
upvoted 3 times

debasishdtta 3 months ago

Selected Answer: D

All certificates in ACM are regional resources, including the certificates that you import. To use the same certificate with Elastic Load Balancing load balancers in different AWS Regions, you must import the certificate into each Region where you want to use it. To use a certificate with Amazon CloudFront, you must import it into the US East (N. Virginia) Region.

<https://docs.aws.amazon.com/acm/latest/userguide/import-certificate.html>
upvoted 2 times

EtherealBagel 3 months, 2 weeks ago

Only if the API Gateway is global then the corresponding AWS ACM Certificate must be placed in us-east-1
upvoted 1 times

luongtrann 5 months, 1 week ago

Selected Answer: C

Correct answer

upvoted 1 times

Abitek007 5 months, 3 weeks ago

Selected Answer: D

A records support Elasticity and load balancing and by default resilience is Key in any configuration in AWS
upvoted 2 times

Abitek007 5 months, 3 weeks ago

now I am confused, I would have chosen C, but with a Closer look D might be right, because of the A records and again the region used and not stated can be for resilience. I think? can someone clarify

upvoted 2 times

OctavioBatera 6 days, 12 hours ago

I think C is the correct answer, because the DNS record in this case must be an alias (cname). DNS A record is for IP address. Here some documentation that can be useful:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-api-gateway.html>
upvoted 1 times

paniya93 5 months, 3 weeks ago

Selected Answer: C

Explain why this saying a different region which not mentioned in the Q.

upvoted 1 times

Hassao0 6 months, 4 weeks ago

c is right

The other options have various issues:

Option A: Using stage variables and importing certificates into ACM is not sufficient for achieving the requirement of associating a custom domain and certificate with the API Gateway endpoint.

Option B: While it mentions importing the certificate into ACM, it doesn't address the need for a Regional API Gateway or the appropriate region for the certificate.

Option D: Using certificates from the us-east-1 region for a Regional API Gateway might cause issues. Additionally, it doesn't provide clear details on how to associate the domain name and certificate with the API Gateway endpoint.

upvoted 2 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

C is the correct solution.

To use a custom domain name with HTTPS for API Gateway:

The API Gateway endpoint needs to be Regional, not private or edge-optimized.

The ACM certificate must be requested in the same region as the API Gateway endpoint.

The custom domain name is then mapped to the Regional API endpoint under API Gateway domain names.

Route 53 is configured to route traffic to the API Gateway regional domain.

The ACM certificate is attached to the API Gateway domain name to enable HTTP

upvoted 1 times

 **TariqKipkemei** 7 months, 2 weeks ago

Selected Answer: C

Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region.

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option C is the correct answer

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

Option C encompasses all the necessary steps to design the API Gateway URL with the company's domain name and enable secure HTTPS access using the appropriate certificate.

A. This approach does not involve using the company's domain name or a custom certificate. It does not provide a solution for enabling HTTPS access with a corresponding certificate.

B. It suggests importing the certificate into ACM in the us-east-1 Region, which may not align with the desired ca-central-1 Region for this scenario. It's important to use ACM in the same Region where API Gateway is deployed to simplify certificate management.

D. It suggests importing the certificate into ACM in the us-east-1 Region, which again does not align with the desired ca-central-1 Region.

Additionally, it mentions attaching the certificate to API Gateway, which is not necessary for achieving the desired outcome of enabling HTTPS access for the API Gateway endpoint.

upvoted 3 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: C

I switch to option C too, which meets the requirements.

upvoted 1 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: D

I vote for option D.

upvoted 1 times

Question #57

Topic 1

A company is running a popular social media website. The website gives users the ability to upload images to share with other users. The company wants to make sure that the images do not contain inappropriate content. The company needs a solution that minimizes development effort.

What should a solutions architect do to meet these requirements?

- A. Use Amazon Comprehend to detect inappropriate content. Use human review for low-confidence predictions.
- B. Use Amazon Rekognition to detect inappropriate content. Use human review for low-confidence predictions.
- C. Use Amazon SageMaker to detect inappropriate content. Use ground truth to label low-confidence predictions.
- D. Use AWS Fargate to deploy a custom machine learning model to detect inappropriate content. Use ground truth to label low-confidence predictions.

Correct Answer: B

Community vote distribution

B (100%)

 **Buruguduystunstugudunstuy**  1 year, 3 months ago

Selected Answer: B

The best solution to meet these requirements would be option B: Use Amazon Rekognition to detect inappropriate content, and use human review for low-confidence predictions.

Amazon Rekognition is a cloud-based image and video analysis service that can detect inappropriate content in images using its pre-trained label detection model. It can identify a wide range of inappropriate content, including explicit or suggestive adult content, violent content, and offensive language. The service provides high accuracy and low latency, making it a good choice for this use case.

upvoted 16 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option A, using Amazon Comprehend, is not a good fit for this use case because Amazon Comprehend is a natural language processing service that is designed to analyze text, not images.

Option C, using Amazon SageMaker to detect inappropriate content, would require significant development effort to build and train a custom machine learning model. It would also require a large dataset of labeled images to train the model, which may be time-consuming and expensive to obtain.

Option D, using AWS Fargate to deploy a custom machine learning model, would also require significant development effort and a large dataset of labeled images. It may not be the most efficient or cost-effective solution for this use case.

In summary, the best solution is to use Amazon Rekognition to detect inappropriate content in images, and use human review for low-confidence predictions to ensure that all inappropriate content is detected.

upvoted 11 times

 **masetromain**  1 year, 5 months ago

Selected Answer: B

Good Answer is B :

<https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html?pg=ln&sec=ft>

upvoted 13 times

 **awsgeek75**  2 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/rekognition/>

Automate and lower the cost of your image recognition and video analysis with machine learning

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

<https://aws.amazon.com/rekognition/content-moderation/>

Amazon Rekognition Content Moderation automates and streamlines your image and video moderation workflows using machine learning (ML), without requiring ML experience.

upvoted 1 times

 **slimen** 4 months, 3 weeks ago

Selected Answer: B

comprehend is for NLP

sagemaker is for training and deploying ML and AI models

deploying custom models using fargate requires time and development effort which is not recommended by the question

upvoted 2 times

 **Ruffyit** 5 months ago

<https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html?pg=ln&sec=ft>
upvoted 1 times

 **AWSStudyBuddy** 5 months, 1 week ago

Selected Answer: B

You can easily incorporate image and video analysis to your applications with the help of Amazon Rekognition. Numerous functions are available to it, including as facial analysis, image classification, and object and scene identification.

DetectModerationLabels is an operation that may be used with Amazon Rekognition to identify incorrect content in photos. By using this procedure, photos with violent, drug-related, tobacco-related, alcohol-related, hate-filled, or provocative material can be identified.

upvoted 2 times

 **Syruis** 7 months, 1 week ago

Selected Answer: B

B is the best solution as far
upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: B

Amazon Rekognition is a fully managed service that provides image and video analysis capabilities. It can be used to detect inappropriate content in images, such as nudity, violence, and hate speech.

Amazon Rekognition is a good choice for this solution because it is a managed service, which means that the company does not have to worry about managing the infrastructure or the machine learning model. Rekognition is also highly accurate, and it can be used to detect a wide range of inappropriate content

upvoted 1 times

 **TariqKipkemei** 7 months, 2 weeks ago

Selected Answer: B

Amazon Rekognition to the rescue...whooosh!
upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Using Amazon Rekognition for content moderation is a cost-effective and efficient solution that reduces the need for developing and training custom machine learning models, making it the best option in terms of minimizing development effort.

A. Amazon Comprehend is a natural language processing service provided by AWS, primarily focused on text analysis rather than image analysis.

C. Amazon SageMaker is a comprehensive machine learning service that allows you to build, train, and deploy custom machine learning models. It requires significant development effort to build and train a custom model. In addition, utilizing ground truth to label low-confidence predictions would further add to the development complexity and maintenance overhead.

D. Similar to C, using AWS Fargate to deploy a custom machine learning model requires significant development effort.

upvoted 2 times

 **krajar** 1 year ago

Selected Answer: B

Amazon Rekognition is a cloud-based image and video analysis service that can detect inappropriate content in images using its pre-trained label detection model. It can identify a wide range of inappropriate content, including explicit or suggestive adult content, violent content, and offensive language.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B
upvoted 1 times

 **Shasha1** 1 year, 3 months ago

B

AWS Rekognition to detect inappropriate content and use human review for low-confidence predictions. This option minimizes development effort because Amazon Rekognition is a pre-built machine learning service that can detect inappropriate content. Using human review for low-confidence predictions allows for more accurate detection of inappropriate content.

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **ArielSchivo** 1 year, 5 months ago

Selected Answer: B

Option B.

<https://docs.aws.amazon.com/rekognition/latest/dg/a2i-rekognition.html>

upvoted 1 times

Question #58

Topic 1

A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.

What should a solutions architect do to meet these requirements?

- A. Use Amazon EC2 instances, and install Docker on the instances.
- B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes.
- C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
- D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

Correct Answer: C

Community vote distribution

C (100%)

✉  **masetromain**  1 year, 5 months ago

Selected Answer: C

Good answer is C:

AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without having to manage servers. AWS Fargate is compatible with Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).

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

upvoted 24 times

✉  **cookieMr**  9 months, 1 week ago

Selected Answer: C

Using ECS on Fargate allows you to run containers without the need to manage the underlying infrastructure. Fargate abstracts away the underlying EC2 and provides serverless compute for containers.

A. This option would require manual provisioning and management of EC2, as well as installing and configuring Docker on those instances. It would introduce additional overhead and responsibilities for maintaining the underlying infrastructure.

B. While this option leverages ECS to manage containers, it still requires provisioning and managing EC2 to serve as worker nodes. It adds complexity and maintenance overhead compared to the serverless nature of Fargate.

D. This option still involves managing and provisioning EC2, even though an ECS-optimized AMI simplifies the process of setting up EC2 for running ECS. It does not provide the level of serverless abstraction and ease of management offered by Fargate.

upvoted 7 times

✉  **awsgEEK75**  2 months, 1 week ago

Selected Answer: C

Managed containers = Fargate

upvoted 2 times

✉  **Ruffyt** 5 months ago

AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without having to manage servers. AWS Fargate is compatible with Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).

upvoted 1 times

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

Selected Answer: C

In order to execute containerized apps without having to manage servers, AWS Fargate is a serverless compute engine for Amazon ECS. Amazon Elastic Compute Cloud (Amazon EC2) instance clusters no longer require provisioning, configuring, or scaling thanks to AWS Fargate. So that you can concentrate on developing and maintaining your applications, AWS Fargate handles the monotonous, repetitive labor of managing servers.

upvoted 1 times

✉  **Teruteru** 6 months, 2 weeks ago

Option C is the correct answer.

upvoted 1 times

✉  **Syrus** 7 months, 1 week ago

Selected Answer: C

C for Fargate

upvoted 1 times

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

Selected Answer: C

The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload = Serverless compute for containers = AWS Fargate

upvoted 1 times

✉️  **miki111** 8 months, 1 week ago

Option C is the correct answer
upvoted 1 times

✉️  **cheese929** 11 months, 2 weeks ago

Selected Answer: C

AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances.

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html>

upvoted 1 times

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

Selected Answer: C

ECS + Fargate
upvoted 3 times

✉️  **gustavtd** 1 year, 2 months ago

Selected Answer: C

AWS Fargate will hide all the complexity for you
upvoted 1 times

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

Selected Answer: C

C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.

AWS Fargate is a fully managed container execution environment that runs containers without the need to provision and manage underlying infrastructure. This makes it a good choice for companies that want to focus on maintaining their critical applications and do not want to be responsible for provisioning and managing the underlying infrastructure.

Option A involves installing Docker on Amazon EC2 instances, which would still require the company to manage the underlying infrastructure. Option B involves using Amazon ECS on Amazon EC2 worker nodes, which would also require the company to manage the underlying infrastructure. Option D involves using Amazon EC2 instances from an Amazon ECS-optimized Amazon Machine Image (AMI), which would also require the company to manage the underlying infrastructure.

upvoted 2 times

✉️  **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C
upvoted 1 times

✉️  **benaws** 1 year, 3 months ago

Selected Answer: C

Obviously anything with EC2 in the answer is wrong...
upvoted 1 times

✉️  **ashish_t** 1 year, 4 months ago

Selected Answer: C

The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload. Fargate is serverless and no need to manage.

Answer: C

upvoted 2 times

✉️  **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

Question #59

Topic 1

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

- A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
- B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
- C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
- D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Correct Answer: D

Community vote distribution



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

Selected Answer: D

Option D is the most appropriate solution for transmitting and processing the clickstream data in this scenario.

Amazon Kinesis Data Streams is a highly scalable and durable service that enables real-time processing of streaming data at a high volume and high rate. You can use Kinesis Data Streams to collect and process the clickstream data in real-time.

Amazon Kinesis Data Firehose is a fully managed service that loads streaming data into data stores and analytics tools. You can use Kinesis Data Firehose to transmit the data from Kinesis Data Streams to an Amazon S3 data lake.

Once the data is in the data lake, you can use Amazon Redshift to load the data and perform analysis on it. Amazon Redshift is a fully managed, petabyte-scale data warehouse service that allows you to quickly and efficiently analyze data using SQL and your existing business intelligence tools.

upvoted 26 times

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

Option A, which involves using AWS Data Pipeline to archive the data to an Amazon S3 bucket and running an Amazon EMR cluster with the data to generate analytics, is not the most appropriate solution because it does not involve real-time processing of the data.

Option B, which involves creating an Auto Scaling group of Amazon EC2 instances to process the data and sending it to an Amazon S3 data lake for Amazon Redshift to use for analysis, is not the most appropriate solution because it does not involve a fully managed service for transmitting the data from the processing layer to the data lake.

Option C, which involves caching the data to Amazon CloudFront, storing the data in an Amazon S3 bucket, and running an AWS Lambda function to process the data for analysis when an object is added to the S3 bucket, is not the most appropriate solution because it does not involve a scalable and durable service for collecting and processing the data in real-time.

upvoted 6 times

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

The question does not say that real-time is needed here

upvoted 3 times

✉️ **pentium75** 3 months ago

Question asks how to "transmit and process the clickstream data", NOT how to analyze it. Thus D.

upvoted 1 times

✉️ **ArielSchivo** Highly Voted 1 year, 5 months ago

Selected Answer: D

Option D.

<https://aws.amazon.com/es/blogs/big-data/real-time-analytics-with-amazon-redshift-streaming-ingestion/>

upvoted 16 times

✉️ **RBSK** 1 year, 3 months ago

Unsure if this is right URL for this scenario. Option D is referring to S3 and then Redshift. Whereas URL discuss about eliminating S3 :- We're excited to launch Amazon Redshift streaming ingestion for Amazon Kinesis Data Streams, which enables you to ingest data directly from the Kinesis data stream without having to stage the data in Amazon Simple Storage Service (Amazon S3). Streaming ingestion allows you to achieve low latency in the order of seconds while ingesting hundreds of megabytes of data into your Amazon Redshift cluster.

upvoted 3 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: D

A: Not sure how recent this question is but Data Pipeline is not really a product AWS is recommending anymore
<https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html>

B: 30TB of clickstream data could be done with EC2 but it would be challenging
C: CloudFront is for CDN and caching and mostly outgoing data, not incoming.

D: Kinesis, S3 data lake and Redshift will work perfectly for this case

upvoted 2 times

 **clumsyninja4life** 3 months ago

Selected Answer: A

The answer should be A. Clickstream does not mean real time, it just means they capture user interactions on the web page. Kinesis data streaming is not required. Furthermore, redshift is a data warehousing solution, it can't run complex analysis as well as EMR. My vote goes for A

upvoted 1 times

 **pentium75** 3 months ago

Question asks how to "transmit and process the clickstream data", NOT how to analyze it. Also question does NOT ask how to archive the data (as is mentioned in A). Thus D.

upvoted 1 times

 **Reckless_Jas** 7 months, 1 week ago

when you see clickstream data, think about Kinesis Data Stream

upvoted 6 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: D

The key reasons are:

Kinesis Data Streams can continuously capture and ingest high volumes of clickstream data in real-time. This handles the large 30TB daily data intake.

Kinesis Firehose can automatically load the streaming data into S3. This creates a data lake for further analysis.

Firehose can transform and analyze the data in flight before loading to S3 using Lambda. This enables real-time processing.

The data in S3 can be easily loaded into Amazon Redshift for interactive analysis at scale.

Kinesis auto scales to handle the high data volumes. Minimal effort is needed for infrastructure management.

upvoted 2 times

 **miki111** 8 months, 1 week ago

Option D is the correct answer

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: D

A. This option utilizes S3 for data storage and EMR for analytics, Data Pipeline is not ideal service for real-time streaming data ingestion and processing. It is better suited for batch processing scenarios.

B. This option involves managing and scaling EC2, which adds operational overhead. It is also not real-time streaming solution. Additionally, use of Redshift for analyzing clickstream data might not be most efficient or cost-effective approach.

C. CloudFront is CDN service and is not designed for real-time data processing or analytics. While using Lambda to process data can be an option, it may not be most efficient solution for processing large volumes of clickstream data.

Therefore, collecting the data from Kinesis Data Streams, using Kinesis Data Firehose to transmit it to S3 data lake, and loading it into Redshift for analysis is the recommended approach. This combination provides scalable, real-time streaming solution with storage and analytics capabilities that can handle high volume of clickstream data.

upvoted 2 times

 **Rahulbit34** 10 months, 4 weeks ago

Clickstream is the key - Answer is D

upvoted 1 times

 **PaoloRoma** 1 year ago

Selected Answer: A

I am going to be unpopular here and I'll go for A). Even if there are other services that offer a better experience, Data Pipeline can do the job here. "you can use AWS Data Pipeline to archive your web server's logs to Amazon Simple Storage Service (Amazon S3) each day and then run a weekly Amazon EMR (Amazon EMR) cluster over those logs to generate traffic reports"
<https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html> In the question there is no specific timing requirement for analytics. Also the EMR cluster job can be scheduled to be executed daily.

Option D is a valid answer too, however with Amazon Redshift Streaming Ingestion "you can connect to Amazon Kinesis Data Streams data streams and pull data directly to Amazon Redshift without staging data in S3" <https://aws.amazon.com/redshift/redshift-streaming-ingestion/>. So in this scenario Kinesis Data Firehose and S3 are redundant.

upvoted 6 times

 **MutiverseAgent** 8 months, 3 weeks ago

I think I agree with you, I does not make sense in option D) using Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake and then to Redshift, as you can send directly the data from Firehose to Redshift.

upvoted 2 times

 **juanrasus2** 5 months, 1 week ago

Also the Kinesis family is related to real time or near real time services. This is not a requirement at all. We have to process data daily, but not need to do it in real time

upvoted 2 times

 **pentium75** 3 months ago

Question asks how to "transmit and process the clickstream data", NOT how to analyze it. This picture shows exactly scenario D:

Producer - Kinesis - Intermediate S3 bucket - Redshift

<https://d2908q01vomqb2.cloudfront.net/b6692ea5df920cad691c20319a6ffd7a4a766b8/2020/07/30/StreamTransformAnalyzeKinesisLambdaRedshift1.png>

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

 **studis** 1 year, 3 months ago

It is C.

The image in here <https://aws.amazon.com/kinesis/data-firehose/> shows how kinesis can send data collected to firehose who can send it to Redshift.

It is also possible to use an intermediary S3 bucket between firehose and redshift. See image in here <https://aws.amazon.com/blogs/big-data/stream-transform-and-analyze-xml-data-in-real-time-with-amazon-kinesis-aws-lambda-and-amazon-redshift/>

upvoted 1 times

 **pentium75** 3 months ago

Makes sense, but this is D, not C

upvoted 1 times

 **sebasta** 1 year, 3 months ago

Why not A?

You can collect data with AWS Data Pipeline and then analyze it with EMR. What's wrong with this option?

upvoted 4 times

 **bearcandy** 1 year, 3 months ago

It's not A, the wording is tricky! It says "to archive the data to S3" - there is no mention of archiving in the question, so it has to be D :)

upvoted 3 times

 **pentium75** 3 months ago

And, the question is not asking about analyzing the data at all, just about "transmitting and processing".

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

D is correct

upvoted 1 times

 **PS_R** 1 year, 4 months ago

Click Stream & Analyse/ process- Think KDS,

upvoted 3 times

 **BoboChow** 1 year, 5 months ago

Selected Answer: D

D seems to make sense

upvoted 4 times

 **JesseesS** 1 year, 5 months ago

Option D is correct... See the resource. Thank you Ariel

upvoted 1 times

Question #60

Topic 1

A company has a website hosted on AWS. The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS. What should a solutions architect do to meet this requirement?

- A. Update the ALB's network ACL to accept only HTTPS traffic.
- B. Create a rule that replaces the HTTP in the URL with HTTPS.
- C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
- D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.

To meet the requirement of forwarding all requests to the website so that the requests will use HTTPS, a solutions architect can create a listener rule on the ALB that redirects HTTP traffic to HTTPS. This can be done by creating a rule with a condition that matches all HTTP traffic and a rule action that redirects the traffic to the HTTPS listener. The HTTPS listener should already be configured to accept HTTPS traffic and forward it to the target group.

upvoted 19 times

 **Burugduystunstugudunstuy** 1 year, 3 months ago

Option A. Updating the ALB's network ACL to accept only HTTPS traffic is not a valid solution because the network ACL is used to control inbound and outbound traffic at the subnet level, not at the listener level.

Option B. Creating a rule that replaces the HTTP in the URL with HTTPS is not a valid solution because this would not redirect the traffic to the HTTPS listener.

Option D. Replacing the ALB with a Network Load Balancer configured to use Server Name Indication (SNI) is not a valid solution because it would not address the requirement to redirect HTTP traffic to HTTPS.

upvoted 15 times

 **masetromain** Highly Voted 1 year, 5 months ago

Selected Answer: C

Answer C :

https://docs.aws.amazon.com/fr_fr/elasticloadbalancing/latest/application/create-https-listener.html

<https://aws.amazon.com/fr/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/>

upvoted 14 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: C

<https://repost.aws/knowledge-center/elb-redirect-http-to-https-using-alb>

Steps 6-8 tells exactly how to do this:

"6. Select a load balancer, and then choose HTTP Listener.

7. Under Rules, choose View/edit rules.

8. Choose Edit Rule to modify the existing default rule to redirect all HTTP requests to HTTPS. Or, insert a rule between the existing rules (if appropriate for your use case)."

upvoted 1 times

 **Ruffyit** 5 months ago

C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.

upvoted 2 times

 **AWSStudyBuddy** 5 months, 1 week ago

Selected Answer: C

This solution meets all of the requirements:

Forward all requests to the website so that the requests will use HTTPS: The ALB can be configured to redirect all HTTP traffic to HTTPS. The other options are not as good for this scenario:

- A. Updating the ALB's network ACL to accept only HTTPS traffic will prevent users from accessing the website using HTTP.
- B. Creating a rule that replaces the HTTP in the URL with HTTPS will not prevent users from accessing the website using HTTP.

D. Replacing the ALB with a Network Load Balancer configured to use Server Name Indication (SNI) is not necessary because the ALB can be configured to redirect all HTTP traffic to HTTPS.

upvoted 2 times

Tom123456ac 5 months, 3 weeks ago

I hate this question description "The company wants to forward all requests to the website so that the requests will use HTTPS."

upvoted 2 times

Guru4Cloud 7 months, 2 weeks ago

Selected Answer: C

The best solution is to create a listener rule on the Application Load Balancer (ALB) to redirect HTTP traffic to HTTPS (option C).

Here is why:

ALB listener rules allow you to redirect traffic from one listener port (e.g. 80 for HTTP) to another (e.g. 443 for HTTPS). This achieves the goal to forward all requests over HTTPS.

Network ACLs control traffic at the subnet level and cannot distinguish between HTTP and HTTPS requests to implement a redirect (option A incorrect).

Replacing HTTP with HTTPS in the URL happens at the client side. It does not redirect at the ALB (option B incorrect).

Network Load Balancers work at the TCP level and do not understand HTTP or HTTPS protocols. So they cannot redirect in this manner (option D incorrect).

upvoted 6 times

miki111 8 months, 1 week ago

Option C is the correct answer

upvoted 1 times

cookieMr 9 months, 1 week ago

Selected Answer: C

A. Network ACLs operate at subnet level and control inbound and outbound traffic. Updating the network ACL alone will not enforce the redirection of HTTP to HTTPS.

B. This approach would require modifying application code or server configuration to perform URL rewrite. It is not an optimal solution as it adds complexity and potential maintenance overhead. Moreover, it does not leverage the ALB's capabilities for handling HTTP-to-HTTPS redirection.

D. While NLB can handle SSL/TLS termination using SNI for routing requests to different services, replacing the ALB solely to enforce HTTP-to-HTTPS redirection would be an unnecessary and more complex solution.

Therefore, the recommended approach is to create a listener rule on the ALB to redirect HTTP traffic to HTTPS. By configuring a listener rule, you can define a redirect action that automatically directs HTTP requests to their corresponding HTTPS versions.

upvoted 4 times

Abrar2022 10 months, 1 week ago

A solutions architect should create listen rules to direct http traffic to https.

upvoted 1 times

cheese929 11 months, 2 weeks ago

Selected Answer: C

C is correct. Traffic redirection will solve it.

upvoted 2 times

elearningtakai 12 months ago

Selected Answer: C

This rule can be created in the following way:

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose Load Balancers.
3. Select the ALB and choose Listeners.
4. Choose View/edit rules and then choose Add rule.
5. In the Add Rule dialog box, choose HTTPS.
6. In the Default action dialog box, choose Redirect to HTTPS.
7. Choose Save rules.

This listener rule will redirect all HTTP requests to HTTPS, ensuring that all traffic is encrypted.

upvoted 4 times

mell1222 1 year ago

Selected Answer: C

Configure an HTTPS listener on the ALB: This step involves setting up an HTTPS listener on the ALB and configuring the security policy to use a secure SSL/TLS protocol and cipher suite.

Create a redirect rule on the ALB: The redirect rule should be configured to redirect all incoming HTTP requests to HTTPS. This can be done by creating a redirect rule that redirects HTTP requests on port 80 to HTTPS requests on port 443.

Update the DNS record: The DNS record for the website should be updated to point to the ALB's DNS name, so that all traffic is routed through the ALB.

Verify the configuration: Once the configuration is complete, the website should be tested to ensure that all requests are being redirected to HTTPS. This can be done by accessing the website using HTTP and verifying that the request is redirected to HTTPS.

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

✉ **Shasha1** 1 year, 3 months ago

C

To redirect HTTP traffic to HTTPS, a solutions architect should create a listener rule on the ALB to redirect HTTP traffic to HTTPS. Option A is not correct because network ACLs do not have the ability to redirect traffic. Option B is not correct because it does not redirect traffic, it only replaces the URL. Option D is not correct because a Network Load Balancer does not have the ability to handle HTTPS traffic.

upvoted 2 times

✉ **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

✉ **hanhdroid** 1 year, 5 months ago

Selected Answer: C

Answer C: <https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/>

upvoted 4 times

Question #61

Topic 1

A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis.

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

- A. Store the database credentials in the instance metadata. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and instance metadata at the same time.
- B. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and the credentials in the configuration file at the same time. Use S3 Versioning to ensure the ability to fall back to previous values.
- C. Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.
- D. Store the database credentials as encrypted parameters in AWS Systems Manager Parameter Store. Turn on automatic rotation for the encrypted parameters. Attach the required permission to the EC2 role to grant access to the encrypted parameters.

Correct Answer: C*Community vote distribution*

C (100%)

 **KVK16**  1 year, 5 months ago

Selected Answer: C

Secrets manager supports Autorotation unlike Parameter store.
upvoted 22 times

 **JesseeS** 1 year, 5 months ago

Parameter store does not support autorotation.
upvoted 9 times

 **Buruguduystunstugudunstuy**  1 year, 3 months ago

Selected Answer: C

The correct solution is C. Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.

AWS Secrets Manager is a service that enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. By storing the database credentials as a secret in Secrets Manager, you can ensure that they are not hardcoded in the application and that they are automatically rotated on a regular basis. To grant the EC2 instance access to the secret, you can attach the required permission to the EC2 role. This will allow the application to retrieve the secret from Secrets Manager as needed.

upvoted 13 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option A, storing the database credentials in the instance metadata and using a Lambda function to update them, would not meet the requirement of not hardcoding the credentials in the application.

Option B, storing the database credentials in an encrypted S3 bucket and using a Lambda function to update them, would also not meet this requirement, as the application would still need to access the credentials from the configuration file.

Option D, storing the database credentials as encrypted parameters in AWS Systems Manager Parameter Store, would also not meet this requirement, as the application would still need to access the encrypted parameters in order to use them.

upvoted 7 times

 **Atul6969**  1 month, 1 week ago

Selected Answer: C

test kjlshfjkh jfskjfnkj kj bskjfb kj kjs bfkjs b kjf
upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: C

Secrets Manager is purpose built for this scenario

AB are wrong and insecure way of doing this

D Parameter store with encrypted string can be used for this but is not ideal choice and AFAIK it does not support automatic rotation without extra programming

upvoted 1 times

1Alpha1 3 months ago

Selected Answer: C

C - "Auto Rotation"

upvoted 1 times

dumpsowner 5 months ago

100% valid dumps i found this site <https://www.linkedin.com/company/amazon-dumps/?viewAsMember=true>

upvoted 1 times

Ruffyt 5 months ago

AWS Secrets Manager is a service that enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. By storing the database credentials as a secret in Secrets Manager, you can ensure that they are not hardcoded in the application and that they are automatically rotated on a regular basis. To grant the EC2 instance access to the secret, you can attach the required permission to the EC2 role.

upvoted 1 times

Guru4Cloud 7 months, 2 weeks ago

Selected Answer: C

Storing the credentials in AWS Secrets Manager and enabling automatic rotation meets the requirements with the least operational overhead. The EC2 instance role just needs permission to access the secret, and Secrets Manager handles rotating the credentials automatically on a schedule.

upvoted 1 times

TariqKipkemei 7 months, 2 weeks ago

Selected Answer: C

Key Autorotation = AWS Secrets Manager

upvoted 2 times

miki111 8 months, 1 week ago

Option C is the right answer.

upvoted 1 times

cookieMr 9 months, 1 week ago

Selected Answer: C

Storing the credentials in Secrets Manager provides dedicated and secure management. With automatic rotation enabled, Secrets Manager handles the credential updates automatically. Attaching the necessary permissions to the EC2 role allows the application to securely access the secret.

This approach minimizes operational overhead and provides a secure and managed solution for credential management.

upvoted 2 times

Bmarodi 9 months, 3 weeks ago

Selected Answer: C

The solution that meets the requirements with the least operational overhead, is option C.

upvoted 1 times

Bmarodi 10 months, 1 week ago

Selected Answer: C

My choice is c.

upvoted 1 times

AndyMartinez 1 year, 1 month ago

Selected Answer: C

The right option is C.

upvoted 1 times

Adios_Amigo 1 year, 1 month ago

C is the most correct answer. Automatic replacement must be performed by the secret manager.

upvoted 1 times

career360guru 1 year, 3 months ago

Selected Answer: C

Option C - As the requirement is to rotate the secrets Secrets manager is the one that can support it.

upvoted 1 times

Wpcorgan 1 year, 4 months ago

C is correct

upvoted 2 times

Question #62

Topic 1

A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB). The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA). The certificate must be rotated each year before the certificate expires.

What should a solutions architect do to meet these requirements?

- A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
- B. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Import the key material from the certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
- C. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
- D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.

Correct Answer: D

Community vote distribution

D (94%) 6%

≡ **Sinaneos** Highly Voted 1 year, 5 months ago

Selected Answer: D

It's a third-party certificate, hence AWS cannot manage renewal automatically. The closest thing you can do is to send a notification to renew the 3rd party certificate.

upvoted 47 times

≡ **mabotega** Highly Voted 1 year, 4 months ago

Selected Answer: D

It is D, because ACM does not manage the renewal process for imported certificates. You are responsible for monitoring the expiration date of your imported certificates and for renewing them before they expire.

Check this question on the link below:

Q: What types of certificates can I create and manage with ACM?

https://www.amazonaws.cn/en/certificate-manager/faqs/#Managed_renewal_and_deployment

upvoted 20 times

≡ **Anji195** Most Recent 1 month, 2 weeks ago

Yes it's D. Here is a clear explanation.

Imported certificates – If you want to use a third-party certificate with Amazon CloudFront, Elastic Load Balancing, or Amazon API Gateway, you may import it into ACM using the AWS Management Console, AWS CLI, or ACM APIs. ACM can not renew imported certificates, but it can help you manage the renewal process. You are responsible for monitoring the expiration date of your imported certificates and for renewing them before they expire. You can use ACM CloudWatch metrics to monitor the expiration dates of an imported certificates and import a new third-party certificate to replace an expiring one.

https://www.amazonaws.cn/en/certificate-manager/faqs/#Managed_renewal_and_deployment

upvoted 2 times

≡ **awsgeek75** 2 months, 1 week ago

Selected Answer: D

"certificate that is issued by an external certificate authority (CA)"

AB will create a new certificate in AWS

C will also create a new certificate but this is not what PCA are for *(<https://docs.aws.amazon.com/privateca/latest/userguide/PcaWelcome.html>)

D: Import the certificate is correct answer

upvoted 1 times

≡ **1Alpha1** 3 months ago

Selected Answer: D

D - "External CA" --> 'Update Manually'

upvoted 1 times

≡ **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: A

internal CA are typically trusted only within the organization unless you manually distribute and trust the root certificate elsewhere

external CA:

Certificates from a well-known external CA are trusted by most browsers and systems by default

<https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html>

"Public certificates that you request through ACM are obtained from Amazon Trust Services, an Amazon managed public certificate authority (CA). ... Any browser, application, or OS that includes the Amazon or Starfield roots will trust public certificates obtained from ACM."

The answer is A, different story if they said external certificate

upvoted 2 times

✉ **Ruffyt** 5 months ago

: What types of certificates can I create and manage with ACM?

https://www.amazonaws.cn/en/certificate-manager/faqs/#Managed_renewal_and_deployment

upvoted 1 times

✉ **est3la21** 6 months, 2 weeks ago

answer is D

upvoted 1 times

✉ **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: D

The key points are:

Obtain certificate from external CA, not ACM

Import the external certificate into ACM

Apply imported certificate to the ALB

Set up EventBridge rule to trigger notification on certificate expiration

Manually renew and rotate the external certificate each year.

upvoted 2 times

✉ **miki111** 8 months, 1 week ago

Option D is the right answer.

upvoted 2 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: D

D: With this approach, you import the third-party certificate into ACM, which allows you to centrally manage and apply it to the ALB. By configuring CloudWatch Events, you can receive notifications when the certificate is close to expiring, prompting you to manually initiate the rotation process.

A & B: These options assume that the SSL/TLS certificate can be issued directly by ACM. However, since the requirement specifies that the certificate should be issued by an external certificate authority (CA), this option is not suitable.

C: ACM Private Certificate Authority is used when you want to create your own private CA and issue certificates from it. It does not support certificates issued by external CAs. Therefore, this option is not suitable for the given requirement.

upvoted 3 times

✉ **Router** 9 months, 1 week ago

D is correct, since it's an external certificate

upvoted 1 times

✉ **Bmarodi** 9 months, 3 weeks ago

Selected Answer: D

Option D meets these requirements.

upvoted 1 times

✉ **Bmarodi** 10 months, 1 week ago

Since the external certificate, you can't automate it. Only u can do is getting notefication, and renew it manually, no other way roud.

upvoted 1 times

✉ **Abrar2022** 10 months, 1 week ago

In the question it mentions that it's a third-party certificate. AWS has not got much control of third-party certificates and cannot manage renewal automatically. The closest thing you can do is to send a notification to renew the 3rd party certificate.

upvoted 1 times

✉ **Rahulbit34** 10 months, 4 weeks ago

EXTERNAL certofocation is the key - Manual rotation is required so Answer is D

upvoted 3 times

✉ **cheese929** 11 months, 2 weeks ago

Selected Answer: D

A B and C are all using AWS issued cert. Only D uses cert issued by external CA, which meets the requirement.

upvoted 1 times

Question #63

Topic 1

A company runs its infrastructure on AWS and has a registered base of 700,000 users for its document management application. The company intends to create a product that converts large .pdf files to .jpg image files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over time.

Which solution meets these requirements MOST cost-effectively?

- A. Save the .pdf files to Amazon S3. Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to .jpg format and store them back in Amazon S3.
- B. Save the .pdf files to Amazon DynamoDB. Use the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to .jpg format and store them back in DynamoDB.
- C. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic Block Store (Amazon EBS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the files to .jpg format. Save the .pdf files and the .jpg files in the EBS store.
- D. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the file to .jpg format. Save the .pdf files and the .jpg files in the EBS store.

Correct Answer: A

Community vote distribution



A (98%)

✉  **ArielSchivo**  1 year, 5 months ago

Selected Answer: A

Option A. Elastic BeanStalk is expensive, and DocumentDB has a 400KB max to upload files. So Lambda and S3 should be the one.
upvoted 45 times

✉  **raffaello44** 1 year, 4 months ago

is lambda scalable as an EC2 ?
upvoted 5 times

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

lambda has near infinite scale
upvoted 2 times

✉  **rob74** 1 year, 4 months ago

In addition to this Lambda is paid only when used....
upvoted 6 times

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

I'm thinking when you wrote DocumentDB you meant it as DynamoDB...yes?
upvoted 6 times

✉  **benjl** 1 year, 3 months ago

Yes, DynamoDB has 400KB limit for the item.
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/ServiceQuotas.html>
upvoted 7 times

✉  **cookieMr**  9 months, 1 week ago

Selected Answer: A

B. Using DynamoDB for storing and processing large .pdf files would not be cost-effective due to storage and throughput costs associated with DynamoDB.

C. Using Elastic Beanstalk with EC2 and EBS storage can work, but it may not be most cost-effective solution. It involves managing the underlying infrastructure and scaling manually.

D. Similar to C, using Elastic Beanstalk with EC2 and EFS storage can work, but it may not be most cost-effective solution. EFS is a shared file storage service and may not provide optimal performance for conversion process, especially as demand and file sizes increase.

A. leverages Lambda and the scalable and cost-effective storage of S3. With Lambda, you only pay for actual compute time used during the file conversion, and S3 provides durable and scalable storage for both .pdf files and .jpg files. The S3 PUT event triggers Lambda to perform conversion, eliminating need to manage infrastructure and scaling, making it most cost-effective solution for this scenario.

upvoted 6 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: A

S3 is the only scalable option for such a large user base in cost effective way.

BCD can work but will be extremely costly

upvoted 1 times

 **Ruffyit** 5 months ago

B. Using DynamoDB for storing and processing large .pdf files would not be cost-effective due to storage and throughput costs associated with DynamoDB.

C. Using Elastic Beanstalk with EC2 and EBS storage can work, but it may not be most cost-effective solution. It involves managing the underlying infrastructure and scaling manual

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: A

Option A is the most cost-effective solution that meets the requirements. Here is why:

Storing the PDFs in Amazon S3 is inexpensive and scalable storage.

Using S3 events to trigger Lambda functions to do the file conversion is a serverless approach that scales automatically. No need to manage EC2 instances.

Lambda usage is charged only for compute time used, which is cost-efficient for spiky workloads like this.

Storing the converted JPGs back in S3 keeps the storage scalable and cost-effective.

upvoted 3 times

 **RDX19** 8 months, 1 week ago

Selected Answer: A

Option A is right answer since Dynamo DB has size limitations.

upvoted 2 times

 **miki111** 8 months, 1 week ago

Option A is the right answer.

upvoted 1 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: A

The solution meets these requirements most cost-effectively is option A.

upvoted 1 times

 **Bmarodi** 10 months, 1 week ago

Selected Answer: A

I think the best solution is A.

Ref. <https://s3.amazonaws.com/doc/s3-developer-guide/RESTObjectPUT.html>

upvoted 1 times

 **Abrar2022** 10 months, 1 week ago

Since this requires a cost-effect solution then you can use Lambda to convert pdf files to jpeg and store them on S3. Lambda is serverless, so only pay when you use it and automatically scales to cope with demand.

upvoted 1 times

 **srirajav** 11 months ago

if Option A is correct, however storing the data back to the same S3, wont it cause infinite looping, it's not best practice right storing a object that is processed by Lambda function to the same S3 bucket, it has chances to cause infinite Loop and then if the option B cant we increase the limits of Dynamo DB requesting AWS?

upvoted 2 times

 **bedwal2020** 11 months ago

In question, it is never mentioned that the jpg files will also be stored in same s3 bucket. We can have different s3 buckets right ?

upvoted 2 times

 **cheese929** 11 months, 2 weeks ago

Selected Answer: A

Answer A is the most cost effective solution that meets the requirement

upvoted 1 times

 **channn** 11 months, 4 weeks ago

Selected Answer: A

Key words: MOST cost-effectively, so S3 + Lambda

upvoted 1 times

 **SilentMilli** 1 year, 2 months ago

Selected Answer: A

This solution will meet the company's requirements in a cost-effective manner because it uses a serverless architecture with AWS Lambda to convert the files and store them in S3. The Lambda function will automatically scale to meet the demand for file conversions and S3 will

automatically scale to store the original and converted files as needed.

upvoted 2 times

Burugduystunstugudunstuy 1 year, 3 months ago

Selected Answer: A

Option A is the most cost-effective solution that meets the requirements.

In this solution, the .pdf files are saved to Amazon S3, which is an object storage service that is highly scalable, durable, and secure. S3 can store unlimited amounts of data at a very low cost.

The S3 PUT event triggers an AWS Lambda function to convert the .pdf files to .jpg format. Lambda is a serverless compute service that runs code in response to specific events and automatically scales to meet demand. This means that the conversion process can scale up or down as needed, without the need for manual intervention.

The converted .jpg files are then stored back in S3, which allows the company to store both the original .pdf files and the converted .jpg files in the same service. This reduces the complexity of the solution and helps to keep costs low.

upvoted 1 times

Burugduystunstugudunstuy 1 year, 3 months ago

Option C is also a valid solution, but it may be more expensive due to the use of EC2 instances, EBS storage, and an Auto Scaling group. These resources can add additional cost, especially if the demand for the conversion service grows rapidly.

Option D is not a valid solution because it uses Amazon EFS, which is a file storage service that is not suitable for storing large amounts of data. EFS is designed for storing and accessing files that are accessed frequently, such as application logs and media files. It is not designed for storing large files like .pdf or .jpg files.

upvoted 2 times

karbob 1 year, 2 months ago

EFS is optimized for a wide range of workloads and file sizes, and it can store files of any size up to the capacity of the file system. EFS scales automatically to meet your storage needs, and it can store petabyte-level capacity.

upvoted 1 times

career360guru 1 year, 3 months ago

Selected Answer: A

Option A

upvoted 1 times

JayBee65 1 year, 3 months ago

This gives an example, using GET rather than PUT, but the idea is the same: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/tutorial-s3-object-lambda-uppercase.html>

upvoted 1 times

Question #64

Topic 1

A company has more than 5 TB of file data on Windows file servers that run on premises. Users and applications interact with the data each day. The company is moving its Windows workloads to AWS. As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency. The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS.

What should a solutions architect do to meet these requirements?

- A. Deploy and configure Amazon FSx for Windows File Server on AWS. Move the on-premises file data to FSx for Windows File Server. Reconfigure the workloads to use FSx for Windows File Server on AWS.
- B. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises file data to the S3 File Gateway. Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway.
- C. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises file data to Amazon S3. Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway, depending on each workload's location.
- D. Deploy and configure Amazon FSx for Windows File Server on AWS. Deploy and configure an Amazon FSx File Gateway on premises. Move the on-premises file data to the FSx File Gateway. Configure the cloud workloads to use FSx for Windows File Server on AWS. Configure the on-premises workloads to use the FSx File Gateway.

Correct Answer: A*Community vote distribution*

sba21 1 year, 5 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/83281-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 23 times

MutiverseAgent 8 months, 3 weeks ago

Agree answer is D)

Requirements are:

- "Users and applications interact with the data each day"
- "the company requires access to AWS and on-premises file storage with minimum latency"

Explanation: Answer A) will work with the same on-prem <> aws latency as in answer D) as both use the VPN Connection. Having said this, by using an Amazon FSx File Gateway on premise as the D) scenario mentioned, all users will have a great benefit on using the cache that the FSx File Gateway has on their daily workloads. And that is part of the requirements: "users", "each day", "latency"

upvoted 3 times

MrAWS 1 year, 2 months ago

D IS WRONG - Its used for caching. you cannot 'Move the on-premises file data to the FSx File Gateway.' which is stated in answer D. It pretty sure AWS employee's are spamming this site with the wrong answers intentionally.

upvoted 15 times

DarthVaper 6 months ago

What's the problem with it being a cache? They did say "the company requires access to AWS and on-premises file storage with minimum latency."

Not discarding what you said but what's wrong here?

upvoted 2 times

chagantik90 3 months, 3 weeks ago

you don't move data to gateway, its cached when people use those files from Fsx server
upvoted 1 times

dsshahu01 1 month ago

The problem with cache is - It needs to refreshed, which is an overkill for a migration project

The cache refresh requires another solution since the users/applications interact with it daily which means it does modify often.

upvoted 1 times

LIORAGE 4 days, 11 hours ago

Selected Answer: D

D: FSX File gateway is nessary for communication between on-premise and aws FSX for window
upvoted 1 times

TheFivePips 1 month ago

I kinda hate this question. A) seems like the least operational overhead and the simplest to do, but doesn't really meet the low latency goal D) provides some of the benefits of caching for low latency for on-prem, but the way it's worded doesn't really make sense. You don't move data to a gateway, and it would be more complicated to set up.

Do you go with an answer that doesn't meet all the criteria, or with the answer that doesn't make a lot of sense. Fuck if I know
upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: D

Windows File Servers + Preserve compatibility so BC is wrong due to S3
A does not provide on-premise access and suggest to move the files which is wrong as company wants to keep on-prem access
D meets all the requirements.
upvoted 2 times

 **ROBERTXLION** 2 months, 3 weeks ago

Selected Answer: A

To meet the company's requirements of accessing both AWS and on-premises file storage with minimum latency, while minimizing operational overhead and maintaining existing file access patterns, a solutions architect should choose

Option A: Deploy and configure Amazon FSx for Windows File Server on AWS. This option allows for the deployment of FSx for Windows File Server on AWS, facilitating the migration of on-premises file data to FSx.

By reconfiguring the workloads to use FSx for Windows File Server on AWS, the company can ensure seamless access to the file data while leveraging the benefits of AWS infrastructure.

This solution aligns with the company's objective of moving Windows workloads to AWS and utilizes the existing AWS Site-to-Site VPN connection for connectivity.

upvoted 1 times

 **ignajtolandstrong** 2 months, 4 weeks ago

Selected Answer: D

Amazon FSx File Gateway is a service that provides low latency and efficient access to Amazon FSx for Windows File Server shares from on-premises facilities. It helps eliminate on-premises file servers and consolidates all the data into AWS to take advantage of the scale and economics of cloud storage
upvoted 1 times

 **pentium75** 3 months ago

Selected Answer: D

A does not include any on-premises component, thus it can't meet the "access to ... on-premises file storage with minimum latency" requirement. B and C use S3 which cannot be directly accessed by the Windows servers they are going to move to AWS.
upvoted 1 times

 **SaurabhTiwari1** 3 months, 1 week ago

Selected Answer: A

Option A is correct because
- minimum latency
- minimum operational overhead
- requires no significant changes to the existing file access patterns

Option D is incorrect -

- Amazon FSx File Gateway on-premises, which would add additional complexity and potential latency, as the data would need to be transferred between the on-premises gateway and AWS. These options would also require reconfiguring the workloads to use the gateways, which could involve significant changes to the existing file access patterns.
- unnecessary complexity and potential latency
upvoted 2 times

 **pentium75** 3 months ago

A does not include any on-premises component, how would it meet the "access to ... on-premises file storage with minimum latency" requirement?
upvoted 1 times

 **chagantik90** 3 months, 3 weeks ago

Selected Answer: A

Moving data to Gateway doesn't make sense and splitting cloud workload and on-prem workload doesn't make sense in D. So closest is A and I know A doesn't really cover about latency but A looks the best option here
upvoted 1 times

 **pentium75** 3 months ago

A does not include any on-premises component, how would it meet the "access to ... on-premises file storage with minimum latency" requirement?

With D you can access the data with minimum latency on-premises (from the gateway) and in AWS (from FSx).

upvoted 1 times

 **MiniYang** 4 months ago

Selected Answer: A

Amazon FSx for Windows File Server provides the feel of a native Windows file server while providing low-latency access on AWS. This allows your local users and applications to seamlessly access file systems in AWS without requiring significant changes to their access.

Although D also mentions Amazon FSx for Windows File Server, it also includes Amazon FSx File Gateway, which may introduce additional complexity. So, for the need to minimize latency without making major changes while minimizing operational overhead, A looks to fit those criteria better. The company uses an AWS site-to-site VPN connection and may prefer option A over D due to some added latency that the VPN may cause, as well as possible bandwidth limitations.

upvoted 1 times

 **pentium75** 3 months ago

Yes, FSx provides "low-latency access on AWS", but we also need "access to ... on-premises file storage with minimum latency". A does not include any on-premises component.

upvoted 1 times

 **tom_cruise** 4 months, 4 weeks ago

Selected Answer: D

Key: minimum latency and on premise:

"The Amazon FSx File Gateway extends Amazon FSx for Windows File Server to any site with an internet connection. It provides a scalable local cache, up to 64 TB, for low latency access to most recently used files. By deploying an Amazon FSx File Gateway within your data center or remote and branch offices, your Windows clients are able to connect over the LAN. As Amazon FSx File Gateway is a local cache of most recently accessed data backed by an Amazon FSx file system, it looks like a local file server to users and applications."

<https://aws.amazon.com/blogs/storage/accessing-your-file-workloads-from-on-premises-with-file-gateway/>

upvoted 2 times

 **Ruffyt** 5 months ago

Agree answer is D)

Requirements are:

- "Users and applications interact with the data each day"
- "the company requires access to AWS and on-premises file storage with minimum latency"

Explanation: Answer A) will work with the same on-prem <> aws latency as in answer D) as both use the VPN Connection. Having said this, by using an Amazon FSx File Gateway on premise as the D) scenario mentioned, all users will have a great benefit on using the cache that the FSx File Gateway has on their daily workloads. And that is part of the requirements: "users", "each day", "latency"

upvoted 2 times

 **AWSStudyBuddy** 5 months, 1 week ago

Selected Answer: D

Amazon FSx for Windows File Server and Amazon FSx File Gateway are two extremely effective file storage options that offer minimal latency access to AWS and on-premises file storage. They offer low-latency access to file data for users and programs, independent of the location of the data.

reduces overhead: Amazon File Server for Windows and Amazon File Gateway are managed services provided by Amazon. Therefore, the management of the underlying infrastructure is not a concern for the organization.

Not much has to be changed about the current file access patterns in order to achieve this: Protocols for the Windows file system are used by Amazon FSx for Windows File Server and Amazon FSx File Gateway. Consequently, the workloads of the organization can access the file data in the same manner that they

upvoted 1 times

 **jibsy** 5 months, 2 weeks ago

from ChatGPT

A. Deploy and configure Amazon FSx for Windows File Server on AWS. Move the on-premises file data to FSx for Windows File Server. Reconfigure the workloads to use FSx for Windows File Server on AWS.

This option is a suitable choice for several reasons:

Amazon FSx for Windows File Server is designed to provide Windows-compatible file storage in AWS.

It minimizes operational overhead as Amazon FSx is a managed service.

No significant changes to the existing file access patterns are required, as FSx is Windows-compatible and allows for seamless integration with existing workloads.

Using an AWS Site-to-Site VPN connection is consistent with the existing connectivity method.

upvoted 1 times

 **Abitek007** 5 months, 3 weeks ago

Selected Answer: A

they already have a site to site VPN connection

upvoted 2 times

 **paniya93** 5 months, 3 weeks ago

Selected Answer: D

Answer is D

somewhere, the 6xx question gives the correct answer as D.

upvoted 2 times

Question #65

Topic 1

A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports.

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

- A. Use existing Python libraries to extract the text from the reports and to identify the PHI from the extracted text.
- B. Use Amazon Textract to extract the text from the reports. Use Amazon SageMaker to identify the PHI from the extracted text.
- C. Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.
- D. Use Amazon Rekognition to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

The correct solution is C: Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.

Option C: Using Amazon Textract to extract the text from the reports, and Amazon Comprehend Medical to identify the PHI from the extracted text, would be the most efficient solution as it would involve the least operational overhead. Textract is specifically designed for extracting text from documents, and Comprehend Medical is a fully managed service that can accurately identify PHI in medical text. This solution would require minimal maintenance and would not incur any additional costs beyond the usage fees for Textract and Comprehend Medical.

upvoted 14 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option A: Using existing Python libraries to extract the text and identify the PHI from the text would require the hospital to maintain and update the libraries as needed. This would involve operational overhead in terms of keeping the libraries up to date and debugging any issues that may arise.

Option B: Using Amazon SageMaker to identify the PHI from the extracted text would involve additional operational overhead in terms of setting up and maintaining a SageMaker model, as well as potentially incurring additional costs for using SageMaker.

Option D: Using Amazon Rekognition to extract the text from the reports would not be an effective solution, as Rekognition is primarily designed for image recognition and would not be able to accurately extract text from PDF or JPEG files.

upvoted 5 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: C

Textract = Extract text from PDF/images

Comprehend Medical = PHI

ABD are wrong products for this requirement so won't achieve the results

upvoted 1 times

 **djgodzilla** 3 months, 1 week ago

Selected Answer: C

Both Rekognition and Textract possess the ability to detect text within images, yet they are optimized for differing applications.

Rekognition specializes in identifying text located spatially within an image, for instance, words displayed on street signs, t-shirts, or license plates. Its typical use cases encompass visual search, content filtering, deriving insights from content, among others. However, it's not the ideal choice for images containing more than 100 words, as this exceeds its limitation.

On the other hand, Textract is tailored more towards processing documents and PDFs, offering a comprehensive suite for Optical Character Recognition (OCR). It proves useful in scenarios involving financial reports, medical records, receipts, ID documents, and more.

upvoted 2 times

 **Ruffyt** 5 months ago

The correct solution is C: Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.

Option C: Using Amazon Textract to extract the text from the reports, and Amazon Comprehend Medical to identify the PHI from the extracted text, would be the most efficient solution as it would involve the least operational overhead. Textract is specifically designed for extracting text from documents, and Comprehend Medical is a fully managed service that can accurately identify PHI in medical text. This solution would require minimal maintenance and would not incur any additional costs beyond the usage fees for Textract and Comprehend Medical.

upvoted 1 times

AWSStudyBuddy 5 months, 1 week ago

Selected Answer: C

- Amazon Textract: This program is made to extract text and data from scanned documents, such as pictures and PDFs. It helps to retain the formatting of the report by automatically extracting text while preserving the document's layout.

Identifying and extracting medical information, including protected health information (PHI), from unstructured text is the specialty of Amazon Comprehend Medical. Medical entities that are frequently included in reporting on healthcare, such as ailments, drugs, and more, can be recognized by it.

upvoted 1 times

Chiquitabandita 6 months, 3 weeks ago

with the choices here, I would go with C, but if offered, I would use amazon extract for the text and use Macie to do the scanning of text files, not comprehend.

upvoted 1 times

Guru4Cloud 7 months, 2 weeks ago

Selected Answer: C

Here's why:

Amazon Textract has built-in support to extract text from PDFs and images, eliminating the need to build this yourself with Python libraries. Amazon Comprehend Medical has pre-trained machine learning models to identify PHI entities out-of-the-box, avoiding the need to train your own SageMaker model.

Using these fully managed AWS services minimizes operational overhead of maintaining machine learning models yourself.

upvoted 1 times

miki111 8 months, 1 week ago

Option C is the right answer.

upvoted 2 times

cookieMr 9 months, 1 week ago

Selected Answer: C

C leverages capabilities of Textract, which is a service that automatically extracts text and data from documents, including PDF and JPEG. By using Textract, hospital can extract text content from reports without need for additional custom code or libraries.

Once text is extracted, hospital can then use Comprehend Medical, a natural language processing service specifically designed for medical text, to analyze and identify PHI. It can recognize medical entities such as medical conditions, treatments, and patient information.

A. suggests using existing Python libraries, which would require hospital to develop and maintain custom code for text extraction and PHI identification.

B and D involve using Textract along with SageMaker or Rekognition, respectively, for PHI identification. While these options could work, they introduce additional complexity by incorporating machine learning models and training.

upvoted 2 times

channn 11 months, 4 weeks ago

Key word: hospital!

upvoted 1 times

alexiscloud 12 months ago

Answer C:

upvoted 1 times

Chirantan 1 year, 3 months ago

Selected Answer: C

Amazon Textract is a machine learning (ML) service that automatically extracts text, handwriting, and data from scanned documents.

upvoted 3 times

career360guru 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

SONA_M_ 1 year, 3 months ago

WHY OPTION D IS WRONG

upvoted 1 times

s_fun 1 year, 2 months ago

D is wrong only because Amazon Rekognition doesn't read text, only explicit image contents.

upvoted 3 times

mj61 1 year, 2 months ago

B/C you use TextTract to extract text not Rekognition.

upvoted 1 times

✉️  **k1kavi1** 1 year, 3 months ago

Selected Answer: C

Agreed

upvoted 1 times

✉️  **Rameez1** 1 year, 3 months ago

C is correct

Textract- for extracting the text and Comprehend to identify the medical info

<https://aws.amazon.com/comprehend/medical/>

upvoted 3 times

✉️  **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

Question #66

Topic 1

A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted. Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days.

Which storage solution is MOST cost-effective?

- A. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Glacier 30 days from object creation. Delete the files 4 years after object creation.
- B. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days from object creation. Delete the files 4 years after object creation.
- C. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Delete the files 4 years after object creation.
- D. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Move the files to S3 Glacier 4 years after object creation.

Correct Answer: C*Community vote distribution*

Six_Fingered_Jose 1 year, 5 months ago

Selected Answer: C

i think C should be the answer here,
> Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce

If they do not explicitly mention that they are using Glacier Instant Retrieval, we should assume that Glacier -> takes more time to retrieve and may not meet the requirements

upvoted 79 times

JayBee65 1 year, 3 months ago

You can make that assumption, but I think it would be wrong to make it. It does not state they are not using Glacier Instant Retrieval, and it's use would be the logical choice in this question, so I'm going for A

upvoted 6 times

syh_rapha 1 year, 3 months ago

I think his assumption is correct because if you go to AWS documentation (<https://aws.amazon.com/s3/storage-classes/glacier/>) they clearly mention: "S3 Glacier Flexible Retrieval (formerly S3 Glacier)". So since this question doesn't specify the S3 Glacier class, then it would default to flexible retrieval (which ofc is not equal to Instant Retrieval).

upvoted 9 times

slackbot 7 months, 1 week ago

why everybody assumed files must be deleted after 4 years. they said files "can" be deleted, and not "must" be deleted. ideally store the files in glacier after 4 years

upvoted 3 times

wearrexdzw3123 5 months ago

Because it requires the lowest cost

upvoted 2 times

Kumaran1508 10 months ago

Yeah, Correct answer is C

Because even if you assume the glacier class as Instant Retrieval. As per the Instant Retrieval class the immediate availability is only once per quarter. But in question it is clearly mentioned that the files should be immediately available anytime.

upvoted 4 times

ninjawrz 1 year, 5 months ago

Selected Answer: A

Most COST EFFECTIVE

A: S3 Glacier Instant Retrieval is a new storage class that delivers the fastest access to archive storage, with the same low latency and high-throughput performance as the S3 Standard and S3 Standard-IA storage classes. You can save up to 68 percent on storage costs as compared with using the S3 Standard-IA storage class when you use the S3 Glacier Instant Retrieval storage class and pay a low price to retrieve data.

upvoted 25 times

wearrexdzw3123 5 months ago

Glaciers usually take some time to retrieve
upvoted 1 times

 **123jh10** 1 year, 5 months ago

I think A is the answer, too. As S3 Glacier has 3 different classes and one of them is able to retrieve objects in milliseconds (Instant Retrieval). As no class has been specified, we can assume the one that meets requirements is selected.

upvoted 6 times

 **GasGasJDM** 1 year, 5 months ago

I agree with this, since no specific information about Glacier modality, we can assume that Instant Retrieval is a possibility and as far as I know, this is cheaper than IA.

upvoted 1 times

 **RBSK** 1 year, 3 months ago

And we have a requirement (Most cost effective solution) hence A is the winner

upvoted 2 times

 **Pamban** 1 year, 4 months ago

"Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce" is the key sentence. answer is C.

upvoted 5 times

 **JayBee65** 1 year, 3 months ago

But S3 Glacier Instant Retrieval "is designed for rarely accessed data that still needs immediate access in performance-sensitive use cases", so it offers lower cost and instant retrieval, so A

upvoted 1 times

 **Bala75krish** 1 year, 1 month ago

I agree with your key sentence..but the one zone infrequent doesn't fit for critical business and it is used for recreate..

upvoted 1 times

 **wh1t4k3r** 1 year, 3 months ago

In the other hand, you need to chose a tier when going for glacier, so my previous comment is not stating well. The question is tricky, I change my mind: agree with you on this one

upvoted 2 times

 **bhushansathe** Most Recent 2 days, 8 hours ago

Selected Answer: C

C is the correct answer

upvoted 1 times

 **LIORAGE** 4 days, 11 hours ago

Selected Answer: C

C: is good option because immediate accessibility is required

upvoted 1 times

 **Hadi003** 6 days, 5 hours ago

Selected Answer: B

The question ask the MOST cost-effective solution

"S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA"

<https://aws.amazon.com/fr/s3/storage-classes/#:~:text=S3%20One%20Zone%2DIA%20is,less%20than%20S3%20Standard%2DIA>.

upvoted 1 times

 **48cd959** 1 week, 1 day ago

Selected Answer: C

Ans -C

It should be C, As Glacier always takes some time in retrieval until they say that they are using Glacier instant access retrieval service.

upvoted 1 times

 **doransignal** 2 weeks, 6 days ago

answer is c because glacier is not immediate thats why a is not the answer

upvoted 1 times

 **Ikki77** 1 month, 1 week ago

Selected Answer: C

Option C: Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Delete the files 4 years after object creation.

Options A, B, and D have drawbacks:

Option A: Transitioning to S3 Glacier might introduce retrieval times and costs, which may not be suitable for files that require immediate accessibility. Deleting directly after 4 years is a more straightforward approach.

Option B: S3 One Zone-Infrequent Access (S3 One Zone-IA) is less durable than Standard or Standard-Infrequent Access, as it stores data in a single availability zone. This may not be ideal for critical business data.

Option D: Transitioning to S3 Glacier after 4 years introduces retrieval times and costs, which might not align with the immediate accessibility requirement. It adds complexity without a clear benefit in this scenario.

upvoted 2 times

 **SMALLE** 1 month, 2 weeks ago

Selected Answer: A

For immediate access Glacier

[https://aws.amazon.com/pm/s3-glacier/?](https://aws.amazon.com/pm/s3-glacier/)

gclid=CjwKCAiAt5euBhB9EiwAdkXWO0uogf9S1lc6VBWw8fX7arlx3P_Le4skMgzg_4QX0V5NEuel9ZtS5hoCN5kQAvD_BwE&trk=c8974be7-bc21-436d-8108-

722e8ab912e1&sc_channel=ps&ef_id=CjwKCAiAt5euBhB9EiwAdkXWO0uogf9S1lc6VBWw8fX7arlx3P_Le4skMgzg_4QX0V5NEuel9ZtS5hoCN5kQAvD_BwE:G:s&s_kwcid=AL!4422!3!674509851564!e!!g!!s3%20glacier!19574556914!153569363253

upvoted 1 times

 **xelopelo** 2 months ago

Selected Answer: C

S3 glacier cannot provide immediate accessibility

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: C

A: S3 Glacier does not provide immediate accessibility

B: "contain critical business data" so one zone IA is not safe in case of zone failure

D: Does not delete the file, just moves them to Glacier

C: S3 for first 30 days, S3 Standard IA for 4 years then deleted. Meets all requirements

upvoted 2 times

 **vip2** 2 months, 2 weeks ago

Selected Answer: C

'Glacier instant' is usually used for query once/quater

upvoted 1 times

 **bujuman** 2 months, 3 weeks ago

Selected Answer: C

Recall: S3 Standard, S3 Standard-IA and S3 One Zone-IA are higher cost than Infrequent Access which include S3 Glacer-IR, S3 Glacier-FR, S3 Glacier-DA.

upvoted 1 times

 **bujuman** 2 months, 3 weeks ago

Erratum: Recall: S3 Standard, are higher cost than S3 Infrequent Access

upvoted 1 times

 **farnamjam** 2 months, 4 weeks ago

Selected Answer: C

C

Retrieving data from glacier takes more time than IA.

upvoted 1 times

 **pentium75** 3 months ago

Selected Answer: C

A - Glacier does not meet the "IMMEDIATE accessibility" requirement

B - "One Zone" does not meet the "access is ALWAYS required" requirement (zone can fail)

C - Correct

D - Files should be deleted, not moved to Glacier, after 4 years.

upvoted 1 times

 **SinghJagdeep** 3 months ago

Selected Answer: B

Please see detail answer from Buruguduystunstugudunstuy

upvoted 1 times

 **SaurabhTiwari1** 3 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

Question #67

Topic 1

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes to an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.

What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue.
- B. Use the AddPermission API call to add appropriate permissions.
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Correct Answer: D

Community vote distribution

D (100%)

✉️  **KVK16**  1 year, 5 months ago

Selected Answer: D

In case of SQS - multi-consumers if one consumer has already picked the message and is processing, in meantime other consumer can pick it up and process the message there by two copies are added at the end. To avoid this the message is made invisible from the time its picked and deleted after processing. This visibility timeout is increased according to max time taken to process the message

upvoted 42 times

✉️  **JayBee65** 1 year, 3 months ago

To add to this "The VisibilityTimeout in SQS is a time frame that the message can be hidden so that no others can consume it except the first consumer who calls the ReceiveMessageAPI." The API ChangeMessageVisibility changes this value.

upvoted 15 times

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

Selected Answer: D

To ensure that messages are being processed only once, a solutions architect should use the ChangeMessageVisibility API call to increase the visibility timeout which is Option D.

The visibility timeout determines the amount of time that a message received from an SQS queue is hidden from other consumers while the message is being processed. If the processing of a message takes longer than the visibility timeout, the message will become visible to other consumers and may be processed again. By increasing the visibility timeout, the solutions architect can ensure that the message is not made visible to other consumers until the processing is complete and the message can be safely deleted from the queue.

Option A (Use the CreateQueue API call to create a new queue) would not address the issue of duplicate message processing.

Option B (Use the AddPermission API call to add appropriate permissions) is not relevant to this issue.

Option C (Use the ReceiveMessage API call to set an appropriate wait time) is also not relevant to this issue.

upvoted 9 times

✉️  **karbob** 1 year, 2 months ago

not relevant to this issue. ??? what is added value

upvoted 3 times

✉️  **Buruguduystunstugudunstuy** 1 year ago

Option B (Use the AddPermission API call to add appropriate permissions) is not relevant to this issue because it deals with setting permissions for accessing an SQS queue, which is not related to preventing duplicate records in the RDS table.

Option C (Use the ReceiveMessage API call to set an appropriate wait time) is not relevant to this issue because it is related to configuring how long the ReceiveMessage API call should wait for new messages to arrive in the SQS queue before returning an empty response. It does not address the issue of duplicate records in the RDS table.

upvoted 5 times

✉️  **awsgeek75**  2 months, 1 week ago

Selected Answer: D

AB: Irrelevant

C: This is for long polling not for execution <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-short-and-long-polling.html#sqs-long-polling>

D: Visibility is correct fix issue because over here other SQS clients are seeing the same message back in the que when the previous processor is taking longer than expected to process the message

upvoted 1 times

 **Subhrangsu** 6 months ago

I also opt for D, but asking does increasing MessageVisibilityTimeOut good always?
upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

This parameter is the timeout after which the SQS assumes that the processing has failed and makes the item visible to other que processors. It is normal to increase the timeout if it takes longer to process items.
upvoted 1 times

 **miki111** 8 months, 1 week ago

Option D is the right answer.
upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: D

The visibility timeout is the duration during which SQS prevents other consumers from receiving and processing the same message. By increasing the visibility timeout, you allow more time for the processing of a message to complete before it becomes visible to other consumers.

Option A, creating a new queue, does not address the issue of concurrent processing and duplicate records. It would only create a new queue, which is not necessary for solving the problem.

Option B, adding permissions, also does not directly address the issue of duplicate records. Permissions are necessary for accessing the SQS queue but not for preventing concurrent processing.

Option C, setting an appropriate wait time using the ReceiveMessage API call, does not specifically prevent duplicate records. It can help manage the rate at which messages are received from the queue but does not address the issue of concurrent processing.

upvoted 4 times

 **cheese929** 11 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **alexiscloud** 12 months ago

Answer D:
visibility timeout begins when amazon SQS return a message
upvoted 1 times

 **test_devops_aws** 1 year ago

Selected Answer: D

D = ChangeMessageVisibility
upvoted 1 times

 **dev1978** 1 year, 2 months ago

In theory, between reception and changing visibility, you can have multiple consumers. Question is not good as it won't guarantee not executing twice.
upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: D

Increasing visibility timeout makes sure message is not visible for time taken to process the message.
upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D
upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

D is correct
upvoted 1 times

 **mabotega** 1 year, 4 months ago

Selected Answer: D

D is the correct choice, increasing the visibility timeout according to max time taken to process the message on the RDS.
upvoted 1 times

 **Valero_** 1 year, 5 months ago

Selected Answer: D

True, it's D.
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>
upvoted 6 times

Question #68

Topic 1

A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.

What should the solutions architect do to meet these requirements?

- A. Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails.
- B. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
- C. Provision an AWS Direct Connect connection to a Region. Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
- D. Provision an AWS Direct Connect connection to a Region. Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

Correct Answer: A

Community vote distribution

A (93%)

7%

≡  **KVK16**  1 year, 5 months ago

Selected Answer: A

Direct Connect + VPN best of both

upvoted 18 times

≡  **mabotega**  1 year, 4 months ago

Selected Answer: A

Direct Connect goes through 1 Gbps, 10 Gbps or 100 Gbps and the VPN goes up to 1.25 Gbps.

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html>
upvoted 13 times

≡  **48cd959**  1 week, 1 day ago

Selected Answer: A

Ans A-

Direct Connect because company needs consistent connection.

As a back up, company wants cheaper solution so VPN Site to Site connection should be okay.

upvoted 1 times

≡  **awsgeek75** 2 months, 1 week ago

Selected Answer: A

HA low latency + minimize cost + acceptable slow traffic if primary fails

B: VPN tunnel will be slow

C: 2 direct connect will be expensive

D: Backup connection for what?

A: Direct connect + VPN as a backup works

upvoted 4 times

≡  **Ruffyit** 5 months ago

A highly available connection with consistent low latency = AWS Direct Connect

Minimize costs and accept slower traffic if the primary connection fails = VPN connection

upvoted 4 times

≡  **benacert** 6 months, 3 weeks ago

A is the right choice to save cost

upvoted 1 times

≡  **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: A

Highly available connectivity using Direct Connect for consistent low latency and high throughput.

Cost optimization by using a VPN as a slower, lower cost backup for when Direct Connect fails.

Automatic failover to the VPN when Direct Connect fails.

upvoted 3 times

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

Selected Answer: A

A highly available connection with consistent low latency = AWS Direct Connect
Minimize costs and accept slower traffic if the primary connection fails = VPN connection
upvoted 1 times

✉️ **hsinchang** 8 months ago

Selected Answer: A

Slower traffic when primary fails, so the backup plan needs a cheaper solution, and the primary requires high performance, so A.
upvoted 1 times

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

Even though, there are a lots of variable affecting the cost of the connection, VPN connection is cheaper than the Direct Connect most of the time since VPN Connection doesn't require any dedicated physical circuit involved.

upvoted 1 times

✉️ **miki111** 8 months, 1 week ago

Option A is the right answer.
upvoted 1 times

✉️ **cookieMr** 9 months, 1 week ago

Selected Answer: A

Options B and C propose using multiple VPN connections for private connectivity and as backups. While VPNs can serve as backups, they may not provide the same level of consistent low latency and high availability as Direct Connect connections. Additionally, provisioning multiple VPN tunnels can increase operational complexity and costs.

Option D suggests using the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails. While this approach can be automated, it does not provide the same level of immediate failover capabilities as having a separate backup connection in place.

Therefore, option A, provisioning an AWS Direct Connect connection to a Region and provisioning a VPN connection as a backup, is the most suitable solution that meets the company's requirements for connectivity, cost-effectiveness, and high availability.

upvoted 4 times

✉️ **th3k33n** 11 months, 1 week ago

Selected Answer: A

highly available - > direct connect because connection can go up to 10GBPs and VPN 1.5GBPs as backup
upvoted 1 times

✉️ **linux_admin** 12 months ago

Selected Answer: A

Option A is the correct solution to meet the requirements of the company. Provisioning an AWS Direct Connect connection to a Region will provide a private and dedicated connection with consistent low latency. As the company requires a highly available connection, a VPN connection can be provisioned as a backup if the primary Direct Connect connection fails. This approach will minimize costs and provide the required level of availability.

upvoted 1 times

✉️ **devonwho** 1 year, 1 month ago

Selected Answer: A

With AWS Direct Connect + VPN, you can combine AWS Direct Connect dedicated network connections with the Amazon VPC VPN. This solution combines the benefits of the end-to-end secure IPSec connection with low latency and increased bandwidth of the AWS Direct Connect to provide a more consistent network experience than internet-based VPN connections.

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html>
upvoted 2 times

✉️ **dev1978** 1 year, 2 months ago

Why not B? Two VPNs on different connections? Direct Connect costs a fortune?
upvoted 2 times

✉️ **J3nkinz** 1 year, 2 months ago

The company requires a highly available connection with consistent low latency to an AWS Region, this is provided by Direct Connect as primary connection. The company allows a slower connection only for the backup option, so A is the right answer
upvoted 3 times

✉️ **thanhch** 1 year, 3 months ago

DX for low latency connect and the company accept slower traffic if the primary connection fails. So we should choose VPN for backup purpose. And the question also mark : minimize cost.

upvoted 1 times

Question #69

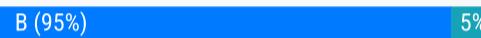
Topic 1

A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data. Which solution will meet these requirements with the LEAST operational effort?

- A. Place the EC2 instances in different AWS Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.
- B. Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.
- C. Configure the Auto Scaling group to use one Availability Zone. Generate hourly snapshots of the database. Recover the database from the snapshots in the event of a failure.
- D. Configure the Auto Scaling group to use multiple AWS Regions. Write the data from the application to Amazon S3. Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

Correct Answer: B

Community vote distribution



✉️ **SilentMilli** Highly Voted 1 year, 2 months ago

Selected Answer: B

By configuring the Auto Scaling group to use multiple Availability Zones, the application will be able to continue running even if one Availability Zone goes down. Configuring the database as Multi-AZ will also ensure that the database remains available in the event of a failure in one Availability Zone. Using an Amazon RDS Proxy instance for the database will allow the application to automatically route traffic to healthy database instances, further increasing the availability of the application. This solution will meet the requirements for high availability with minimal operational effort.

upvoted 20 times

✉️ **KVK16** Highly Voted 1 year, 5 months ago

Selected Answer: B

RDS Proxy for Aurora <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 8 times

✉️ **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: B

A: Different region doesn't help
 C: Would have made sense if it wasn't restricting to one AZ.
 D: Regions + S3 + Lambda = Operational effort extreme
 B: Although not entirely sure how RDS Proxy helps because it is for connection pooling but it is the only workable solution using multi AZ

upvoted 2 times

✉️ **dkw2342** 3 weeks, 5 days ago

One of the benefits of Amazon RDS Proxy is that it can improve application recovery time after database failovers. While RDS Proxy supports both MySQL as well as PostgreSQL engines, in this post, we will use a MySQL test workload to demonstrate how RDS Proxy reduces client recovery time after failover by up to 79% for Amazon Aurora MySQL and by up to 32% for Amazon RDS for MySQL.

-> contributes to minimum downtime req

upvoted 1 times

✉️ **dkw2342** 3 weeks, 5 days ago

PS: <https://aws.amazon.com/blogs/database/improving-application-availability-with-amazon-rds-proxy/>

upvoted 1 times

✉️ **MiniYang** 4 months ago

Selected Answer: A

The company wants to minimize costs and is willing to accept slower traffic if the primary connection fails, it may be tempted to choose a VPN connection as a backup, in which case the answer is A. Cost-Effectiveness: VPN connections are generally more economical than AWS Direct Connect, especially for low to moderate bandwidth needs.

Backup connection: A VPN connection can serve as a more cost-effective backup if the primary Direct Connect connection fails, even if it may be slower. Acceptance of slower traffic: The question clearly states that the company is willing to accept slower traffic if the primary connection fails, which implies a tolerance for connection speeds.

upvoted 1 times

✉️ **pentium75** 3 months ago

This is about the previous question ;)

upvoted 3 times

 **asulhi** 6 months, 1 week ago

Selected Answer: B

ASG and MultiAZ is the best answer

upvoted 1 times

 **benacert** 6 months, 3 weeks ago

B is the right answer

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: B

Option B requires the least operational effort to meet the high availability and minimum downtime/data loss requirements.

The key points are:

Use an Auto Scaling group across multiple AZs for high availability of the EC2 instances.

Configure the Aurora DB as Multi-AZ for high availability, automatic failover, and minimum data loss.

Use RDS Proxy for connection pooling to the DB for performance

upvoted 2 times

 **TariqKipkemei** 7 months, 2 weeks ago

Selected Answer: B

Highly available, Minimum downtime and Minimum loss of data = Auto Scaling group on Multi-AZ, Database on Multi-AZ, Amazon RDS Proxy.

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option B is the right answer.

upvoted 1 times

 **hiepdz98** 9 months ago

Selected Answer: B

B is correct answer

upvoted 2 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B

A. This approach provides geographic redundancy, it introduces additional complexity and operational effort, including managing replication, handling latency, and potentially higher data transfer costs.

C. While snapshots can be used for data backup and recovery, they do not provide real-time failover capabilities and can result in significant data loss if a failure occurs between snapshots.

D. While this approach offers some decoupling and scalability benefits, it adds complexity to the data flow and introduces additional overhead for data processing.

In comparison, option B provides a simpler and more streamlined solution by utilizing multiple AZs, Multi-AZ configuration for the database, and RDS Proxy for improved connection management. It ensures high availability, minimal downtime, and minimum loss of data with the least operational effort.

upvoted 6 times

 **Abrar2022** 10 months, 1 week ago

@Wajif the reason why it's not A is because the question mentions High availability and nothing to do with region. You can achieve HA without spanning multiple regions. Also B is incorrect because ALB are region specific and span across multiple AZ with that specific region (not cross region)

upvoted 1 times

 **UnluckyDucky** 1 year, 1 month ago

Selected Answer: B

RDS Proxy is fully managed by AWS for RDS/Aurora. It is auto-scaling and highly available by default.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: B

The correct solution is B: Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.

This solution will meet the requirements of high availability with minimum downtime and minimum loss of data with the least operational effort. By configuring the Auto Scaling group to use multiple Availability Zones, the web application will be able to withstand the failure of one Availability Zone without any disruption to the service. By configuring the database as Multi-AZ, the database will automatically failover to a standby instance in a different Availability Zone in the event of a failure, ensuring minimal downtime. Additionally, using an RDS Proxy instance will help to improve the performance and scalability of the database.

upvoted 3 times

✉  **k1kavi1** 1 year, 3 months ago

Selected Answer: B

Aurora PostgreSQL DB clusters don't support Aurora Replicas in different AWS Regions
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Replication.html>

upvoted 2 times

✉  **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

✉  **Shasha1** 1 year, 3 months ago

Answer is B

it will ensure that the database is highly available by replicating the data to a secondary instance in a different Availability Zone. In the event of a failure, the secondary instance will automatically take over and continue servicing database requests without any data loss. Additionally, configuring an Amazon RDS Proxy instance for the database will help improve the availability and scalability of the database

upvoted 4 times

Question #70

Topic 1

A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service. The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code. What should a solutions architect do to meet these requirements?

- A. Enable HTTP health checks on the NLB, supplying the URL of the company's application.
- B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.
- C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.
- D. Create an Amazon Cloud Watch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Correct Answer: C

Community vote distribution



✉️ **123jh10** 1 year, 5 months ago

Selected Answer: C

I would choose A, as NLB supports HTTP and HTTPS Health Checks, BUT you can't put any URL (as proposed), only the node IP addresses. So, the solution is C.

upvoted 27 times

✉️ **Ack3rman** 1 year, 4 months ago

can you elaborate more pls

upvoted 3 times

✉️ **BlueVolcano1** 1 year, 2 months ago

NLBs support HTTP, HTTPS and TCP health checks:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html> (check HealthCheckProtocol)

But NLBs only accept either selecting EC2 instances or IP addresses directly as targets. You can't provide a URL to your endpoints, only a health check path (if you're using HTTP or HTTPS health checks).

upvoted 9 times

✉️ **km142646** 11 months ago

What's the difference between endpoint URL and health check path?

upvoted 2 times

✉️ **majubmo** 9 months, 3 weeks ago

A URL includes the hostname. The health check path is only the path portion. For example,

URL = <https://i-0123456789abcdef.us-west-2.compute.internal/index.html>

health check path= /index.html

upvoted 11 times

✉️ **ArielSchivo** 1 year, 5 months ago

Selected Answer: C

Option C. NLB works at Layer 4 so it does not support HTTP/HTTPS. The replacement for the ALB is the best choice.

upvoted 17 times

✉️ **BlueVolcano1** 1 year, 2 months ago

That's incorrect. NLB does support HTTP and HTTPS (and TCP) health checks.

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

There just isn't an answer option that reflects that. My guess is that the question and/or answer options are outdated.

upvoted 4 times

✉️ **awsgeek75** 2 months, 1 week ago

Selected Answer: C

NLB is for network errors and low level traffic stuff

ALB is for application so C is the only realistic option here

upvoted 2 times

 **kel2023** 2 months, 3 weeks ago

Selected Answer: A

NLB does support HTTP/HTTPS Health Checks.

I saw other people comments, it seems like the question were rephrased. The comments were highlighting "application URL", but I don't see words on the question.

upvoted 1 times

 **ignajtpolandstrong** 2 months, 4 weeks ago

Selected Answer: C

You can use HTTP/HTTPS ONLY when Target is ALB.

By default it is TCP.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html#health-check-settings>

HealthCheckProtocol

The protocol the load balancer uses when performing health checks on targets. The possible protocols are HTTP, HTTPS, and TCP. The default is the TCP protocol. If the target type is ALB, the supported health check protocols are HTTP and HTTPS.

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: C

ALB allows you to specify the path which helps to check the error. NLB cannot do that.

upvoted 2 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

The key points are:

Use an Application Load Balancer (ALB) instead of a Network Load Balancer (NLB) since ALBs support HTTP health checks.

Configure HTTP health checks on the ALB to monitor the application health.

Use an Auto Scaling action triggered by the ALB health checks to automatically replace unhealthy instances.

upvoted 1 times

 **miki111** 8 months, 1 week ago

Option C is the right answer.

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

A. NLB, but NLB's health checks are designed for TCP/UDP protocols and lack the advanced features specific to HTTP applications provided by ALB.

B. This approach involves custom scripting and manual intervention, which contradicts the requirement of not writing custom scripts or code.

D. Since the NLB does not detect HTTP errors, relying solely on the UnhealthyHostCount metric may not accurately capture the health of the application instances.

Therefore, C is the recommended choice for improving the application's availability without custom scripting or code. By replacing the NLB with an ALB, enabling HTTP health checks, and configuring Auto Scaling to replace unhealthy instances, the company can ensure that only healthy instances are serving traffic, enhancing the application's availability automatically.

upvoted 6 times

 **Abrar2022** 10 months, 1 week ago

Replace the NLB (layer 4 udp and tcp) with an Application Load Balancer - ALB (layer 7) supports http and https requests.

upvoted 1 times

 **datz** 1 year ago

Selected Answer: C

must be C

Application availability: NLB cannot assure the availability of the application. This is because it bases its decisions solely on network and TCP-layer variables and has no awareness of the application at all. Generally, NLB determines availability based on the ability of a server to respond to ICMP ping or to correctly complete the three-way TCP handshake. ALB goes much deeper and is capable of determining availability based on not only a successful HTTP GET of a particular page but also the verification that the content is as was expected based on the input parameters.

upvoted 1 times

 **datz** 1 year ago

Also A doesn't offer what bellow in C offers...

Configure an Auto Scaling action to replace unhealthy instances

upvoted 1 times

 **Tony1980** 1 year, 1 month ago

Answer is C

A solution architect can use Amazon EC2 Auto Scaling health checks to automatically detect and replace unhealthy instances in the EC2 Auto Scaling group. The health checks can be configured to check the HTTP errors returned by the application and terminate the unhealthy instances. This will ensure that the application's availability is improved, without requiring custom scripts or code.

upvoted 1 times

 **aakashkumar1999** 1 year, 1 month ago

I will go with A as Network load balancer supports HTTP and HTTPS health checks, maybe the answer is outdated.

upvoted 2 times

 **pentium75** 3 months ago

But you'd need to check the health of the individual nodes, NOT "the URL of the company's application" which points to the Load Balancer.

upvoted 1 times

 **John_Zhuang** 1 year, 2 months ago

Selected Answer: C

<https://medium.com/awesome-cloud/aws-difference-between-application-load-balancer-and-network-load-balancer-cb8b6cd296a4>

As NLB does not support HTTP health checks, you can only use ALB to do so.

upvoted 1 times

 **BlueVolcano1** 1 year, 2 months ago

That's incorrect. NLB does support HTTP and HTTPS (and TCP) health checks.

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

Just a general tip: Medium is not a reliable resource. Anyone can create content there. Rely only on official AWS documentation.

upvoted 3 times

 **pentium75** 3 months ago

But you'd need to check the health of the individual nodes, NOT "the URL of the company's application" which points to the Load Balancer (as mentioned in A).

upvoted 1 times

 **benjl** 1 year, 2 months ago

Answer is C, and A is wrong because

In NLB, for HTTP or HTTPS health check requests, the host header contains the IP address of the load balancer node and the listener port, not the IP address of the target and the health check port.

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

upvoted 3 times

 **Silvestr** 1 year, 3 months ago

Selected Answer: C

Correct answer - C

Network load balancers (Layer 4) allow to:

- Forward TCP & UDP traffic to your instances
- Handle millions of request per seconds
- Less latency ~100 ms (vs 400 ms for ALB)

Best choice for HTTP traffic - replace to Application load balancer

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: A

The best option to meet the requirements is to enable HTTP health checks on the NLB by supplying the URL of the company's application. This will allow the NLB to automatically detect HTTP errors and take action, such as marking the target instance as unhealthy and routing traffic away from it.

Option A - Enable HTTP health checks on the NLB, supplying the URL of the company's application.

This is the correct solution as it allows the NLB to automatically detect HTTP errors and take action.

upvoted 5 times

 **Schladde** 11 months, 4 weeks ago

This won't increase availability when instances become unavailable.

upvoted 1 times

 **vipyodha** 9 months, 1 week ago

Option C right. A is not necessarily wrong, but it may not be the most effective solution to meet the requirements in this scenario. Here's why:

Option A suggests enabling HTTP health checks on the Network Load Balancer (NLB) by supplying the URL of the company's application. While this can help the NLB detect if the application is accessible or not, it does not directly address the specific requirement of automatically restarting the EC2 instances when HTTP errors occur.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option B - Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.

This option involves writing custom scripts or code, which is not allowed by the requirements. Additionally, this solution may not be reliable or efficient, as it relies on checking the logs locally on each instance and may not catch all errors.

Option C - Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.

While this option may improve the availability of the application, it is not necessary to replace the NLB with an Application Load Balancer in order to enable HTTP health checks. The NLB can support HTTP health checks as well, and replacing it may involve additional effort and cost.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option D - Create an Amazon CloudWatch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

This option involves monitoring the UnhealthyHostCount metric, which only reflects the number of unhealthy targets that the NLB is currently routing traffic away from. It does not directly monitor the health of the application or detect HTTP errors. Additionally, this solution may not be sufficient to detect and respond to HTTP errors in a timely manner.

upvoted 1 times

 **pentium75** 3 months ago

But A suggests to monitor health of "the URL of the company's application", which would point to the Load Balancer and return the health of a random node, not the one that is checked.

So you're checking Node 3 using the application URL, the Load Balancer directs your request to Node 2 which is unhealthy, thus the health check for Node 3 fails and Node 3 gets evicted.

upvoted 1 times

Question #71

Topic 1

A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour. What should the solutions architect recommend to meet these requirements?

- A. Configure DynamoDB global tables. For RPO recovery, point the application to a different AWS Region.
- B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.
- C. Export the DynamoDB data to Amazon S3 Glacier on a daily basis. For RPO recovery, import the data from S3 Glacier to DynamoDB.
- D. Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes. For RPO recovery, restore the DynamoDB table by using the EBS snapshot.

Correct Answer: B

Community vote distribution

B (100%)

✉  **123jh10**  1 year, 5 months ago

Selected Answer: B

A - DynamoDB global tables provides multi-Region, and multi-active database, but it not valid "in case of data corruption". In this case, you need a backup. This solutions isn't valid.

B - Point in Time Recovery is designed as a continuous backup juts to recover it fast. It covers perfectly the RPO, and probably the RTO.
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/PointInTimeRecovery.html>

C - A daily export will not cover the RPO of 15min.

D - DynamoDB is serverless... so what are these EBS snapshots taken from???

upvoted 40 times

✉  **LionelSid** 1 year, 1 month ago

Yes, it is possible to take EBS snapshots of a DynamoDB table. The process for doing this involves the following steps:

Create a new Amazon Elastic Block Store (EBS) volume from the DynamoDB table.

Stop the DynamoDB service on the instance.

Detach the EBS volume from the instance.

Create a snapshot of the EBS volume.

Reattach the EBS volume to the instance.

Start the DynamoDB service on the instance.

You can also use AWS Data pipeline to automate the above process and schedule regular snapshots of your DynamoDB table.

Note that, if your table is large and you want to take a snapshot of it, it could take a long time and consume a lot of bandwidth, so it's recommended to use the Global Tables feature from DynamoDB in order to have a Multi-region and Multi-master DynamoDB table, and you can snapshot each region separately.

upvoted 4 times

✉  **pavik** 11 months, 3 weeks ago

What is "DynamoDB service on the instance" ?

upvoted 2 times

✉  **pentium75** 3 months ago

DynamoDB is a native cloud service, there is no "instance" that you could "stop", or detach an "EBS volume" from.

upvoted 1 times

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

Selected Answer: B

The best solution to meet the RPO and RTO requirements would be to use DynamoDB point-in-time recovery (PITR). This feature allows you to restore your DynamoDB table to any point in time within the last 35 days, with a granularity of seconds. To recover data within a 15-minute RPO, you would simply restore the table to the desired point in time within the last 35 days.

To meet the RTO requirement of 1 hour, you can use the DynamoDB console, AWS CLI, or the AWS SDKs to enable PITR on your table. Once enabled, PITR continuously captures point-in-time copies of your table data in an S3 bucket. You can then use these point-in-time copies to restore your table to any point in time within the retention period.

CORRECT

Option B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.

upvoted 8 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

WRONG

Option A (configuring DynamoDB global tables) would not meet the RPO requirement, as global tables are designed to replicate data to multiple regions for high availability, but they do not provide a way to restore data to a specific point in time.

Option C (exporting data to S3 Glacier) would not meet the RPO or RTO requirements, as S3 Glacier is a cold storage service with a retrieval time of several hours.

Option D (scheduling EBS snapshots) would not meet the RPO requirement, as EBS snapshots are taken on a schedule, rather than continuously. Additionally, restoring a DynamoDB table from an EBS snapshot can take longer than 1 hour, so it would not meet the RTO requirement.

upvoted 6 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: B

A: Scalability across regions which is not required

C: Glacier exports and backup restore won't meet 1 hour RPO time

D EBS for DynamoDB table? Sounds impractical

B: DynamoDB point-in-time recovery is for this scenario.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/PointInTimeRecovery.html>

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: B

The best option to meet the RPO of 15 minutes and RTO of 1 hour is B) Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.

The key points:

DynamoDB point-in-time recovery can restore to any point in time within the last 35 days. This supports an RPO of 15 minutes.

Restoring from a point-in-time backup meets the 1 hour RTO.

Point-in-time recovery is specifically designed to restore DynamoDB tables with second-level granularity.

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

A. Global tables provide multi-region replication for disaster recovery purposes, they may not meet the desired RPO of 15 minutes without additional configuration and potential data loss.

C. Exporting and importing data on a daily basis does not align with the desired RPO of 15 minutes.

D. EBS snapshots can be used for data backup, they are not directly applicable to DynamoDB and cannot provide the desired RPO and RTO without custom implementation.

In comparison, option B utilizing DynamoDB's built-in point-in-time recovery functionality provides the most straightforward and effective solution for meeting the specified RPO of 15 minutes and RTO of 1 hour. By enabling PITR and restoring the table to the desired point in time, the company can recover the customer information with minimal data loss and within the required time frame.

upvoted 3 times

 **Abrar2022** 10 months, 1 week ago

The answer is in the question. Read the question again!!! Option B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.

upvoted 1 times

 **[Removed]** 11 months ago

If there is anyone who is willing to share his/her contributor access, then please write to vinaychethi99@gmail.com

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

 **Shasha1** 1 year, 3 months ago

B is correct

DynamoDB point-in-time recovery allows the solutions architect to recover the DynamoDB table to a specific point in time, which would meet the RPO of 15 minutes. This feature also provides an RTO of 1 hour, which is the desired recovery time objective for the application. Additionally, configuring DynamoDB point-in-time recovery does not require any additional infrastructure or operational effort, making it the best solution for this scenario.

Option D is not correct because scheduling Amazon EBS snapshots for the DynamoDB table every 15 minutes would not meet the RPO or RTO requirements. While EBS snapshots can be used to recover data from a DynamoDB table, they are not designed to provide real-time data protection or recovery capabilities

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

SimonPark 1 year, 4 months ago

Selected Answer: B

B is the answer
upvoted 1 times

BoboChow 1 year, 5 months ago

Selected Answer: B

I think DynamoDB global tables also work here, but Point in Time Recovery is a better choice
upvoted 1 times

Kikiokiki 1 year, 5 months ago

I THINK B.
<https://dynobase.dev/dynamodb-point-in-time-recovery/>
upvoted 1 times

priya2224 1 year, 5 months ago

answer is D
upvoted 1 times

123jhlo 1 year, 5 months ago

DynamoDB is serverless, so no storage snapshots available. <https://aws.amazon.com/dynamodb/>
upvoted 2 times

[Removed] 1 year, 5 months ago

bhk gandu chutiye glt ans btata hai
upvoted 1 times

Az900500 1 year, 4 months ago

Try communicate in English for audience
upvoted 4 times

Question #72

Topic 1

A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.

How can the solutions architect meet this requirement?

- A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through it.
- B. Deploy a NAT gateway into a public subnet and attach an endpoint policy that allows access to the S3 buckets.
- C. Deploy the application into a public subnet and allow it to route through an internet gateway to access the S3 buckets.
- D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

Correct Answer: D

Community vote distribution

D (100%)

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

Selected Answer: D

CORRECT

The correct answer is Option D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

By deploying an S3 VPC gateway endpoint, the application can access the S3 buckets over a private network connection within the VPC, eliminating the need for data transfer over the internet. This can help reduce data transfer fees as well as improve the performance of the application. The endpoint policy can be used to specify which S3 buckets the application has access to.

upvoted 34 times

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

WRONG

Option A, deploying Amazon API Gateway into a public subnet and adjusting the route table, would not address the issue of data transfer fees as the application would still be transferring data over the internet.

Option B, deploying a NAT gateway into a public subnet and attaching an endpoint policy, would not address the issue of data transfer fees either as the NAT gateway is used to enable outbound internet access for instances in a private subnet, rather than for connecting to S3.

Option C, deploying the application into a public subnet and allowing it to route through an internet gateway, would not reduce data transfer fees as the application would still be transferring data over the internet.

upvoted 11 times

✉  **KVK16**  1 year, 5 months ago

Selected Answer: D

To reduce costs get rid of NAT Gateway , VPC endpoint to S3

upvoted 23 times

✉  **awsgeek75**  2 months, 1 week ago

Selected Answer: D

S3 VPC Gateway is the cheapest solution as it does not use any billable traffic within same region

upvoted 1 times

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

Selected Answer: D

Prevent traffic from traversing the internet = Gateway VPC endpoint for S3.

upvoted 1 times

✉  **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: D

The best solution to reduce data transfer costs for an application frequently accessing S3 buckets in the same region is option D - Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

The key points:

- S3 gateway endpoints allow private connections between VPCs and S3 without going over the public internet.
- This avoids data transfer fees for traffic between the VPC and S3 within the same region.
- An endpoint policy controls access to specific S3 buckets.

upvoted 1 times

✉  **cookieMr** 9 months, 1 week ago

Selected Answer: D

A. API Gateway can serve as a proxy for S3 requests, it adds unnecessary complexity and additional costs compared to a direct VPC endpoint.

B. Using a NAT gateway for accessing S3 introduces unnecessary data transfer costs as traffic would still flow over the internet.

C. This approach would incur data transfer fees as the traffic would go through the public internet.

In comparison, option D using an S3 VPC gateway endpoint provides a direct and cost-effective solution for accessing S3 buckets within the same Region. By keeping the data transfer within the AWS network infrastructure, it helps reduce data transfer fees and provides secure access to the S3 resources.

upvoted 2 times

✉ **Bmarodi** 9 months, 3 weeks ago

Selected Answer: D

Option D is correct answer.

upvoted 1 times

✉ **Erbug** 1 year, 1 month ago

To answer this question, I need to know the comparison of the types of gateway of costs, please give me a tip about that issue.

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

✉ **9014** 1 year, 3 months ago

Selected Answer: D

The answer is D:- Actually, the Application (EC2) is running in the same region...instead of going to the internet, data can be copied through the VPC endpoint...so there will be no cost because data is not leaving the AWS infra

upvoted 1 times

✉ **JayBee65** 1 year, 3 months ago

Can somebody please explain this question? Are we assuming the application is running in AWS and that adding the gateway endpoint avoids the need for the EC2 instance to access the internet and thus avoid costs? Thanks a lot.

upvoted 2 times

✉ **SR0611** 1 year, 3 months ago

Yes correct

upvoted 1 times

✉ **Wpcorgan** 1 year, 4 months ago

D is correct

upvoted 1 times

✉ **yd_h** 1 year, 5 months ago

Selected Answer: D

FYI :

-There is no additional charge for using gateway endpoints.

-Interface endpoints are priced at ~ \$0.01/per AZ/per hour. Cost depends on the Region

- S3 Interface Endpoints resolve to private VPC IP addresses and are routable from outside the VPC (e.g via VPN, Direct Connect, Transit Gateway, etc). S3 Gateway Endpoints use public IP ranges and are only routable from resources within the VPC.

upvoted 5 times

✉ **123jhlo** 1 year, 5 months ago

Selected Answer: D

Close question to the Question #4, with same solution.

upvoted 3 times

Question #73

Topic 1

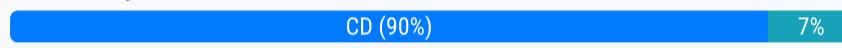
A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.

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

- A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
- B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
- C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
- D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
- E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

Correct Answer: CD

Community vote distribution



Six_Fingered_Jose Highly Voted 1 year, 5 months ago

Selected Answer: CD

C because from on-prem network to bastion through internet (using on-prem resource's public IP),
D because bastion and ec2 is in same VPC, meaning bastion can communicate to EC2 via its private IP address
upvoted 37 times

awsgeek75 Most Recent 2 months, 1 week ago

Selected Answer: CD

C: Bastion in public subnet should only allow access from public IP of the company
D: app instance in private subnet should only allow access from bastion

ABD are wrong choices

Here is a working example on AWS docs if you want to learn about Bastion setup
<https://aws.amazon.com/solutions/implementations/linux-bastion/>

upvoted 1 times

awsgeek75 2 months, 1 week ago

Good way to remember this one is to think of movie scene where someone is visiting a prisoner in a prison and talks to them from behind a glass using a 2 way phone.

Visitor is in company
Visitor area is public subnet
Prisoner area is private subnet
Phone is bastion

Visitor (company) must only be allowed to use the phone (bastion) from the public area (public subnet) and the phone (bastion) must only be allowed to talk to the prisoner in the prisoner area (private subnet)

upvoted 11 times

Marco_St 4 months, 1 week ago

Selected Answer: BD

the question mentioned from on-prem network to bastion through the company's internet then it should use the internal IP range not external ip ranges. so BD
upvoted 2 times

awsgeek75 2 months, 1 week ago

How would you know the internal IP range of the company? B is wrong.
upvoted 1 times

ATInnovandoJuntos 4 months, 1 week ago

https://en.wikipedia.org/wiki/Network_address_translation
That's the reason is C and not B
upvoted 2 times

✉️ **virus** 3 months, 1 week ago

Company's internet is internet - unless its company's intranet
upvoted 2 times

✉️ **slimen** 4 months, 3 weeks ago

Selected Answer: CD

on-prem ----> bastion host (we use internet, means that we need external IPs of the company)
bastion host ----> private subnet (we use private IP since we are in the same AWS network)
upvoted 4 times

✉️ **wearrexdzw3123** 5 months ago

Why are there always such unclear questions?
upvoted 3 times

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

Selected Answer: CD

Key: through the company's internet connection
upvoted 2 times

✉️ **prabhjot** 5 months, 3 weeks ago

Option B - inbound access from the internal IP range for the company. This step ensures that only internal IP addresses from your company's network can access the bastion host, enhancing security and then Option D
upvoted 1 times

✉️ **Subhrangsu** 6 months ago

Please check first comments from top of them:
Help2023
Whericanlstart
Buruguduystunstugudunstuy
upvoted 1 times

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

Selected Answer: CD

Allows inbound access from the external IP range for the company. Then allow inbound SSH access from only the private IP address of the bastion host.
upvoted 1 times

✉️ **cookieMr** 9 months, 1 week ago

Selected Answer: CD

C. This will restrict access to the bastion host from the specific IP range of the on-premises network, ensuring secure connectivity. This step ensures that only authorized users from the on-premises network can access the bastion host.

D. This step enables SSH connectivity from the bastion host to the application instances in the private subnet. By allowing inbound SSH access only from the private IP address of the bastion host, you ensure that SSH access is restricted to the bastion host only.

upvoted 2 times

✉️ **stanleyjade** 10 months, 4 weeks ago

the internal and external IP range is not clear
upvoted 4 times

✉️ **PLN6302** 7 months ago

yes same for me
upvoted 1 times

✉️ **pentium75** 3 months ago

The admin is supposed to use "the company's Internet connection", NOT a VPN tunnel or DirectConnect. Thus the connection originates from the company's public/external IP.
upvoted 1 times

✉️ **km142646** 11 months ago

The private/public IP address thing is confusing. Ideally, the private instances inbound rule would just allow traffic from the security group of the bastion host.
upvoted 2 times

✉️ **Spiffaz** 1 year ago

Why external and not internal?
upvoted 2 times

✉️ **TariqKipkemei** 1 year ago

Because the traffic goes through the public internet. In the public internet, public IP(external IP) is used.
upvoted 6 times

✉️ **Help2023** 1 year, 1 month ago

Selected Answer: CE

Application is in private subnet
Bastion Host is in public subnet

D does not make sense because the bastion host is in public subnet and they don't have a private IP but only a public IP address attached to them. The IP wanting to connect is Public as well.

Bastion host in public subnet allows external IP (via internet) of the company to access it. Which then leaves us to give permission to the application private subnet and for that the private subnet with the application accepts the IP coming from Bastion Host by changing its SG. C&E upvoted 2 times

 **Whericanstart** 1 year ago

Bastion host in public subnet because it has a public IP and a NAT Gateway that can route traffic out of your AWS VPC but it does have the ability to access the private subnet using private IP since it's not leaving AWS to access the private subnet. So C&D are the right answers.

upvoted 3 times

 **sidharthwader** 3 weeks, 5 days ago

You are right E is also fine but its not a best thing to do Using private IP is always better than using public IP unless the situation demands the use of Public IP.

upvoted 1 times

 **swolfgang** 1 year, 2 months ago

I dont understand why not CE . Because question ask through internet connection to servers and boston host.I understand they want to access both of from public. I mean not from the servers to bastion host.

upvoted 2 times

 **RupeC** 8 months, 1 week ago

E doesn't seem right to me as this is not a layered approach. i.e. on prem to public subnet, 1st then 2nd bastion to application. That layering is missed in option E.

upvoted 1 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: CD

<https://www.examtopics.com/discussions/amazon/view/51356-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: CE

To meet the requirements, the solutions architect should take the following steps:

C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company. This will allow the solutions architect to connect to the bastion host from the company's on-premises network through the internet connection.

E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host. This will allow the solutions architect to connect to the application instances through the bastion host using SSH.

Note: It's important to ensure that the security groups for the bastion host and application instances are configured correctly to allow the desired inbound traffic, while still protecting the instances from unwanted access.

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

WRONG

Here is why the other options are not correct:

A. Replacing the current security group of the bastion host with one that only allows inbound access from the application instances would not allow the solutions architect to connect to the bastion host from the company's on-premises network through the internet connection. The bastion host needs to be accessible from the external network in order to allow the solutions architect to connect to it.

B. Replacing the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company would not allow the solutions architect to connect to the bastion host from the company's on-premises network through the internet connection. The internal IP range is not accessible from the external network.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

D. Replacing the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host would not allow the solutions architect to connect to the application instances through the bastion host using SSH. The private IP address of the bastion host is not accessible from the external network, so the solutions architect would not be able to connect to it from the on-premises network.

upvoted 1 times

 **pentium75** 3 months ago

Huh? The administrator can access the bastion host through his company's Internet connection through the Bastion host's public IP. Then he can connect from the Bastion host to the application servers. The Bastion host's network interface has a private IP, it's just mapped to a public IP by the IGW, but ofc it can use its private IP for communication within the VPN.

upvoted 1 times

Question #74

Topic 1

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.

How should security groups be configured in this situation? (Choose two.)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Correct Answer: AC

Community vote distribution

AC (98%)

✉️  **Athena**  1 year, 4 months ago

Selected Answer: AC

Web Server Rules: Inbound traffic from 443 (HTTPS) Source 0.0.0.0/0 - Allows inbound HTTPS access from any IPv4 address
Database Rules : 1433 (MS SQL)The default port to access a Microsoft SQL Server database, for example, on an Amazon RDS instance

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html>
upvoted 23 times

✉️  **ArielSchivo**  1 year, 5 months ago

Selected Answer: AC

EC2 web on public subnets + EC2 SQL on private subnet + security is high priority. So, Option A to allow HTTPS from everywhere. Plus option C to allow SQL connection from the web instance.
upvoted 17 times

✉️  **awsgeek75**  2 months, 1 week ago

Selected Answer: AC

SG are blocked by default and stateful so
A: Allows inbound traffic from web to the HTTPS default port on web servers
B: Outbound is not required if inbound is configured due to stateful nature of SG
C: 1433 is SQL default so allow access from web-tier only
D: Opens up the database to web on 1433 port
E: opens up 443 port unnecessarily on the DB tier so less secure
AC is the most secure config
upvoted 2 times

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

Selected Answer: AC

Allow inbound traffic on port 443 from 0.0.0.0/0 on the web tier. Then allow inbound traffic on port 1433 from the security group for the web tier on the database tier.
upvoted 1 times

✉️  **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: AC

The security group for the web tier should allow inbound traffic on port 443 from 0.0.0.0/0. This will allow clients to connect to the web tier using HTTPS. The security group for the web tier should also allow outbound traffic on port 443 to 0.0.0.0/0. This will allow the web tier to connect to the internet to download updates and other resources.

The security group for the database tier should allow inbound traffic on port 1433 from the security group for the web tier. This will allow the web tier to connect to the database tier to access data. The security group for the database tier should not allow outbound traffic on ports 443 and 1433 to the security group for the web tier. This will prevent the database tier from being exposed to the public internet.
upvoted 2 times

✉️  **cookieMr** 9 months, 1 week ago

Selected Answer: AC

A. This configuration allows external users to access the web tier over HTTPS (port 443). However, it's important to note that it is generally recommended to restrict the source IP range to a more specific range rather than allowing access from 0.0.0.0/0 (anywhere). This would limit access to only trusted sources.

C. By allowing inbound traffic on port 1433 (default port for Microsoft SQL Server) from the security group associated with the web tier, you ensure that the database tier can only be accessed by the EC2 instances in the web tier. This provides a level of isolation and restricts direct access to the database tier from external sources.

upvoted 2 times

 **Abrar2022** 10 months, 1 week ago

DB tier: Port 1433 is the known standard for SQL server and should be used.

web tier on port 443 (HTTPS)

upvoted 3 times

 **beginnercloud** 10 months, 1 week ago

Selected Answer: AC

AC is correct

upvoted 1 times

 **Wheretocanstart** 1 year ago

A & C are the correct answer.

Inbound traffic to the web tier on port 443 (HTTPS)

The web tier will then access the Database tier on port 1433 - inbound.

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: AC

AC 443-HTTP inbound and 1433-SQL Server

Security group => focus on inbound traffic since by default outbound traffic is allowed

upvoted 2 times

 **aba2s** 1 year, 2 months ago

Selected Answer: AC

Security group => focus on inbound traffic since by default outbound traffic is allowed

upvoted 2 times

 **orionizzie** 1 year, 3 months ago

why both are inbound rules

upvoted 1 times

 **kraken21** 12 months ago

Because security groups are stateful.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: CE

CORRECT

The correct answers are C and E.

For security purposes, it is best practice to limit inbound and outbound traffic as much as possible. In this case, the web tier should only be able to access the database tier and not the other way around. Therefore, the security group for the web tier should only allow outbound traffic to the security group for the database tier on the necessary ports. Similarly, the security group for the database tier should only allow inbound traffic from the security group for the web tier on the necessary ports.

Answer C: Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier. This is correct because the web tier needs to be able to connect to the database on port 1433 in order to access the data.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Answer E: Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier. This is correct because the web tier needs to be able to connect to the database on both port 443 and 1433 in order to access the data.

WRONG

Answer A: Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0. This is not correct because the web tier should not allow inbound traffic from the internet. Instead, it should only allow outbound traffic to the security group for the database tier.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

WRONG

Answer B: Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0. This is not correct because the web tier should not allow outbound traffic to the internet. Instead, it should only allow outbound traffic to the security group for the database tier.

Answer D: Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier. This is not correct because the database tier should not allow outbound traffic to the web tier. Instead, it should only allow inbound traffic from the security group for the web tier on the necessary ports.

upvoted 1 times

 **techhb** 1 year, 2 months ago

Chatgpt is unreliable this answer from same.

upvoted 1 times

 **pentium75** 3 months ago

"The web tier needs to be able to connect to the database on both port 443 and 1433 in order to access the data" -> Nonsense, SQL Server needs only tcp/1433. Or tcp/1433 + udp/1433 plus the instance port if you have multiple instances. But you NEVER need tcp/443 to access SQL Server.

upvoted 1 times

 **PassNow1234** 1 year, 3 months ago

This is WRONG. Browse to a website and type :443 at the end of it. IT will translate to HTTPS. HTTPS = 443.

answers are A and C

upvoted 3 times

 **career360guru** 1 year, 3 months ago

Selected Answer: AC

A and C

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

A and C

upvoted 1 times

 **gcmrjbr** 1 year, 5 months ago

Agree with AC.

upvoted 2 times

 **srshekhar** 1 year, 5 months ago

Very good questions

upvoted 3 times

Question #75

Topic 1

A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application. Which solution meets these requirements and is the MOST operationally efficient?

- A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
- B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the servers' peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
- C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Correct Answer: A*Community vote distribution*

gcmrjbr Highly Voted 1 year, 5 months ago

Agree with A>>> Lambda = serverless + autoscale (modernize), SQS= decouple (no more drops)
upvoted 37 times

LuckyAro Highly Voted 1 year, 1 month ago

Selected Answer: A

The catch phrase is "scale up when communication failures are detected" Scaling should not be based on communication failures, that'll be crying over spilled milk ! or rather too late. So D is wrong.
upvoted 17 times

mauroicardi 1 week, 5 days ago

Spot on

upvoted 1 times

remand 1 year, 1 month ago

it says "one tier becomes overloaded" , Not communication failure...

upvoted 2 times

LuckyAro 1 year, 1 month ago

D says: "Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected".

upvoted 4 times

SMALLE Most Recent 1 month, 2 weeks ago

RESTful services = API Gateways

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

upvoted 1 times

awsgeek75 2 months, 1 week ago

Selected Answer: A

Least operational overhead = API Gateway + Lambda + SQS

BC wrong applications

D: Will work but more operational overhead than A with less resilience to failures

upvoted 1 times

pentium75 3 months ago

Selected Answer: A

You want to "modernize the application", that a modern application is serverless, in any case a modern application does NOT use EC2 instances. Also, managing EC2 instances (with the OS etc pp) is NOT "operationally efficient". Thus not D.
upvoted 1 times

anikolov 3 months ago

Selected Answer: C

For me the solution could be based on using SNS with multiple topics to organize communication between different tiers (Using Subscriber for one and Producer for another topic to proceed with transactions over multi-tiers). CloudWatch to monitor SNS topics queue length and scale

up/down based on counts of messages (NumberOfMessagesPublished)

upvoted 1 times

 **pentium75** 3 months ago

Wouldn't the scaling take some time? If there is queue length, then one tier IS already overloaded.

upvoted 2 times

 **MrPCarrot** 4 months, 1 week ago

A is the perfect answer no need for the ASG

upvoted 1 times

 **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: D

D is better because in answer A there is a bottleneck on a SQS - service app,

D is as operationally efficient as A and solves the above issue

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: A

ASG is not as efficient as Lambda!

upvoted 1 times

 **vijaykamal** 6 months ago

I feel the answer is D, Lambda would increase the complexity and overhead and it has limitation of running for 15 min.

upvoted 4 times

 **pentium75** 3 months ago

How would Lambda increase the operational (!) complexity over handling and scaling servers (and their operating systems and patches etc.) on EC2?

upvoted 1 times

 **TariqKipkemei** 7 months, 1 week ago

Selected Answer: A

MOST operationally efficient = Serverless = AWS Lambda functions, Amazon Simple Queue Service

upvoted 1 times

 **zjcorpuz** 8 months ago

A and D are both good solution however A will suffice the requirement as it is the most operational efficient for modern applications, AWS Lambda will scale elastically when application will become overloaded and the fact that it is serverless. SQS will handle the queue as well..

upvoted 2 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: D

This solution addresses the issue of dropped transactions by decoupling the communication between application tiers using SQS. It ensures that transactions are not lost even if one tier becomes overloaded.

By using EC2 in ASG, the application can automatically scale based on the demand and the length of the SQS. This allows for efficient utilization of resources and ensures that the application can handle increased workload and communication failures.

CloudWatch is used to monitor the length of SQS. When queue length exceeds a certain threshold, indicating potential communication failures, the ASG can be configured to scale up by adding more instances to handle the load.

D. This solution utilizes Lambda and API Gateway, which can be a valid approach for building serverless applications. However, it may introduce additional complexity and operational overhead compared to the requirement of modernizing an existing multi-tiered application.

upvoted 4 times

 **MutiverseAgent** 8 months, 3 weeks ago

Supposing the solution is D), what is the point of monitoring the SQS queue length if then the system scales up when communication failures are detected? Why not monitoring the amount of failures? Is it ok to assume that when the queue grows the system is failing? What is the system is under more demand? So, my guess, the solution is A)

upvoted 1 times

 **prakashiyyanarappan** 11 months ago

ANS: A Key word - RESTful services - Amazon API Gateway

upvoted 6 times

 **ajaynaik44** 11 months, 3 weeks ago

Must be D :

Please refer to thread <https://pupuweb.com/aws-saa-c02-actual-exam-question-answer-dumps-3/6/>

upvoted 2 times

 **hemantjv** 11 months, 3 weeks ago

@Buruguduystunstugudunstuy Kindly share your comments for this question

upvoted 1 times

 **remand** 1 year, 1 month ago

Selected Answer: D

Must be D.

A is incorrect. Even though lambda could auto scale, SQS communication between tiers is not addressing drop in transaction per se as SQS would allow to read (say serially with FIFO or NOT) in a controlled way, your application code determines how many threads are being spanned to process those messages. This could still overload the tier.

upvoted 5 times

 **pentium75** 3 months ago

If you "modernize the application" to a serverless one, then you invoke a Lambda function on each API call. It's not like a server where "your application code determines how many threads are being spanned".

upvoted 1 times

Question #76

Topic 1

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive.

Which solution offers the MOST reliable data transfer?

- A. AWS DataSync over public internet
- B. AWS DataSync over AWS Direct Connect
- C. AWS Database Migration Service (AWS DMS) over public internet
- D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Correct Answer: B

Community vote distribution


 B (100%)

✉  **ArielSchivo**  1 year, 5 months ago

Selected Answer: B

DMS is for databases and here refers to "JSON files". Public internet is not reliable. So best option is B.
upvoted 31 times

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

Selected Answer: B

CORRECT
The most reliable solution for transferring the data in a secure manner would be option B: AWS DataSync over AWS Direct Connect.

AWS DataSync is a data transfer service that uses network optimization techniques to transfer data efficiently and securely between on-premises storage systems and Amazon S3 or other storage targets. When used over AWS Direct Connect, DataSync can provide a dedicated and secure network connection between your on-premises data center and AWS. This can help to ensure a more reliable and secure data transfer compared to using the public internet.

upvoted 14 times

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

WRONG

Option A, AWS DataSync over the public internet, is not as reliable as using Direct Connect, as it can be subject to potential network issues or congestion.

Option C, AWS Database Migration Service (DMS) over the public internet, is not a suitable solution for transferring large amounts of data, as it is designed for migrating databases rather than transferring large amounts of data from a storage area network (SAN).

Option D, AWS DMS over AWS Direct Connect, is also not a suitable solution, as it is designed for migrating databases and may not be efficient for transferring large amounts of data from a SAN.

upvoted 12 times

✉  **doorahmie** 1 year, 1 month ago

explanation about D option is good

upvoted 1 times

✉  **awsgeek75**  2 months, 1 week ago

Selected Answer: B

near-real-time + large data + secure = DataSync over DirectConnect

A: Less secure due to public internet

C: Slow and not secure

D: Slow even if more secure

DC may not even work as we don't know if there is a DB on other side but even if it was there, it is less preferred way

upvoted 1 times

✉  **JTruong** 2 months, 3 weeks ago

Any DMS related-service will not be efficient because DMS can only process JSON files UPTO 2 MB in size

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Tasks.CustomizingTasks.TableMapping.SelectionTransformation.html

so B is CORRECT

upvoted 1 times

✉  **Ruffyit** 4 months, 4 weeks ago

AWS DataSync is a data transfer service that uses network optimization techniques to transfer data efficiently and securely between on-premises storage systems and Amazon S3 or other storage targets. When used over AWS Direct Connect, DataSync can provide a dedicated and secure

network connection between your on-premises data center and AWS. This can help to ensure a more reliable and secure data transfer compared to using the public internet.

upvoted 2 times

 **TariqKipkemei** 7 months, 1 week ago

Selected Answer: B

Secure and Most reliable transfer = AWS DataSync over AWS Direct Connect

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: B

AWS DataSync is designed for large scale, high speed data transfer between on-prem and S3.

Using AWS Direct Connect provides a dedicated, private connection for reliable, consistent data transfer.

DataSync seamlessly handles data replication, encryption, recovery etc.

upvoted 1 times

 **MNotABot** 8 months, 2 weeks ago

Not over public hence AC out / DMS is for databases and here refers to "JSON files".

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B

DataSync is a service specifically designed for data transfer and synchronization between on-premises storage systems and AWS storage services like S3. It provides reliable and efficient data transfer capabilities, ensuring the secure movement of large volumes of data.

By leveraging Direct Connect, which establishes a dedicated network connection between the on-premises data center and AWS, the data transfer is conducted over a private and dedicated network link. This approach offers increased reliability, lower latency, and consistent network performance compared to transferring data over the public internet.

Database Migration Service is primarily focused on database migration and replication, and it may not be the most appropriate tool for general-purpose data transfer like JSON files.

Transferring data over the public internet may introduce potential security risks and performance variability due to factors like network congestion, latency, and potential interruptions.

upvoted 2 times

 **beginnercloud** 10 months, 1 week ago

Best option and correct is B

upvoted 1 times

 **Abrar2022** 10 months, 1 week ago

Selected Answer: B

as Ariel suggested and rightly so....DMS is for databases and here refers to "JSON files". Public internet is not reliable. so B

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B. DMS is not needed as there is no Database migration requirement.

upvoted 1 times

 **Wajif** 1 year, 3 months ago

Selected Answer: B

Public internet options automatically out being best-effort. DMS is for database migration service and here they have to just transfer the data to S3. Hence B.

upvoted 2 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **yd_h** 1 year, 5 months ago

B

- A SAN presents storage devices to a host such that the storage appears to be locally attached. (NFS is, or can be, a SAN - <https://serverfault.com/questions/499185/is-san-storage-better-than-nfs>)

- AWS Direct Connect does not encrypt your traffic that is in transit by default. But the connection is private (<https://docs.aws.amazon.com/directconnect/latest/UserGuide/encryption-in-transit.html>)

upvoted 4 times

Question #77

Topic 1

A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data.

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

- A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
- B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.
- C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
- D. Configure an Amazon API Gateway API to send data to AWS Glue. Use AWS Lambda functions to transform the data. Use AWS Glue to send the data to Amazon S3.

Correct Answer: C*Community vote distribution*

123jh10 Highly Voted 1 year, 5 months ago

Selected Answer: C

(A) - You don't need to deploy an EC2 instance to host an API - Operational overhead
 (B) - Same as A
 (**C**) - Is the answer
 (D) - AWS Glue gets data from S3, not from API GW. AWS Glue could do ETL by itself, so don't need lambda. Non sense.
<https://aws.amazon.com/glue/>

upvoted 41 times

Futurebones 10 months, 2 weeks ago

I don't understand is why we should use Lambda in between to transform data. To me, Kinesis data firehose is enough as it is an extract, transform, and load (ETL) service.

upvoted 5 times

Remy_d 5 months, 3 weeks ago

It is because they assume that Kinesis Data Firehose built-in transformations are not enough. So you have to use specific lambda transformation. Please refer to this link : <https://aws.amazon.com/kinesis/data-firehose/#:~:text=Amazon%20Kinesis%20Data%20Firehose%20is,data%20stores%2C%20and%20analytics%20services.>

upvoted 5 times

TariqKipkemei Highly Voted 7 months, 1 week ago

Selected Answer: C

The company needs an API = Amazon API Gateway API
 A real-time data ingestion = Amazon Kinesis data stream
 A process that transforms data = AWS Lambda functions
 Kinesis Data Firehose delivery stream to send the data to Amazon S3
 A storage solution for the data = Amazon S3

upvoted 17 times

awsgeek75 Most Recent 2 months, 1 week ago

Selected Answer: C

C is least operational overhead

- A: EC2 is overhead in this scenario
- B: Same as A
- D: Glue is not real time data streaming

upvoted 2 times

Mikado211 3 months, 3 weeks ago

Selected Answer: C

It looks overengineered, but as it works, let's go for the C

upvoted 3 times

Ruffyit 4 months, 4 weeks ago

The company needs an API = Amazon API Gateway API
 A real-time data ingestion = Amazon Kinesis data stream
 A process that transforms data = AWS Lambda functions
 Kinesis Data Firehose delivery stream to send the data to Amazon S3
 A storage solution for the data = Amazon S3
 upvoted 2 times

 **peekingpicker** 5 months, 2 weeks ago

Selected Answer: D

"a real-time data ingestion"
 isn't firehose not realtime ? Kinesis FireHose is "Near" Real-time . It has 60 seconds gap. I think it should be D
 upvoted 1 times

 **rlamberti** 5 months, 1 week ago

The real-time part (data ingestion) will be performed by Kinesis Data Stream and API Gateway. After this, the transformation and storage of the data don't need to be in real-time, since it was already ingested, so Kinesis Firehose + Lambda is perfect. C makes sense to me.
 upvoted 4 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

Option C provides the least operational overhead to meet the requirements:

API Gateway provides the API
 Kinesis Data Streams ingests the real-time data
 Lambda functions transform the data
 Firehose delivers the data to S3 storage
 The key advantages are:

Serverless architecture requires minimal operational overhead
 Fully managed ingestion, processing and storage services
 No need to manage EC2 instances
 upvoted 2 times

 **diabloexodia** 8 months, 2 weeks ago

Requirements:
 API- API gateway
 Real time data ingestion - AWS Kinesis data stream
 ETL(Extract Transform Load) - Kinesis Firehose
 Storage- S3
 upvoted 3 times

 **tamefi5512** 8 months, 4 weeks ago

Selected Answer: C

C - is the answer
 upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

C. By leveraging these services together, you can achieve a real-time data ingestion architecture with minimal operational overhead. The data flows from the API Gateway to the Kinesis data stream, undergoes transformations with Lambda, and is then sent to S3 via the Kinesis Data Firehose delivery stream for storage.

- A. This adds operational overhead as you need to handle EC2 management, scaling, and maintenance. It is less efficient compared to using a serverless solution like API Gateway.
 - B. It requires deploying and managing an EC2 to host the API and configuring Glue. This adds operational overhead, including EC2 management and potential scalability limitations.
 - D. It still requires managing and configuring Glue, which adds operational overhead. Additionally, it may not be the most efficient solution as Glue is primarily used for ETL scenarios, and in this case, real-time data transformation is required.
- upvoted 2 times

 **winzzhhzzhh** 10 months, 1 week ago

Selected Answer: D

I am gonna choose D for this.
 Kinesis Data Stream + Data Firehose will adds up to the operational overhead, plus it is "Near real-time", not a real time solution.
 Lambda functions scale automatically, so no management of scaling/compute resources is needed.
 AWS Glue handles the data storage in S3, so no management of that is needed.

upvoted 2 times

 **UnluckyDucky** 1 year ago

Gotta love all those chatgpt answers y'all are throwing at us.

Kinesis Firehose is NEAR real-time, not real-time like your bots tell you.
 upvoted 2 times

👤 **pentium75** 3 months ago

Stem is about "real-time data INGESTION", not real-time processing.
upvoted 2 times

👤 **bullrem** 1 year, 2 months ago

Selected Answer: C

option C is the best solution. It uses Amazon Kinesis Data Firehose which is a fully managed service for delivering real-time streaming data to destinations such as Amazon S3. This service requires less operational overhead as compared to option A, B, and D. Additionally, it also uses Amazon API Gateway which is a fully managed service for creating, deploying, and managing APIs. These services help in reducing the operational overhead and automating the data ingestion process.

upvoted 1 times

👤 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: C

Option C is the solution that meets the requirements with the least operational overhead.

In Option C, you can use Amazon API Gateway as a fully managed service to create, publish, maintain, monitor, and secure APIs. This means that you don't have to worry about the operational overhead of deploying and maintaining an EC2 instance to host the API.

Option C also uses Amazon Kinesis Data Firehose, which is a fully managed service for delivering real-time streaming data to destinations such as Amazon S3. With Kinesis Data Firehose, you don't have to worry about the operational overhead of setting up and maintaining a data ingestion infrastructure.

upvoted 1 times

👤 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Finally, Option C uses AWS Lambda, which is a fully managed service for running code in response to events. With AWS Lambda, you don't have to worry about the operational overhead of setting up and maintaining a server to run the data transformation code.

Overall, Option C provides a fully managed solution for real-time data ingestion with minimal operational overhead.

upvoted 2 times

👤 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option A is incorrect because it involves deploying an EC2 instance to host an API, which adds operational overhead in the form of maintaining and securing the instance.

Option B is incorrect because it involves deploying an EC2 instance to host an API and disabling source/destination checking on the instance. Disabling source/destination checking can make the instance vulnerable to attacks, which adds operational overhead in the form of securing the instance.

upvoted 2 times

👤 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option D is incorrect because it involves using AWS Glue to send the data to Amazon S3, which adds operational overhead in the form of maintaining and securing the AWS Glue infrastructure.

Overall, Option C is the best choice because it uses fully managed services for the API, data transformation, and data delivery, which minimizes operational overhead.

upvoted 2 times

👤 **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

👤 **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

👤 **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

Question #78

Topic 1

A company needs to keep user transaction data in an Amazon DynamoDB table. The company must retain the data for 7 years.

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

- A. Use DynamoDB point-in-time recovery to back up the table continuously.
- B. Use AWS Backup to create backup schedules and retention policies for the table.
- C. Create an on-demand backup of the table by using the DynamoDB console. Store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function. Configure the Lambda function to back up the table and to store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.

Correct Answer: B

Community vote distribution

B (100%)

✉  **123jh10**  1 year, 5 months ago

Selected Answer: B

Answer is B

"Amazon DynamoDB offers two types of backups: point-in-time recovery (PITR) and on-demand backups. (==> D is not the answer)
 PITR is used to recover your table to any point in time in a rolling 35 day window, which is used to help customers mitigate accidental deletes or writes to their tables from bad code, malicious access, or user error. (==> A isn't the answer)
 On demand backups are designed for long-term archiving and retention, which is typically used to help customers meet compliance and regulatory requirements.
 This is the second of a series of two blog posts about using AWS Backup to set up scheduled on-demand backups for Amazon DynamoDB. Part 1 presents the steps to set up a scheduled backup for DynamoDB tables from the AWS Management Console." (==> Not the DynamoDB console and C isn't the answer either)
<https://aws.amazon.com/blogs/database/part-2-set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/>

upvoted 44 times

✉  **LuckyAro** 1 year, 2 months ago

I think the answer is C because of storage time.

upvoted 1 times

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

Dynamo backups cannot be scheduled or sent to S3, so answer should be B)

- 1) <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/BackupRestore.html>
- 2) <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Backup.Tutorial.html>

upvoted 1 times

✉  **app12** 2 months, 1 week ago

In the very same link you shared it says that you CAN send backups to S3

https://youtu.be/4INEu_hw30Q?t=54

upvoted 1 times

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

Selected Answer: B

The most operationally efficient solution that meets these requirements would be to use option B, which is to use AWS Backup to create backup schedules and retention policies for the table.

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS resources. It allows you to create backup policies and schedules to automatically back up your DynamoDB tables on a regular basis. You can also specify retention policies to ensure that your backups are retained for the required period of time. This solution is fully automated and requires minimal maintenance, making it the most operationally efficient option.

upvoted 13 times

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

Option A, using DynamoDB point-in-time recovery, is also a viable option but it requires continuous backup, which may be more resource-intensive and may incur higher costs compared to using AWS Backup.

Option C, creating an on-demand backup of the table and storing it in an S3 bucket, is also a viable option but it requires manual intervention and does not provide the automation and scheduling capabilities of AWS Backup.

Option D, using Amazon EventBridge (CloudWatch Events) and a Lambda function to back up the table and store it in an S3 bucket, is also a viable option but it requires more complex setup and maintenance compared to using AWS Backup.

upvoted 14 times

✉  **OctavioBatera**  5 days, 6 hours ago

Selected Answer: B

Agreed with option B is the right one. AWS backup retention goes from 1 day to 100 years (or even indefinitely, if you do not enter a retention period), so will meet the requirements.

upvoted 1 times

 **cheroh_tots** 1 month, 1 week ago

Why is the answer not C?

upvoted 2 times

 **1dfed2b** 2 weeks ago

As I see, we are looking for the most operationally efficient solution. So it's B, but the most cost effective its - C (but it isn't a question).

upvoted 1 times

 **psyllon** 1 month, 4 weeks ago

https://youtu.be/g4WPLFXLwDE?si=nTWqqDcBe_Y6dtl3

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: B

Operational efficiency is always a managed service from AWS. AWS Backup is the right one in this case so B is right answer

upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

Answer is simply B as it is MOST operationally efficient. Other options are "distractors" to confuse everyone.

upvoted 1 times

 **viru** 3 months, 1 week ago

Selected Answer: B

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

upvoted 1 times

 **Mikado211** 3 months, 3 weeks ago

Selected Answer: B

Well a 7 years TTL on the dynamoDB records could be the simplest to answer the question, so B for the "retention policies". And since the B also propose AWS backup with a retention time at 7 years, why not.

upvoted 2 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: B

The key advantages of using AWS Backup are:

Fully managed backup service requiring minimal operational overhead

Built-in scheduling, retention policies, and backup monitoring

Supports point-in-time restore for DynamoDB

Automated and scalable solution

upvoted 1 times

 **tamefi5512** 8 months, 4 weeks ago

Selected Answer: B

B - is the answer because it's easy to setup via AWS Backup & It indicates the keyword "MOST Operational Efficient". Other answers are indicating Cost efficient

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

AWS Backup is a fully managed backup service that simplifies the process of creating and managing backups across various AWS services, including DynamoDB. It allows you to define backup schedules and retention policies to automatically take backups and retain them for the desired duration. By using AWS Backup, you can offload the operational overhead of managing backups to the service itself, ensuring that your data is protected and retained according to the specified retention period.

This solution is more efficient compared to the other options because it provides a centralized and automated backup management approach specifically designed for AWS services. It eliminates the need to manually configure and maintain backup processes, making it easier to ensure data retention compliance without significant operational effort.

upvoted 2 times

 **Rahul2212** 9 months, 2 weeks ago

A

PITR is used to recover your table to any point in time in a rolling 35 day window, which is used to help customers mitigate accidental deletes or writes to their tables from bad code, malicious access, or user error. (==> A is the answer)

upvoted 1 times

 **Abrar2022** 10 months ago

using AWS Backup cheaper than DynamoDB point-in-time recovery

upvoted 1 times

 **kraken21** 11 months, 3 weeks ago

Selected Answer: B

With less overhead is AWS Backups:

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

upvoted 1 times

✉ **klayytech** 12 months ago

Selected Answer: B

To retain data for 7 years in an Amazon DynamoDB table, you can use AWS Backup to create backup schedules and retention policies for the table. You can also use DynamoDB point-in-time recovery to back up the table continuously.

upvoted 1 times

✉ **test_devops_aws** 1 year ago

Selected Answer: B

B = AWS backup

upvoted 1 times

Question #79

Topic 1

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly.

What should a solutions architect recommend?

- A. Create a DynamoDB table in on-demand capacity mode.
- B. Create a DynamoDB table with a global secondary index.
- C. Create a DynamoDB table with provisioned capacity and auto scaling.
- D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Correct Answer: A

Community vote distribution

A (79%) C (21%)

SimonPark Highly Voted 1 year, 4 months ago

Selected Answer: A

On-demand mode is a good option if any of the following are true:

- You create new tables with unknown workloads.
- You have unpredictable application traffic.
- You prefer the ease of paying for only what you use.

upvoted 42 times

123jh10 Highly Voted 1 year, 5 months ago

Selected Answer: A

A - On demand is the answer -

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html#HowItWorks.OnDemand>

B - not related with the unpredictable traffic

C - provisioned capacity is recommended for known patterns. Not the case here.

D - same as C

upvoted 21 times

NasosoAuxtyno 1 year ago

Thanks. Your reference link perfectly supports the option "A". 100% correct

upvoted 2 times

awsgeek75 Most Recent 2 months, 1 week ago

Selected Answer: A

cost is concern so CD are not right as provisioning is costly

B is irrelevant

A on-demand is correct as it will scale according to the usage pattern which is from low to very abrupt high

upvoted 1 times

MiniYang 4 months ago

Selected Answer: C

Choosing the On-Demand Capacity model (Option A) may cause performance issues during peak periods because it relies on DynamoDB to automatically adjust throughput based on actual usage, which may not be able to cope with sudden traffic increases in time.

Choosing a DynamoDB table with a global secondary index (option B) is independent of the capacity model and does not directly solve the problem of peak traffic.

Choosing to build DynamoDB tables in provisioned capacity mode and configure them as global tables (option D) may increase costs in some cases without necessarily providing the flexibility to accommodate unpredictable peak traffic.

upvoted 1 times

MiniYang 4 months ago

sorry I want to change my answer to A . Because the point is the " cost "

upvoted 3 times

BartoszGolebiowski24 5 months ago

Selected Answer: A

DynamoDB autoscaling takes 2 minutes to increase capacity. We need to handle it immediately.

"Application Auto Scaling automatically scales the provisioned capacity only when the consumed capacity is higher than target utilization for two consecutive minutes".

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TroubleshootingThrottling.html>

upvoted 2 times

 **xdkonorek2** 4 months, 3 weeks ago

This is important, thank you for the link. A definitely

upvoted 1 times

 **Wayne23Fang** 5 months, 2 weeks ago

Selected Answer: A

The costly part of (C) is you need to pay for what you order not what you have used for (A) On-Demand: A reserved capacity purchase is an agreement to pay for a minimum amount of provisioned throughput capacity, for the duration of the term of the agreement, in exchange for discounted pricing. If you use less than your reserved capacity, you will still be charged each month for that minimum amount of provisioned throughput capacity.

upvoted 1 times

 **clark777** 6 months ago

<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>

With on-demand capacity mode, DynamoDB charges you for the data reads and writes your application performs on your tables. You do not need to specify how much read and write throughput you expect your application to perform because DynamoDB instantly accommodates your workloads as they ramp up or down.

With provisioned capacity mode, you specify the number of reads and writes per second that you expect your application to require, and you are billed based on that. Furthermore if you can forecast your capacity requirements you can also reserve a portion of DynamoDB provisioned capacity and optimize your costs even further.

upvoted 2 times

 **TariqKipkemei** 7 months, 1 week ago

Selected Answer: A

With on-demand capacity mode, DynamoDB instantly accommodates your workloads as they ramp up or down.

upvoted 1 times

 **ontheyun** 9 months ago

on-demand capacity : unpredictable application traffic

provisioned capacity : predictable application traffic, run applications whose traffic is consistent, and ramps up or down gradually.

<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

By choosing provisioned capacity, you can allocate a specific amount of read and write capacity units based on your expected usage during peak times. This helps in cost optimization as you only pay for the provisioned capacity, which can be adjusted according to your anticipated traffic.

Enabling auto scaling allows DynamoDB to automatically adjust the provisioned capacity up or down based on the actual usage. This is beneficial in handling quick traffic spikes without manual intervention and ensuring that the required capacity is available to handle increased load efficiently. Auto scaling helps to optimize costs by dynamically adjusting the capacity to match the demand, avoiding overprovisioning during periods of low usage.

A. Creating a DynamoDB table in on-demand capacity mode, may not be the most cost-effective solution in this scenario. On-demand capacity mode charges you based on the actual usage of read and write requests, which can be beneficial for sporadic or unpredictable workloads. However, it may not be the optimal choice if the table is not used on most mornings.

upvoted 8 times

 **beginnercloud** 10 months, 1 week ago

Selected Answer: A

Correct answer is A

- You create new tables with unknown workloads. - You have unpredictable application traffic. - You prefer the ease of paying for only what you use.

upvoted 1 times

 **Abrar2022** 10 months, 1 week ago

Selected Answer: A

"On-demand" is a good option for applications that have unpredictable or sudden spikes, since it automatically provisions read/write capacity.

"Provisioned capacity" is suitable for applications with predictable usage.

upvoted 1 times

 **cheese929** 11 months ago

Selected Answer: A

Answer is A.

Provisioned capacity is best if you have relatively predictable application traffic, run applications whose traffic is consistent, and ramps up or down gradually.

On-demand capacity mode is best when you have unknown workloads, unpredictable application traffic and also if you only want to pay exactly for what you use. The on-demand pricing model is ideal for bursty, new, or unpredictable workloads whose traffic can spike in seconds or minutes, and when under-provisioned capacity would impact the user experience.

<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>

upvoted 2 times

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

Selected Answer: A

For unpredictable cases there's no way you can provision something, as it cannot be predicted, so the answer is A
upvoted 1 times

✉️  **linux_admin** 12 months ago

Selected Answer: A

On-demand capacity mode allows a DynamoDB table to automatically scale up or down based on the traffic to the table. This means that capacity will be allocated as needed and billing will be based on actual usage, providing flexibility in capacity while minimizing costs. This is an ideal choice for a table that is not used on most mornings and has unpredictable traffic spikes in the evenings.

upvoted 1 times

✉️  **datz** 1 year ago

Selected Answer: A

unpredictable application traffic meaning answer is on demand Capacity

"This means that provisioned capacity is probably best for you if you have relatively predictable application traffic, run applications whose traffic is consistent, and ramps up or down gradually.

Whereas on-demand capacity mode is probably best when you have new tables with unknown workloads, unpredictable application traffic and also if you only want to pay exactly for what you use. The on-demand pricing model is ideal for bursty, new, or unpredictable workloads whose traffic can spike in seconds or minutes, and when under-provisioned capacity would impact the user experience."

upvoted 2 times

✉️  **mell1222** 1 year ago

Selected Answer: A

Use on-demand capacity mode: With on-demand capacity mode, DynamoDB automatically scales up and down to handle the traffic without requiring any capacity planning. This way, the company only pays for the actual amount of read and write capacity used, with no minimums or upfront costs.

upvoted 1 times

Question #80

Topic 1

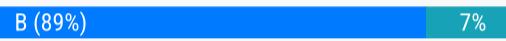
A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs to share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt EBS volume snapshots.

What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

- A. Make the encrypted AMI and snapshots publicly available. Modify the key policy to allow the MSP Partner's AWS account to use the key.
- B. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to allow the MSP Partner's AWS account to use the key.
- C. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to trust a new KMS key that is owned by the MSP Partner for encryption.
- D. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account, Encrypt the S3 bucket with a new KMS key that is owned by the MSP Partner. Copy and launch the AMI in the MSP Partner's AWS account.

Correct Answer: B

Community vote distribution



✉️ **Sauran** 1 year, 5 months ago

Selected Answer: B

Share the existing KMS key with the MSP external account because it has already been used to encrypt the AMI snapshot.

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html>
upvoted 17 times

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

Selected Answer: B

CORRECT

B. Modify the launchPermission property of the AMI.

The most secure way for the solutions architect to share the AMI with the MSP Partner's AWS account would be to modify the launchPermission property of the AMI and share it with the MSP Partner's AWS account only. The key policy should also be modified to allow the MSP Partner's AWS account to use the key. This ensures that the AMI is only shared with the MSP Partner and is encrypted with a key that they are authorized to use.

upvoted 7 times

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

Option A, making the AMI and snapshots publicly available, is not a secure option as it would allow anyone with access to the AMI to use it.

Option C, modifying the key policy to trust a new KMS key owned by the MSP Partner, is also not a secure option as it would involve sharing the key with the MSP Partner, which could potentially compromise the security of the data encrypted with the key.

Option D, exporting the AMI to an S3 bucket in the MSP Partner's AWS account and encrypting the S3 bucket with a new KMS key owned by the MSP Partner, is also not the most secure option as it involves sharing the AMI and a new key with the MSP Partner, which could potentially compromise the security of the data.

upvoted 10 times

✉️ **awsgeek75** 2 months, 1 week ago

Selected Answer: B

AD are unsecure.

I was confused between B and C but read the article (link below). You have to allow the other account to use your key somehow otherwise they won't be able to use your AMI. C just allows a trust relationship with MSP's KMS, it won't give them access to your key.

<https://aws.amazon.com/blogs/security/how-to-share-encrypted-amis-across-accounts-to-launch-encrypted-ec2-instances/>
upvoted 1 times

✉️ **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: B

when you export AMI to s3 bucket it remains encrypted, so partner couldn't launch ec2 instance

upvoted 1 times

✉️ **Ruffyit** 4 months, 4 weeks ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html>
upvoted 1 times

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

Selected Answer: B

Share the AMI and Key with the MSP Partner's AWS account only

upvoted 1 times

✉️ **tamefi5512** 8 months, 4 weeks ago

Selected Answer: B

B - is the Answer

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html>

upvoted 1 times

✉️ **cookieMr** 9 months, 1 week ago

Selected Answer: B

By modifying the launchPermission property of the AMI and sharing it with the MSP Partner's account only, the solutions architect restricts access to the AMI and ensures that it is not publicly available.

Additionally, modifying the key policy to allow the MSP Partner's account to use KMS customer managed key used for encrypting the EBS snapshots ensures that the MSP Partner has the necessary permissions to access and use the key for decryption.

upvoted 2 times

✉️ **Abrar2022** 10 months, 1 week ago

CORRECTION to my last comment Option B is correct not A.

Explanation why..

Making the AMI and snapshots publicly available, is not a secure option as it would allow anyone with access to the AMI to use it. Best practice would be to share the AMI with the MSP Partner's AWS account then Modify launchPermission property of the AMI. This ensures that the AMI is shared only with the MSP Partner and is encrypted with a key that they are authorised to use.

upvoted 2 times

✉️ **Abrar2022** 10 months, 1 week ago

Selected Answer: A

Option A, making the AMI and snapshots publicly available, is not a secure option as it would allow anyone with access to the AMI to use it. Best practice would be to share the AMI with the MSP Partner's AWS account then Modify launchPermission property of the AMI. This ensures that the AMI is shared only with the MSP Partner and is encrypted with a key that they are authorised to use.

upvoted 1 times

✉️ **Simons123** 12 months ago

It is Good but you Can also have a Gift Card and more information Here <https://tinyurl.com/mr4ckeda>

upvoted 1 times

✉️ **draum010** 12 months ago

Selected Answer: D

Option D

upvoted 1 times

✉️ **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

✉️ **Jtic** 1 year, 4 months ago

Selected Answer: B

Must use and share the existing KMS key to decrypt the same key

upvoted 3 times

✉️ **flbcobra** 1 year, 4 months ago

Selected Answer: B

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

upvoted 1 times

✉️ **ManoAni** 1 year, 5 months ago

Selected Answer: B

If EBS snapshots are encrypted, then we need to share the same KMS key to partners to be able to access it. Read the note section in the link <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html>

upvoted 5 times

✉️ **tubtab** 1 year, 5 months ago

Selected Answer: C

MOST secure way should be C

upvoted 3 times

Question #81

Topic 1

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.

Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

decoupled = SQS

Launch template = AMI

Launch configuration = EC2

upvoted 37 times

✉  **cookieMr**  9 months, 1 week ago

Selected Answer: C

This design follows the best practices for loosely coupled and scalable architecture. By using SQS, the jobs are durably stored in the queue, ensuring they are not lost. The processor application is stateless, which aligns with the design requirement. The AMI allows for consistent deployment of the application. The launch template and ASG facilitate the dynamic scaling of the application based on the number of items in the SQS, ensuring parallel processing of jobs.

Options A and D suggest using SNS, which is a publish/subscribe messaging service and may not provide the durability required for job storage.

Option B suggests using network usage as a scaling metric, which may not be directly related to the number of jobs to be processed. The number of items in the SQS provides a more accurate metric for scaling based on the workload.

upvoted 6 times

✉  **awsgeek75**  2 months, 3 weeks ago

Selected Answer: C

SNS is not reliable in case of processing failure which is why none of the SNS options are useful. SQS (not in FIFO mode) allows parallel message processing but reliability/durability of messages is guaranteed. AMI/EC2 scaling is good choice and scaling parameter should be number of messages. Hence "C" is the correct answer

upvoted 1 times

✉  **pentium75** 3 months ago

Selected Answer: C

"Based on the number of jobs to be processed" -> that alone rules out ABD because only C is based on queue length. (D is based on "number of messages published to the queue", not number of messages currently in queue.)

"Job items are durably stored" also speaks for SQS over SNS.

upvoted 2 times

✉  **clumsyninja4life** 3 months ago

so many words...

upvoted 2 times

✉  **awsgeek75** 2 months, 1 week ago

... yet only one answer is correct
upvoted 1 times

 **slimen** 4 months, 3 weeks ago

Selected Answer: C
from my perspective, I didn't go for D even though it provides decoupled architecture is because in the question they said "parallel processing" SNS sends the same message to all the subscribers, but in this case we don't want all the nodes to process the same message instead we want them to process as much jobs as possible in a parallel fashion.
SQS in this case is more suitable because each job will get a message and process it and the next message will be taken by another job and so on..
upvoted 2 times

 **darekw** 6 months, 3 weeks ago

<https://aws.amazon.com/about-aws/whats-new/2021/03/aws-certificate-manager-provides-certificate-expiry-monitoring-through-amazon-cloudwatch/>
upvoted 2 times

 **TariqKipkemei** 7 months, 1 week ago

Selected Answer: C
Loosely coupled = Amazon SQS queue
New application being deployed = deploy on Amazon Machine Image
Adding and removing application nodes as needed based on the number of jobs to be processed = Auto Scaling group with launch template
upvoted 2 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C
The recommended design is to use an SQS queue to store jobs (option C):

SQS provides a durable and decoupled queue to store job items
An Auto Scaling group with scaling policies based on SQS queue length will add/remove nodes as needed
Launch templates provide flexibility to update AMIs
The key points:

SQS enables loose coupling and stores jobs durably
Auto Scaling provides parallel processing
Scaling based on queue length manages nodes effectively
upvoted 2 times

 **Bmarodi** 10 months, 1 week ago

Selected Answer: C
C for sure
upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: C
CORRECT
The correct design is Option C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.

This design satisfies the requirements of the application by using Amazon Simple Queue Service (SQS) as durable storage for the job items and Amazon Elastic Compute Cloud (EC2) Auto Scaling to add and remove nodes based on the number of items in the queue. The processor application can be run in parallel on multiple nodes, and the use of launch templates allows for flexibility in the configuration of the EC2 instances.
upvoted 5 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

WRONG
Option A is incorrect because it uses Amazon Simple Notification Service (SNS) instead of SQS, which is not a durable storage solution.

Option B is incorrect because it uses CPU usage as the scaling trigger instead of the number of items in the queue.

Option D is incorrect for the same reasons as option A.
upvoted 7 times

 **graveend** 7 months, 3 weeks ago

SNS provides durable storage of all messages that it receives.
Ref:
<https://aws.amazon.com/sns/faqs/#:~:text=SNS%20provides%20durable%20storage%20of%20all%20messages%20that%20it%20receives.>

Why use SQS instead of SNS? In the question it says parallel execution of processes. SNS has that ability.
upvoted 1 times

 **cyber_bedouin** 4 months, 2 weeks ago

SQS satisfies the decoupling requirement
upvoted 1 times

 **awsgEEK75** 2 months, 1 week ago

SNS is not a durable storage. SQS stores the messages until they are process. SNS just notifies the subscribers and doesn't care if the notification is processed or not. It's kind of "fire and forget"

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: C

SQS with EC2 autoscaling policy based number of messages in the queue.

upvoted 1 times

✉ **Uhrien** 1 year, 3 months ago

Selected Answer: C

C is correct

upvoted 2 times

✉ **kelljons** 1 year, 3 months ago

what about the word "coupled"

upvoted 1 times

✉ **kewl** 1 year, 3 months ago

Selected Answer: C

AWS strongly recommends that you do not use launch configurations hence answer is C

https://docs.amazonaws.cn/en_us/autoscaling/ec2/userguide/launch-configurations.html

upvoted 3 times

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

Selected Answer: C

answer is C a there is nothing called " Launch Configuration" it's called "Launch Template" which is used by the autoscalling group to creat the new instances.

upvoted 5 times

✉ **lulzsec2019** 1 year, 2 months ago

There's launch configuration. Search

upvoted 3 times

✉ **Liliwood** 1 year, 4 months ago

I was not sure between Launch template and Launch configuration.

upvoted 2 times

Question #82

Topic 1

A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificates that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate. What should a solutions architect recommend to meet this requirement?

- A. Add a rule in ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day, beginning 30 days before any certificate will expire.
- B. Create an AWS Config rule that checks for certificates that will expire within 30 days. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource.
- C. Use AWS Trusted Advisor to check for certificates that will expire within 30 days. Create an Amazon CloudWatch alarm that is based on Trusted Advisor metrics for check status changes. Configure the alarm to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days. Configure the rule to invoke an AWS Lambda function. Configure the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

Correct Answer: D

Community vote distribution



✉ **LeGloupier** 1 year, 5 months ago

B

AWS Config has a managed rule named acm-certificate-expiration-check to check for expiring certificates (configurable number of days)

upvoted 64 times

✉ **LeGloupier** 1 year, 5 months ago

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

upvoted 12 times

✉ **ChrisG1454** 1 year ago

Answer B and answer D are possible according to this article.

So, need to read B & D carefully to determine the most suitable answer.

Reference: <https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

upvoted 6 times

✉ **TTaws** 8 months, 2 weeks ago

Its B, simply because in option D - event bridge cannot "detect" anything.

upvoted 7 times

✉ **RupeC** 8 months, 1 week ago

My understanding is that the ACM sends a Cert Expiration event to EventBridge. Thus EB. does not need to detect anything.

upvoted 2 times

✉ **pentium75** 3 months ago

"ACM sends a Cert Expiration event to EventBridge" yes, but 45 (not 30) days before expiration.

upvoted 1 times

✉ **darekw** 6 months, 3 weeks ago

AWS Certificate Manager (ACM) now publishes certificate metrics and events through Amazon CloudWatch and Amazon EventBridge.

<https://aws.amazon.com/about-aws/whats-new/2021/03/aws-certificate-manager-provides-certificate-expiry-monitoring-through-amazon-cloudwatch/>

upvoted 4 times

✉ **Mia2009687** 8 months, 2 weeks ago

B costs more than D

To get a notification that your certificate is about to expire, use one of the following methods:

Use the ACM API in Amazon EventBridge to configure the ACM Certificate Approaching Expiration event.

Create a custom EventBridge rule to receive email notifications when certificates are nearing the expiration date.

Use AWS Config to check for certificates that are nearing the expiration date.
If you use AWS Config for this resolution, then be aware of the following:

Before you set up the AWS Config rule, create the Amazon Simple Notification Service (Amazon SNS) topic and EventBridge rule. This makes sure that all non-compliant certificates invoke a notification before the expiration date.
Activating AWS Config incurs an additional cost based on usage. For more information, see AWS Config pricing.
<https://repost.aws/knowledge-center/acm-certificate-expiration>

upvoted 4 times

 **pentium75** 2 months, 2 weeks ago

Nobody asked for cost optimization.

upvoted 4 times

 **ManoAni**  1 year, 5 months ago

Selected Answer: B

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

upvoted 14 times

 **bhushansathe**  1 day, 21 hours ago

Selected Answer: D

I think the answer is D as the question is to get a report only for the ACM notification not for the all non-compliant resource

upvoted 1 times

 **Uzbekistan** 4 days, 6 hours ago

Selected Answer: D

Amazon EventBridge Rule: Set up a rule in Amazon EventBridge (formerly CloudWatch Events) to monitor for certificates nearing expiration. You can configure this rule to trigger actions based on certain events.

AWS Lambda Function: Upon detection of certificates that will expire within 30 days, configure the EventBridge rule to invoke an AWS Lambda function. Lambda functions are ideal for executing custom logic in response to events.

Lambda Function to Send Alert: In the Lambda function, implement the logic to send a custom alert via Amazon SNS. SNS is a messaging service that can send notifications to various endpoints, including email, SMS, or other AWS services. This ensures that the security team receives timely notifications regarding certificate expirations.

upvoted 1 times

 **CloudLearner01** 3 weeks, 2 days ago

Answer: B

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

To get a notification that your certificate is about to expire, use one of the following methods:

Use the ACM API in Amazon EventBridge to configure the ACM Certificate Approaching Expiration event.

Create a custom EventBridge rule to receive email notifications when certificates are nearing the expiration date.

Use AWS Config to check for certificates that are nearing the expiration date.

upvoted 1 times

 **sidharthwader** 3 weeks, 5 days ago

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

This AWS document says:

Imported certificates – If you want to use a third-party certificate with Amazon CloudFront, Elastic Load Balancing, or Amazon API Gateway, you may import it into ACM using the AWS Management Console, AWS CLI, or ACM APIs. ACM can not renew imported certificates, but it can help you manage the renewal process. You are responsible for monitoring the expiration date of your imported certificates and for renewing them before they expire. You can use ACM CloudWatch metrics to monitor the expiration dates of an imported certificates and import a new third-party certificate to replace an expiring one.

upvoted 1 times

 **Garen_Lee** 3 weeks, 5 days ago

Selected Answer: D

Refer to the official documents, ACM can use Amazon EventBridge to manage credentials.

<https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html>

upvoted 1 times

 **Risin42** 4 weeks, 1 day ago

Selected Answer: B

D is incorrect because EventBridge can only detect certificates that have already expired, not those that will expire within 30 days. Also, using a Lambda function to send an alert via SNS is unnecessary and adds complexity to the solution.

upvoted 2 times

 **Ikki77** 1 month ago

Selected Answer: B

This option involves using AWS Config to assess the compliance of resources (certificates) and triggering an alert through Amazon EventBridge and Amazon SNS when a noncompliant resource is detected. It provides a proactive and automated approach to monitor certificate expirations.

upvoted 2 times

 **asdfcdsxdfc** 1 month, 1 week ago

Selected Answer: B

I think its B
upvoted 2 times

 **Parul25** 1 month, 3 weeks ago

I choose B.
<https://docs.aws.amazon.com/config/latest/developerguide/acm-certificate-expiration-check.html>
upvoted 1 times

 **psyll0n** 1 month, 4 weeks ago

According to CoPilot (Chat GPT), the correct answer is:

The correct answer is B.

You can create an AWS Config rule that checks for certificates that will expire within 30 days. Then, you can configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a non-compliant resource. This approach allows you to be notified when a certificate is nearing its expiration date, giving you time to renew it before it expires.

Please note that AWS Certificate Manager (ACM) does not automatically renew certificates that you import. Therefore, it's important to monitor the expiration of these certificates and renew them manually as needed.

upvoted 1 times

 **psyll0n** 1 month, 4 weeks ago

Here is an example of how you can set up an AWS Config rule to check for certificates that are nearing the expiration date:

JSON

```
{
  "ConfigRuleName": "acm-certificate-expiration-check",
  "Description": "Checks if AWS Certificate Manager Certificates in your account are marked for expiration within the specified number of days.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::ACM::Certificate"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "ACM_CERTIFICATE_EXPIRATION_CHECK"
  },
  "InputParameters": {
    "daysToExpiration": "30"
  }
}
```

upvoted 1 times

 **thewalker** 2 months ago

Selected Answer: D

D is the correct answer as per the FAQs : <https://aws.amazon.com/certificate-manager/faqs/>

upvoted 2 times

 **xelopelo** 2 months ago

Selected Answer: B

AWS config has a rule specifically created for checking expiration of acm certificates

upvoted 2 times

 **Charumathi** 2 months ago

Selected Answer: B

B is the correct answer,

To get a notification that your certificate is about to expire, use one of the following methods:

Use the ACM API in Amazon EventBridge to configure the ACM Certificate Approaching Expiration event.
Create a custom EventBridge rule to receive email notifications when certificates are nearing the expiration date.
Use AWS Config to check for certificates that are nearing the expiration date.

If you use AWS Config for this resolution, then be aware of the following:

Before you set up the AWS Config rule, create the Amazon Simple Notification Service (Amazon SNS) topic and EventBridge rule. This makes sure that all non-compliant certificates invoke a notification before the expiration date.

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

upvoted 2 times

 **Charumathi** 2 months ago

B is the correct answer,

To get a notification that your certificate is about to expire, use one of the following methods:

Use the ACM API in Amazon EventBridge to configure the ACM Certificate Approaching Expiration event.
Create a custom EventBridge rule to receive email notifications when certificates are nearing the expiration date.
Use AWS Config to check for certificates that are nearing the expiration date.
If you use AWS Config for this resolution, then be aware of the following:

Before you set up the AWS Config rule, create the Amazon Simple Notification Service (Amazon SNS) topic and EventBridge rule. This makes sure that all non-compliant certificates invoke a notification before the expiration date.

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

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/config/latest/developerguide/acm-certificate-expiration-check.html>

B is correct as AWS Config is exactly for this.

A: cannot be done without using CloudWatch (basically D)

C: Trusted Advisor is not for this, it's for performance improvements

D: Why do you need a custom alert?

upvoted 1 times

Question #83

Topic 1

A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed.

What should the solutions architect recommend?

- A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.
- B. Move the website to Amazon S3. Use Cross-Region Replication between Regions.
- C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.
- D. Use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers.

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

CORRECT

C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

Amazon CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as HTML, CSS, JavaScript, images, and videos. By using CloudFront, the company can distribute the content of their website from edge locations that are closer to the users in Europe, reducing the loading times for these users.

To use CloudFront, the company can set up a custom origin pointing to their on-premises servers in the United States. CloudFront will then cache the content of the website at edge locations around the world and serve the content to users from the location that is closest to them. This will allow the company to optimize the loading times for their European users without having to move the backend of the website to a different region.

upvoted 27 times

 **Euowellima** 6 months, 2 weeks ago

excelente explicação

upvoted 1 times

 **TariqKipkemei** 1 year ago

good explanation..thanks

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

WRONG

Option A (launch an Amazon EC2 instance in us-east-1 and migrate the site to it) would not address the issue of optimizing loading times for European users.

Option B (move the website to Amazon S3 and use Cross-Region Replication between Regions) would not be an immediate solution as it would require time to set up and migrate the website.

Option D (use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers) would not be suitable because it would not improve the loading times for users in Europe.

upvoted 16 times

 **SVDK** 2 months, 3 weeks ago

S3 doesn't support dynamic website hosting. Therefore, can be ruled out.

upvoted 3 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: C

Immediate solution is C

A: Requires site migration so won't be immediate

B: Dynamic site cannot work from S3

D: Geoproximity routing policy finds a server close to the user so this makes no sense

C: Not ideal but best option given the "immediate" requirement as CloudFront is a CDN so it will cache whatever is possible as close to the user giving best performance in this case (i.e. when compared to other options)

upvoted 1 times

 **Ruffyit** 4 months, 4 weeks ago

C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

The key reasons are:

CloudFront can cache static content close to European users using edge locations, improving site performance. The custom origin feature allows seamlessly integrating the CloudFront CDN with existing on-premises servers. No changes are needed to the site backend or servers. CloudFront just acts as a globally distributed cache. This can be set up very quickly, meeting the launch deadline. Other options like migrating to EC2 or S3 would require more time and changes. CloudFront is an easier lift. Route 53 geoproximity routing alone would not improve performance much without a CDN.

upvoted 2 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

C. This solution leverages the global network of CloudFront edge locations to cache and serve the website's static content from the edge locations closest to the European users.

A. Hosting the website in a single region would still result in increased latency for European users accessing the site.

B. Moving the website to S3 and implementing Cross-Region Replication would distribute the website's content across multiple regions, including Europe. S3 is primarily used for static content hosting, and it does not provide server-side processing capabilities necessary for dynamic website functionality.

D. Using a geoproximity routing policy in Route 53 would allow you to direct traffic to the on-premises servers based on the geographic location of the users. However, this option does not optimize site loading times for European users as it still requires them to access the website from the on-premises servers in the United States. It does not leverage the benefits of content caching and edge locations for improved performance.

upvoted 3 times

 **Bmarodi** 10 months, 1 week ago

Selected Answer: C

C is best solution.

upvoted 1 times

 **gustavtd** 1 year, 2 months ago

Selected Answer: C

Within few days you can not do more than using CloudFront

upvoted 3 times

 **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

 **kajal1206** 1 year, 3 months ago

Selected Answer: C

C is correct answer

upvoted 1 times

 **koreanmonkey** 1 year, 3 months ago

Selected Answer: C

CloudFront = CDN Service

upvoted 3 times

 **Liliwood** 1 year, 4 months ago

C.

S3 Cross region Replication minimize latency but also copies objects across Amazon S3 buckets in different AWS Regions(data has to remain in origin thou) so B wrong.

Route 53 geo, does not help reducing the latency.

upvoted 2 times

 **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

 **Hunkie** 1 year, 4 months ago

Same question with detailed explanation

<https://www.examtopics.com/discussions/amazon/view/27898-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

 **ArielSchivo** 1 year, 5 months ago

Selected Answer: C

Option C, use CloudFront.

upvoted 3 times

Question #84

Topic 1

A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours.

The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use.

Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

- A. Use Spot Instances for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.
- B. Use Reserved Instances for the production EC2 instances. Use On-Demand Instances for the development and test EC2 instances.
- C. Use Spot blocks for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.
- D. Use On-Demand Instances for the production EC2 instances. Use Spot blocks for the development and test EC2 instances.

Correct Answer: B

Community vote distribution



✉️ **ArielSchivo** Highly Voted 1 year, 5 months ago

Selected Answer: B

Spot blocks are not longer available, and you can't use spot instances on Prod machines 24x7, so option B should be valid.
upvoted 15 times

✉️ **cookieMr** Highly Voted 9 months, 1 week ago

Selected Answer: B

Option B, would indeed be the most cost-effective solution. Reserved Instances provide cost savings for instances that run consistently, such as the production environment in this case, while On-Demand Instances offer flexibility and are suitable for instances with variable usage patterns like the development and test environments. This combination ensures cost optimization based on the specific requirements and usage patterns described in the question.

upvoted 8 times

✉️ **devmon** 6 months, 3 weeks ago

In addition to this, we can set up an automated process to start and stop the EC2 instances in the test and dev environment
upvoted 2 times

✉️ **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: B

Isn't this simple or am I thinking wrong?

"The production EC2 instances run 24 hours a day"

AC are not going to give the 24 hour usage as spot is for intermittent pattern.

D is just normal cost without any discounts for production

B use "reserved" instances so there is an option for discount in billing. On-demand for dev/test is ok as their usage patter doesn't really fall in reserved or spot usage discounts

upvoted 2 times

✉️ **MrPCarrot** 4 months, 1 week ago

B = Reserved for Prod and On Demand for Dev

upvoted 2 times

✉️ **Bmarodi** 10 months, 1 week ago

Selected Answer: B

B meets the requirements, and most cost-effective.

upvoted 1 times

✉️ **ChanghyeonYoon** 11 months, 2 weeks ago

Selected Answer: B

Spot instances are not suitable for production due to the possibility of not running.

upvoted 2 times

✉️ **alexiscloud** 12 months ago

Answeer B:

Sopt block are not longer available and you can't use spot instace on production

upvoted 1 times

✉️ **Nandan747** 1 year, 2 months ago

Selected Answer: B

Well, AWS has DISCONTINUED the Spot-Block option. so that rules out the two options that use spot-block. Wait, this question must be from SAA-C02 or even 01. STALE QUESTION. I don't think this will feature in SAA-C03. Anyhow, the most cost-effective solution would be Option "b"

upvoted 5 times

 **Wajif** 1 year, 3 months ago

Selected Answer: B

Choosing B as spot blocks (Spot instances with a finite duration) are no longer offered since July 2021

upvoted 1 times

 **sparky231** 10 months ago

https://aws.amazon.com/ec2/spot/?cards.sort-by=item.additionalFields.startDateTime&cards.sort-order=asc&trk=8e336330-37e5-41e0-8438-bc1c75320d09&sc_channel=ps&ef_id=CjwKCAjw67ajBhAVEiwA2g_jECglX_lcbqawbH-wVx2Y_EozBm8xv3g3Ci1eps0V49XcZRyfuy9xPhoCOKcQAvD_BwE:G:s&s_kwcid=AL!4422!3!517520538467!p!!g!!aws%20ec%20spot!12831094520!122300635918

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: A

The most cost-effective solution for the company's requirements would be to use Spot Instances for the development and test EC2 instances and Reserved Instances for the production EC2 instances.

Spot Instances are a cost-effective choice for non-critical, flexible workloads that can be interrupted. Since the development and test EC2 instances are only needed for at least 8 hours per day and can be stopped when not in use, they would be a good fit for Spot Instances.

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Reserved Instances are a good fit for production EC2 instances that need to run 24 hours a day, as they offer a significant discount compared to On-Demand Instances in exchange for a one-time payment and a commitment to use the instances for a certain period of time.

Option A is the correct answer because it meets the company's requirements for cost-effectively running the development and test EC2 instances and the production EC2 instances.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option B is not the most cost-effective solution because it suggests using On-Demand Instances for the development and test EC2 instances, which would be more expensive than using Spot Instances. On-Demand Instances are a good choice for workloads that require a guaranteed capacity and can't be interrupted, but they are more expensive than Spot Instances.

Option C is not the correct solution because Spot blocks are a variant of Spot Instances that offer a guaranteed capacity and duration, but they are not available for all instance types and are not necessarily the most cost-effective option in all cases. In this case, it would be more cost-effective to use Spot Instances for the development and test EC2 instances, as they can be interrupted when not in use.

upvoted 1 times

 **WhericanIstart** 1 year ago

Can't use Spot instances for Production environment that needs to run 24/7. That should tell you that Production instances can't have a downtime. Spot instances are used when an application or service can allow disruption and 24/7 production environment won't allow that.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option D is not the correct solution because it suggests using On-Demand Instances for the production EC2 instances, which would be more expensive than using Reserved Instances. On-Demand Instances are a good choice for workloads that require a guaranteed capacity and can't be interrupted, but they are more expensive than Reserved Instances in the long run. Using Reserved Instances for the production EC2 instances would offer a significant discount compared to On-Demand Instances in exchange for a one-time payment and a commitment to use the instances for a certain period of time.

upvoted 1 times

 **PassNow1234** 1 year, 3 months ago

The production EC2 instances run 24 hours a day.

upvoted 2 times

 **pentium75** 3 months ago

A says to use Spot instances for production, which is nonsense as production must run "24 hours a day." Even DEV and TEST can't use Spot because you can't guarantee that they are available for "at least 8 hours each day". That rules out everything but B.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

 **Vickysss** 1 year, 3 months ago

Selected Answer: B

Reserved instances for 24/7 production instances seems reasonable. By exclusion I will choose the on-demand for dev and test (despite thinking that Spot Fleets may be even a better solution from a cost-wise perspective)

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **Jtic** 1 year, 4 months ago

Selected Answer: B

Reserved Instances and On-demand

Spot is out as the use case required continues instance running

upvoted 1 times

 **Nigma** 1 year, 4 months ago

B is the answer

<https://www.examtopics.com/discussions/amazon/view/80956-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Question #85

Topic 1

A company has a production web application in which users upload documents through a web interface or a mobile app. According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored.

What should a solutions architect do to meet this requirement?

- A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.
- B. Store the uploaded documents in an Amazon S3 bucket. Configure an S3 Lifecycle policy to archive the documents periodically.
- C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an ACL to restrict all access to read-only.
- D. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

Correct Answer: A

Community vote distribution

A (100%)

✉  **123jh10**  1 year, 5 months ago

Selected Answer: A

You can use S3 Object Lock to store objects using a write-once-read-many (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use S3 Object Lock to meet regulatory requirements that require WORM storage, or add an extra layer of protection against object changes and deletion. Versioning is required and automatically activated as Object Lock is enabled.
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>
 upvoted 26 times

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

Selected Answer: A

CORRECT

A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.

S3 Versioning allows multiple versions of an object to be stored in the same bucket. This means that when an object is modified or deleted, the previous version is preserved. S3 Object Lock adds additional protection by allowing objects to be placed under a legal hold or retention period, during which they cannot be deleted or modified. Together, S3 Versioning and S3 Object Lock can be used to meet the requirement of not allowing documents to be modified or deleted after they are stored.

upvoted 8 times

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

WRONG

Option B, storing the documents in an S3 bucket and configuring an S3 Lifecycle policy to archive them periodically, would not prevent the documents from being modified or deleted.

Option C, storing the documents in an S3 bucket with S3 Versioning enabled and configuring an ACL to restrict all access to read-only, would also not prevent the documents from being modified or deleted, since an ACL only controls access to the object and does not prevent it from being modified or deleted.

Option D, storing the documents on an Amazon Elastic File System (Amazon EFS) volume and accessing the data in read-only mode, would prevent the documents from being modified, but would not prevent them from being deleted.

upvoted 4 times

✉  **awsgeek75**  2 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>

"S3 Object Lock can help prevent Amazon S3 objects from being deleted or overwritten for a fixed amount of time or indefinitely."

B is archiving which won't stop deletion

C ACL can be modified

D Sounds like there will be a write volume and a read volume which means write volume will have permissions for deletion

upvoted 1 times

✉  **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: A

S3 Versioning ensures that all versions of an object are retained when overwritten or deleted - this prevents deletion.

S3 Object Lock can be used to apply a retention period and legal hold on objects to prevent them from being overwritten or deleted, even by users with full permissions.

Option B only archives objects on a schedule but does not prevent modification or deletion.

Option C uses ACLs which can still be overridden by users with full permissions.

Option D relies on the application to enforce mounting as read-only, which is not as robust as using S3 Object Lock.

upvoted 2 times

 **Subhrangsu** 6 months ago

Liked the explanation for option C.Thanks!

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: A

S3 Versioning allows you to preserve every version of a document as it is uploaded or modified. This prevents accidental or intentional modifications or deletions of the documents.

S3 Object Lock allows you to set a retention period or legal hold on the objects, making them immutable during the specified period. This ensures that the stored documents cannot be modified or deleted, even by privileged users or administrators.

B. Configuring an S3 Lifecycle policy to archive documents periodically does not guarantee the prevention of document modification or deletion after they are stored.

C. Enabling S3 Versioning alone does not prevent modifications or deletions of objects. Configuring an ACL does not guarantee the prevention of modifications or deletions by authorized users.

D. Using EFS does not prevent modifications or deletions of the documents by users or processes with write permissions.

upvoted 2 times

 **Bmarodi** 10 months, 1 week ago

Selected Answer: A

S3 Versioning and S3 Object Lock enabled meet the requirements, hence A is correct ans.

upvoted 2 times

 **SilentMilli** 1 year, 2 months ago

Selected Answer: A

Option A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled. This will ensure that the documents cannot be modified or deleted after they are stored, and will meet the regulatory requirement. S3 Versioning allows you to store multiple versions of an object in the same bucket, and S3 Object Lock enables you to apply a retention policy to objects in the bucket to prevent their deletion.

upvoted 2 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

Option A. Object Lock will prevent modifications to documents

upvoted 1 times

 **HarryZ** 1 year, 3 months ago

Why not C

upvoted 3 times

 **JayBee65** 1 year, 3 months ago

Configure an ACL to restrict all access to read-only would be you could not write the docs to the bucket in the first place.

upvoted 2 times

 **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 1 times

 **flbcobra** 1 year, 4 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

upvoted 1 times

 **Evangelia** 1 year, 5 months ago

Selected Answer: A

aaaaaaaaaa

upvoted 1 times

 **Evangelia** 1 year, 5 months ago

aaaaaaaaaaaaaa

upvoted 1 times

Question #86

Topic 1

A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB instance. The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently. Which solution meets these requirements?

- A. Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.
- B. Store the database user credentials in AWS Systems Manager OpsCenter. Grant the necessary IAM permissions to allow the web servers to access OpsCenter.
- C. Store the database user credentials in a secure Amazon S3 bucket. Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.
- D. Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database.

Correct Answer: A

Community vote distribution

A (100%)

✉  **123jh10**  1 year, 5 months ago

Selected Answer: A

Secrets Manager enables you to replace hardcoded credentials in your code, including passwords, with an API call to Secrets Manager to retrieve the secret programmatically. This helps ensure the secret can't be compromised by someone examining your code, because the secret no longer exists in the code. Also, you can configure Secrets Manager to automatically rotate the secret for you according to a specified schedule. This enables you to replace long-term secrets with short-term ones, significantly reducing the risk of compromise.
<https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html>

upvoted 22 times

✉  **cookieMr**  9 months, 1 week ago

Selected Answer: A

B. SSM OpsCenter is primarily used for managing and resolving operational issues. It is not designed to securely store and manage credentials like AWS Secrets Manager.

C. Storing credentials in an S3 bucket may provide some level of security, but it lacks the additional features and security controls offered by AWS Secrets Manager.

D. While using KMS for encryption is a good practice, managing credentials directly on the web server file system can introduce complexities and potential security risks. It can be challenging to securely manage and rotate credentials across multiple web servers, especially when considering scalability and automation.

In summary, option A is the recommended solution as it leverages AWS Secrets Manager, which is purpose-built for securely storing and managing secrets, and provides the necessary IAM permissions to allow the web servers to access the credentials securely.

upvoted 5 times

✉  **awsgeek75**  2 months, 1 week ago

Selected Answer: A

AWS Secrets Manager is best for storing credentials and supports auto rotation so A is the best choice

upvoted 1 times

✉  **MrPCarrot** 4 months, 1 week ago

A = Rotation of user credentials can be automated using Secrets Manager.

upvoted 1 times

✉  **Ruffyit** 4 months, 4 weeks ago

option A is the recommended solution as it leverages AWS Secrets Manager, which is purpose-built for securely storing and managing secrets, and provides the necessary IAM permissions to allow the web servers to access the credentials securely.

upvoted 1 times

✉  **TariqKipkemei** 7 months ago

Selected Answer: A

AWS Secrets Manager to the rescue....up up and awaaaay

upvoted 1 times

✉  **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: A

The correct answer is A.

Here is the explanation:

AWS Secrets Manager is a service that helps you store, manage, and rotate secrets. Secrets Manager is a good choice for storing database user credentials because it is secure and scalable.

IAM permissions can be used to grant web servers access to AWS Secrets Manager. This will allow the web servers to retrieve the database user credentials from Secrets Manager and use them to connect to the database.

Rotation of user credentials can be automated using Secrets Manager. This will ensure that the database user credentials are rotated on a regular basis, meeting the security requirement.

upvoted 2 times

 **Bmarodi** 10 months, 1 week ago

Selected Answer: A

Option A is ans.

upvoted 2 times

 **vherman** 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

 **thensanity** 1 year, 2 months ago

literally screams for AWS secrets manager to rotate the credentials

upvoted 4 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: A

CORRECT

Option A. Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.

Option A is correct because it meets the requirements specified in the question: a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently. AWS Secrets Manager is designed specifically to store and manage secrets like database credentials, and it provides an automated way to rotate secrets every time they are used, ensuring that the secrets are always fresh and secure. This makes it a good choice for storing and managing the database user credentials in a secure way.

upvoted 5 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

WRONG

Option B, storing the database user credentials in AWS Systems Manager OpsCenter, is not a good fit for this use case because OpsCenter is a tool for managing and monitoring systems, and it is not designed for storing and managing secrets.

Option C, storing the database user credentials in a secure Amazon S3 bucket, is not a secure option because S3 buckets are not designed to store secrets. While it is possible to store secrets in S3, it is not recommended because S3 is not a secure secrets management service and does not provide the same level of security and automation as AWS Secrets Manager.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option D, storing the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system, is not a secure option because it relies on the security of the web server file system, which may not be as secure as a dedicated secrets management service like AWS Secrets Manager. Additionally, this option does not meet the requirement to rotate user credentials frequently because it does not provide an automated way to rotate the credentials.

upvoted 5 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

Option A

upvoted 1 times

 **kewl** 1 year, 3 months ago

Selected Answer: A

Rotate credentials = Secrets Manager

upvoted 3 times

 **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 1 times

 **renekton** 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 2 times

Question #87

Topic 1

A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the event. A solutions architect needs to design a solution that stores customer data that is created during database upgrades. Which solution will meet these requirements?

- A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.
- B. Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.
- C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.
- D. Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

Correct Answer: A*Community vote distribution*

brushiek Highly Voted 1 year, 5 months ago

Selected Answer: A

<https://aws.amazon.com/rds/proxy/>

RDS Proxy minimizes application disruption from outages affecting the availability of your database by automatically connecting to a new database instance while preserving application connections. When failovers occur, RDS Proxy routes requests directly to the new database instance. This reduces failover times for Aurora and RDS databases by up to 66%.

upvoted 44 times

SaurabhTiwari1 3 months, 1 week ago

The original question was about handling a situation where the database is unavailable due to an upgrade, not a failover situation. During a database upgrade, the database instance is not available, and RDS Proxy would not be able to connect to a new database instance because there isn't one.

In this specific scenario, using Amazon SQS as described in option D provides a buffer for the incoming data during the period when the database is unavailable. This ensures that no data is lost, and it can be written to the database once the upgrade is complete.

upvoted 11 times

PassNow1234 1 year, 3 months ago

This is MySQL Database. RDS proxy = no no

upvoted 2 times

Robrobtutu 11 months, 2 weeks ago

It literally says RDS Proxy is available for Aurora MySQL on the link in the comment you're replying to.

upvoted 5 times

pentium75 3 months ago

But still RDS proxy won't help because during upgrades there is no database that it could proxy to.

upvoted 1 times

attila9778 1 year, 4 months ago

Aurora supports RDS proxy!

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 5 times

bgsanata 10 months, 2 weeks ago

This is incorrect as nowhere in the question is mentioned the RDS have more than 1 instance. So... when the instance is down for maintenance there is no second instance to which RDS Proxy can redirect the requests.

The correct answer is D.

upvoted 30 times

Abdou1604 7 months, 2 weeks ago

rDS PROXY Supports RDS (MySQL, PostgreSQL, MariaDB, MS SQL Server) and Aurora (MySQL, PostgreSQL)

upvoted 2 times

 **123jh10**  1 year, 5 months ago

Selected Answer: D

The answer is D.

RDS Proxy doesn't support Aurora DBs. See limitations at:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 25 times

 **JayBee65** 1 year, 3 months ago

It does, according to that link

upvoted 1 times

 **gcmrjbr** 1 year, 4 months ago

You can use RDS Proxy with Aurora Serverless v2 clusters but not with Aurora Serverless v1 clusters.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 4 times

 **adeyinkaamole** 7 months ago

This not RDS supports Aurora mysql database. All the limitations listed in the link you posted above are not related to the question, hence the answer is B

upvoted 1 times

 **adeyinkaamole** 7 months ago

I meant the answer answer is A

upvoted 1 times

 **tinyfoot** 1 year, 4 months ago

Actually RDS Proxy supports Aurora DBs running on PostgreSQL and MySQL.

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.Aurora_Fea_Regions_DB-eng.Feature.RDS_Proxy.html

With RDS proxy, you only expose a single endpoint for request to hit and any failure of the primary DB in a Multi-AZ configuration is will be managed automatically by RDS Proxy to point to the new primary DB. Hence RDS proxy is the most efficient way of solving the issue as additional code change is required.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.howitworks.html>

upvoted 10 times

 **Duke_YU** 11 months, 4 weeks ago

The question doesn't say the RDS is deployed in a Mutli-AZ mode. which means RDS is not accessible during upgrade anyway. RDS proxy couldn't resolve the DB HA issue. The question is looking for a solution to store the data during DB upgrade. I don't know RDS proxy very well, but the RDS proxy introduction doesn't mention it has the capability of storing data. So, answer A couldn't store the data created during the DB upgrade.

I'm assuming this is a bad question design. The expected answer is A, but the question designer missed some important information.

upvoted 6 times

 **rismail** 10 months, 2 weeks ago

<https://aws.amazon.com/rds/proxy/>, if you go down the page, you will see that RDS is deployed in Multi-AZ (amazon RDS Proxy is highly available and deployed over multiple Availability Zones (AZs) to protect you from infrastructure failure. Each AZ runs on its own physically distinct, independent infrastructure and is engineered to be highly reliable. In the unlikely event of an infrastructure failure, the RDS Proxy endpoint remains online and consistent allowing your application to continue to run database operations.) from the link.

upvoted 1 times

 **Uzbekistan**  4 days, 6 hours ago

Selected Answer: D

Amazon SQS FIFO Queue: Amazon SQS FIFO (First-In-First-Out) queues provide exactly-once processing, ensuring that messages are processed in the order they are received and are not duplicated. This ensures the reliability of message delivery, crucial for preserving customer data.

Lambda Function to Process Queue: Create a new Lambda function that regularly polls the SQS FIFO queue for messages containing customer data. Lambda can be configured to trigger based on a schedule or on demand. This function will retrieve messages from the queue and process them, storing the customer data in the database.

upvoted 1 times

 **CloudLearner01** 3 weeks, 2 days ago

RDS proxy is correct

Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability. With RDS Proxy, failover times for Aurora and RDS databases are reduced by up to 66% and database credentials, authentication, and access can be managed through integration with AWS Secrets Manager and AWS Identity and Access Management (IAM).

upvoted 1 times

 **Ikki77** 1 month ago

Selected Answer: D

This option introduces a decoupling mechanism using SQS, allowing the Lambda functions to push customer data to a queue during database upgrades. Another Lambda function can then process the queue and store the customer data in the database. This helps to ensure that customer data is not lost during database upgrades, providing a reliable and asynchronous approach to handle such scenarios.

upvoted 2 times

✉ **thewalker** 2 months ago

Selected Answer: A

Option to have RDS Proxy is available, then why to go other routes ?

upvoted 1 times

✉ **thewalker** 2 months ago

From Amazon Q:

RDS Proxy can be used with Amazon Aurora. Here are some key points about using RDS Proxy with Aurora:

RDS Proxy supports connecting to Aurora MySQL and Aurora PostgreSQL databases. This allows applications to connect to Aurora clusters via the proxy.

Using a proxy provides better scalability by allowing connections to be distributed among Aurora replica instances. It also improves availability since the proxy can direct connections to other Aurora replicas if the primary becomes unavailable.

The Aurora database and RDS Proxy must be in the same VPC to allow connections. Your applications can be deployed in the same VPC or a different one, as long as they have network access to the proxy.

Certain regions and Aurora engine versions support RDS Proxy based on the database engine. You can check the AWS documentation for the latest supported versions in each region.

upvoted 1 times

✉ **thewalker** 2 months ago

The database and proxy need appropriate security group rules and IAM permissions configured to allow connections. The RDS Proxy also requires a secret with database credentials stored in Secrets Manager.

You would connect applications to the proxy endpoint rather than directly connecting to the Aurora endpoint. This allows the proxy to handle and load balance connections to the Aurora replicas.

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.Aurora_Fea_Regions_DB-eng.Feature.RDS_Proxy.html

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy-setup.html>

upvoted 1 times

✉ **Charumathi** 2 months ago

Selected Answer: D

D is the correct answer,

For failover we can use RDS proxy, here the database is upgrade, so there should be a SQS to store the customer data during upgrade, hence we go for option D.

<https://docs.aws.amazon.com/lambda/latest/dg/with-sqs.html>

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Selected Answer: D

I originally voted A but now I believe it's D

RDS Proxy needs something to pool connection against. If the Aurora DB is down the connection pools will not help as they are not connected to anything. SQS FIFO queue will act as a "queue" to store the data until the DB is back up.

Having said all of that I think some critical context is missing from this question which is why there is so much confusion between A/D. Hopefully exam question will have more info.

upvoted 2 times

✉ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: A

I originally would have gone with D but given this is AWS, I would focus on native AWS product based solution as sold by the "marketing" team. "A" will use RDS proxy which is a product suitable for Database failures or unavailability during upgrades.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.howitworks.html#rds-proxy-failover>

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Ignore my answer, it has to be D.

upvoted 1 times

✉ **cheroh_tots** 1 month ago

Given the requirement to ensure customer data is not lost during database upgrades when Lambda functions fail to establish connections, the most appropriate solution is to decouple the Lambda functions from the database using a queueing mechanism. This way, the customer data can be temporarily stored and processed independently of the database availability.

Option D, which suggests storing customer data in an Amazon SQS FIFO queue and creating a new Lambda function to poll the queue and store the data in the database, aligns with this requirement and is the recommended solution.

upvoted 1 times

kel2023 2 months, 3 weeks ago

Selected Answer: D

AWS API Gateway has 29 seconds timeout. Please let me know who can finish database upgrade (and database backup prior upgrade) within 29 seconds then I will vote for A?

upvoted 1 times

DHADD003 3 months ago

Selected Answer: A

It's not D and here is why. As soon as the lambda function fails while using FIFO it will lose the record it processed but didn't save to the database. There is no retry with Lambda. Yes, FIFO will stop from sending further message but you will lose the last record that was sent to the Lambda function. D would be correct if a Dead Letter Queue was added as well.

upvoted 1 times

pentium75 3 months ago

D is correct. If the Lambda function fails, it does not remove the message from the queue, thus it will be picked up again. A is nonsense because during database upgrades, there is no available database. RDS proxy helps to fail over, but there is nothing that you could fail over to.

upvoted 1 times

SaurabhTiwari1 3 months, 1 week ago

Selected Answer: D

D is correct

upvoted 2 times

ansagr 3 months, 2 weeks ago

Selected Answer: D

I would like to retract my previous answer. RDS Proxy helps with read scaling by efficiently distributing read queries among the available read replicas, but it doesn't handle writes during an interruption on the primary instance. When the primary instance is unavailable, write operations are impacted until the primary instance is restored. RDS Proxy primarily focuses on improving the scalability and availability of read-heavy database workloads.

upvoted 3 times

ansagr 3 months, 2 weeks ago

Selected Answer: A

Amazon RDS Proxy helps manage database connections, especially during maintenance events like upgrades. It maintains a pool of established connections, reducing the impact on your application during database upgrades. Configuring Lambda functions to connect to an RDS proxy can help maintain the continuity of storing customer data.

upvoted 1 times

pentium75 3 months ago

But only if there is a second instance that you can fail over to.

upvoted 1 times

Shalen 4 months ago

Selected Answer: D

SQS can store customer data. FIFO guarantees that if the previous message is not processed, the rest will suspend.

upvoted 1 times

MoshiurGCP 4 months ago

ChatGPT chooses SQS

upvoted 1 times

Bjfikky 4 months, 1 week ago

Selected Answer: D

ChatGPT, so take it with a grain of salt, but the explanation makes sense to me "While an RDS proxy can help with managing database connections, it might not completely solve the problem during database upgrades. Connections might still be affected during certain upgrade activities."

upvoted 1 times

Question #88

Topic 1

A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible.

Which solution will meet these requirements?

- A. Configure the Requester Pays feature on the company's S3 bucket.
- B. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.
- C. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.
- D. Configure the company's S3 bucket to use S3 Intelligent-Tiering. Sync the S3 bucket to one of the marketing firm's S3 buckets.

Correct Answer: B

Community vote distribution



✉️ **Six_Fingered_Jose** Highly Voted 1 year, 5 months ago

Selected Answer: B

this question is too vague imho
if the question is looking for a way to incur charges to the European company instead of the US company, then requester pay makes sense.

if they are looking to reduce overall data transfer cost, then B makes sense because the data does not leave the AWS network, thus data transfer cost should be lower technically?

A. makes sense because the US company saves money, but the European company is paying for the charges so there is no overall saving in cost when you look at the big picture

I will go for B because they are not explicitly stating that they want the other company to pay for the charges

upvoted 56 times

✉️ **FNJ1111** 1 year, 2 months ago

I disagree. The question says, "the company wants to ensure that ITS data transfer costs remain as low as possible" -- 'it' being the US company. The question would have stayed "ensure that data transfer costs" (without the word 'its') if they meant the overall data transfer cost.
upvoted 12 times

✉️ **aadityaravi8** 9 months ago

I don't agree with your explanation, you are overthinking it in wrong direction.
upvoted 1 times

✉️ **Kp88** 8 months ago

What if company decides to share data with 10 new companies ? Why would a company pay for data transfer when there is a requestor pay feature available.
upvoted 2 times

✉️ **TariqKipkemei** 1 year ago

I concur with your explanation 100%
upvoted 1 times

✉️ **rushi0611** 10 months, 4 weeks ago

Agree, B) Cross Region Replication: \$0.02/GB
A) over the internet it is \$0.09/GB
Answer is B
upvoted 6 times

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

is S3 Cross-Region Replication works between 2 separate aws accounts? shouldn't the answer is C?
upvoted 2 times

✉️ **awsgeek75** 2 months, 3 weeks ago

"C" can't be the answer as it means the S3 data access survey company will incur the cost when data is accessed by European company.
upvoted 1 times

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

I agree, also the question says that the target firm "has S3 buckets." so I think that is a clue to say they can accept replication data on any of those buckets.
upvoted 1 times

 **123jh10**  1 year, 5 months ago

Selected Answer: A

"Typically, you configure buckets to be Requester Pays buckets when you want to share data but not incur charges associated with others accessing the data. For example, you might use Requester Pays buckets when making available large datasets, such as zip code directories, reference data, geospatial information, or web crawling data."

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

upvoted 36 times

 **Uzbekistan**  4 days, 6 hours ago

Selected Answer: B

S3 Cross-Region Replication: This feature automatically replicates objects from the source bucket (owned by the survey company) to a destination bucket (owned by the marketing firm) in a different AWS region. By replicating the data to the marketing firm's region, data transfer costs can be minimized, as data transfers within the same AWS region are typically cheaper than those across regions.

Cost Efficiency: Since the marketing firm is located in Europe, having the data replicated to an S3 bucket in a European AWS region reduces the data transfer costs associated with transferring data across regions.

upvoted 1 times

 **Ikki77** 1 month ago

Selected Answer: B

This option allows the data to be replicated to the European marketing firm's S3 bucket, minimizing data transfer costs. Cross-Region Replication enables the efficient transfer of data between regions, and since the marketing firm has its own S3 bucket, they can access the replicated data without incurring additional costs. This approach provides a cost-effective way to share the data while maintaining low transfer costs.

upvoted 2 times

 **vip2** 1 month, 1 week ago

Selected Answer: B

B is correct

The data in US S3 is '3T and growing' and better to use Cross-Region-Replica.

A as my understanding is mainly useful for consumer takes care of their cost to use S3 data

upvoted 1 times

 **arslantobe** 1 month, 3 weeks ago

why not option d

upvoted 1 times

 **tuso** 1 month, 3 weeks ago

I tend to go for A, but it says the company is "sharing" data, so it sounds like a collaboration, not a sale, so B makes sense too. Again, another vague question

upvoted 1 times

 **thewalker** 2 months ago

Selected Answer: C

As per Amazon Q:

Cross Region Replication would be more expensive than cross account access across different regions in S3.

While data transfer between S3 buckets within the same region is free, transferring objects between regions would incur data transfer charges. Cross Region Replication also requires that the objects be replicated to the other regions periodically based on configured rules.

On the other hand, accessing objects across accounts within the same region does not involve any data transfer charges. The objects do not need to be replicated. Applications can access objects in another account's S3 bucket within the same region at no additional cost other than standard S3 storage and request charges.

upvoted 1 times

 **thewalker** 2 months ago

Some key factors to consider are data transfer costs, replication overhead, and latency requirements for accessing objects in other regions. The AWS documentation provides up-to-date pricing details for different data transfer scenarios that can help evaluate the total cost.

<https://repost.aws/questions/QU1TLOxt1TSRyCqqCuP1FulA/s3-cross-account-cross-region-replication>

<https://repost.aws/questions/QUORpWYUPSS6e9e6AVLVyGNQ/cost-of-moving-objects-between-buckets-in-s3-from-multiple-account-under-same-region>

upvoted 1 times

 **Charumathi** 2 months ago

Selected Answer: B

B is the correct answer,

* Cut Down On Cross-Regional Data Transfer

If you frequently transfer data between S3 buckets in different regions, you can use the cross-region replication feature to mirror your S3 bucket in a different region.

This will improve performance and save you money on data transfer and Amazon S3 storage costs.

For example, if you are transferring 20 GB from a bucket in US-west-2 to an EC2 instance in US-east-1, you would be charged \$0.20.

However, if you first downloaded the data to a mirror S3 bucket in US-east-1, you would only pay \$0.02 for transfer and \$0.03 for storage over the course of a month, which would be significantly less expensive.

upvoted 2 times

bujuman 2 months, 2 weeks ago

Selected Answer: A

If the Requester Pays feature is a valuable option and can be configured on S3 bucket level, why not using it. Finally vote for A.
upvoted 1 times

awsgeek75 2 months, 3 weeks ago

Selected Answer: B

For those confused between "A" and "B", the correct answer is "B" because there are conditions where the survey company can incur charges to S3 access under Requester Pays Fee feature. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/RequesterPaysBuckets.html#ChargeDetails>

As US S3 to EU S3 data transfer will cost about 60\$ (<https://aws.amazon.com/s3/pricing/>), it seems like a fixed price to charge the buyer of the data and just replicate it to their S3.

upvoted 2 times

bujuman 2 months, 2 weeks ago

If the Requester Pays feature is a valuable option and can be configured on S3 bucket level, why not using it. Finally vote for A.

upvoted 1 times

awsgeek75 2 months, 1 week ago

The question is vague. In exam, if the language is much more clear I would definitely go for A myself as this looks like a logical option. Also, remember from exam guide, some questions are just for valuation without a score to see how testers will react. Some questions also have multiple correct answers. So this could be one of either. Who knows...

upvoted 1 times

SaurabhTiwari1 3 months, 1 week ago

Selected Answer: A

Data transferred within the AWS network may incur lower costs, this could also lead to additional costs for data storage in the second region. so correct ans is A
upvoted 2 times

Vladan0 3 months, 4 weeks ago

Selected Answer: A

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

upvoted 2 times

RyanMccar 4 months, 1 week ago

Selected Answer: C

Cross account access. No transfer fees at all

upvoted 5 times

awsgeek75 2 months, 1 week ago

It will be cross region too as the customer is in Europe and company is in US which has a fee

upvoted 2 times

aptx4869 4 months, 4 weeks ago

Selected Answer: C

The answer is obviously C. We can share the s3 bucket using IAM of other AWS account.

upvoted 4 times

awsgeek75 2 months, 1 week ago

Yes you can but the cost of transfer across regions (US-Europe) will be on the S3 owner

upvoted 1 times

David_Ang 5 months, 3 weeks ago

Selected Answer: B

here we have to ensure that the data transfer cost less money, so if the European company is my customer and he is paying me for the data that is in my S3 bucket, then is my responsibility to transfer the data the most cost efficient way. in another case this European company is part of my principal company then is has absolutely no sense to pay more to transfer data in any way, the correct answer is "B".
upvoted 2 times

Abitek007 5 months, 3 weeks ago

Selected Answer: B

Best way to reduce cost.
choosing A will be additional cost for data transfer
upvoted 1 times

Question #89

Topic 1

A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.

What should a solutions architect do to secure the audit documents?

- A. Enable the versioning and MFA Delete features on the S3 bucket.
- B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.
- C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3>DeleteObject action during audit dates.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Correct Answer: A*Community vote distribution*

A (100%)

 **123jh10**  1 year, 5 months ago

Selected Answer: A

Same as Question #44

upvoted 14 times

 **awsgEEK75**  2 months, 3 weeks ago

Selected Answer: A

Accidental deletion is the key. Deletion is allowed but MFA deletion ensures that deletion requires an additional step.
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiFactorAuthenticationDelete.html>

upvoted 1 times

 **TariqKipkemei** 7 months ago

Selected Answer: A

Enable the versioning to ensure restoration in case of accidental deletion and MFA Delete for double verification before deletion.
 upvoted 2 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: A

Versioning will keep multiple variants of an object in case one is accidentally or intentionally deleted - the previous versions can still be restored.

MFA Delete requires additional authentication to permanently delete an object version. This prevents accidental deletion
 upvoted 2 times

 **cookieMr** 9 months, 1 week ago

B. Enabling MFA on the IAM user credentials adds an extra layer of security to the user authentication process. However, it does not specifically address the concern of accidental deletion of documents in the S3 bucket.

C. Adding an S3 Lifecycle policy to deny the delete action during audit dates would prevent intentional deletions during specific time periods. However, it does not address accidental deletions that can occur at any time.

D. Using KMS for encryption and restricting access to the KMS key provides additional security for the data stored in the S3 . However, it does not directly prevent accidental deletion of documents in the S3.

Enabling versioning and MFA Delete on the S3 (option A) is the most appropriate solution for securing the audit documents. Versioning ensures that multiple versions of the documents are stored, allowing for easy recovery in case of accidental deletions. Enabling MFA Delete requires the use of multi-factor authentication to authorize deletion actions, adding an extra layer of protection against unintended deletions.

upvoted 2 times

 **beginnercloud** 10 months, 1 week ago

Selected Answer: A

A is answer.

upvoted 1 times

 **Bmarodi** 10 months, 1 week ago

Selected Answer: A

A is answer.

upvoted 1 times

 **Robrobtutu** 11 months, 2 weeks ago

Selected Answer: A

A is correct.

upvoted 1 times

 **remand** 1 year, 2 months ago

Selected Answer: A

only accidental deletion should be avoided. IAM policy will completely remove their access.hence, MFA is the right choice.

upvoted 1 times

 **karbob** 1 year, 2 months ago

what about : IAM policies are used to specify permissions for AWS resources, and they can be used to allow or deny specific actions on those resources.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyDeleteObject",
      "Effect": "Deny",
      "Action": "s3:DeleteObject",
      "Resource": [
        "arn:aws:s3:::my-bucket/my-object",
        "arn:aws:s3:::my-bucket"
      ]
    }
  ]
}
```

upvoted 2 times

 **remand** 1 year, 2 months ago

only accidental deletion should be avoided. IAM policy will completely remove their access.hence, MFA is the right choice.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: A

The solution architect should do Option A: Enable the versioning and MFA Delete features on the S3 bucket.

This will secure the audit documents by providing an additional layer of protection against accidental deletion. With versioning enabled, any deleted or overwritten objects in the S3 bucket will be preserved as previous versions, allowing the company to recover them if needed. With MFA Delete enabled, any delete request made to the S3 bucket will require the use of an MFA code, which provides an additional layer of security.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Option B: Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account, would not provide protection against accidental deletion.

Option C: Adding an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates, which would not provide protection against accidental deletion outside of the specified audit dates.

Option D: Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key, would not provide protection against accidental deletion.

upvoted 2 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

A is the right answer

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 1 times

 **Jtic** 1 year, 4 months ago

Selected Answer: A

Enable the versioning and MFA Delete features on the S3 bucket.

upvoted 1 times

Question #90

Topic 1

A company is using a SQL database to store movie data that is publicly accessible. The database runs on an Amazon RDS Single-AZ DB instance. A script runs queries at random intervals each day to record the number of new movies that have been added to the database. The script must report a final total during business hours.

The company's development team notices that the database performance is inadequate for development tasks when the script is running. A solutions architect must recommend a solution to resolve this issue.

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

- A. Modify the DB instance to be a Multi-AZ deployment.
- B. Create a read replica of the database. Configure the script to query only the read replica.
- C. Instruct the development team to manually export the entries in the database at the end of each day.
- D. Use Amazon ElastiCache to cache the common queries that the script runs against the database.

Correct Answer: D

Community vote distribution

B (94%) 4%

 **alvarez100**  1 year, 5 months ago

Selected Answer: B

Elasti Cache if for reading common results. The script is looking for new movies added. Read replica would be the best choice.
upvoted 37 times

 **Gil80**  1 year, 4 months ago

Selected Answer: B

- You have a production DB that is taking on a normal load
 - You want to run a reporting application to run some analytics
 - You create a read replica to run the new workload there
 - The prod application is unaffected
 - Read replicas are used for SELECT (=read) only kind of statements
- Therefore I believe B to be the better answer.

As for "D" - ElastiCache use cases are:

1. Your data is slow or expensive to get when compared to cache retrieval.
2. Users access your data often.
3. Your data stays relatively the same, or if it changes quickly staleness is not a large issue.

- 1 - Somewhat true.
- 2 - Not true for our case.
- 3 - Also not true. The data changes throughout the day.

For my understanding, caching has to do with millisecond results, high-performance reads. These are not the issues mentioned in the questions, therefore B.

upvoted 16 times

 **NitiATOS** 1 year, 1 month ago

I will support this by point to the question : " with the LEAST operational overhead?"

Configuring the read replica is much easier than configuring and integrating new service.

upvoted 4 times

 **awsgeek75**  2 months, 1 week ago

Selected Answer: B

Just read from read replica.

- A: This will make it HA but won't solve any problems
 C: We want an AWS solution not change the development team's ways of working
 D: ElastiCache is cache of read queries when data doesn't change. It's useless for finding new data.
 upvoted 2 times

 **bujuman** 2 months, 2 weeks ago

Selected Answer: A

Answer C is inconceivable according to LEAST operational overhead?

We will exclude answer D because question is about RDS databases and ElastiCache is not.

Between answers A and B , A is the most appropriate answer due to 2 following points:

- Possible to transform a Single-AZ RDS to Multi-AZ
- LEAST operational overhead

upvoted 1 times

✉ **smdrouiss** 3 months, 2 weeks ago

Selected Answer: A

It is A , because the scenario mention "single db instance" which is not possible to enable read replica

upvoted 1 times

✉ **pentium75** 3 months ago

Doesn't it become a multi-instance DB when you add a read replica? A can't be because you can't read from the passive replica of a multi-AZ DB.

upvoted 3 times

✉ **slimen** 4 months, 3 weeks ago

Selected Answer: B

lol seriously the person who wrote the answer wants us to fail

upvoted 4 times

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

Selected Answer: B

This is what we do in the real world.

upvoted 1 times

✉ **joshik** 6 months ago

Selected Answer: B

- Cached data might not always be up-to-date, so you need to manage cache expiry and invalidation carefully.
- It may require some code changes to implement caching logic in your script.
- ElastiCache comes with additional costs, so you should assess the cost implications based on your usage.

upvoted 1 times

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

Selected Answer: B

Why not D:

While ElastiCache can be relatively easy to set up, it still requires ongoing management, monitoring, and potentially scaling as the dataset and query load grow. This introduces operational overhead that may not align with the goal of minimizing operational work.

upvoted 1 times

✉ **Router** 6 months, 4 weeks ago

the correct answer should be A, you can't create a read replica on a single-AZ DB instance

upvoted 1 times

✉ **TariqKipkemei** 7 months ago

Selected Answer: B

a read replica is always fit for these type of scenarios.

upvoted 1 times

✉ **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: B

The key requirements are:

The script must report a final total during business hours

Resolve the issue of inadequate database performance for development tasks when the script is running

With the least operational overhead

upvoted 1 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: B

A. Modifying the DB to be a Multi-AZ deployment improves high availability and fault tolerance but does not directly address the performance issue during the script execution.

C. Instructing the development team to manually export the entries in the database introduces manual effort and is not a scalable or efficient solution.

D. While using ElastiCache for caching can improve read performance for common queries, it may not be the most suitable solution for the scenario described. Caching is effective for reducing the load on the database for frequently accessed data, but it may not directly address the performance issue during the script execution.

Creating a read replica of the database (option B) provides a scalable solution that offloads read traffic from the primary database. The script can be configured to query the read replica, reducing the impact on the primary database during the script execution.

upvoted 4 times

✉ **MostafaWardany** 10 months, 1 week ago

Selected Answer: B

For LEAST operational overhead, I recommended to use read replica DB

upvoted 1 times

 **Bmarodi** 10 months, 1 week ago

Selected Answer: B

The option B will reduce burden on DB, because the script will read only from replica, not from DB, hence option B is correct answer.
upvoted 1 times

 **Siva007** 10 months, 1 week ago

Selected Answer: B

B is correct. Read replica for read only script any analytical loads.
upvoted 1 times

 **cheese929** 11 months ago

Selected Answer: B

B is correct. Run the script on the read replica.
upvoted 1 times

Question #91

Topic 1

A company has applications that run on Amazon EC2 instances in a VPC. One of the applications needs to call the Amazon S3 API to store and read objects. According to the company's security regulations, no traffic from the applications is allowed to travel across the internet. Which solution will meet these requirements?

- A. Configure an S3 gateway endpoint.
- B. Create an S3 bucket in a private subnet.
- C. Create an S3 bucket in the same AWS Region as the EC2 instances.
- D. Configure a NAT gateway in the same subnet as the EC2 instances.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **ArielSchivo**  1 year, 5 months ago

Selected Answer: A

Gateway endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC. It should be option A.

<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html>
upvoted 27 times

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

Selected Answer: A

CORRECT

The correct solution is Option A (Configure an S3 gateway endpoint.)

A gateway endpoint is a VPC endpoint that you can use to connect to Amazon S3 from within your VPC. Traffic between your VPC and Amazon S3 never leaves the Amazon network, so it doesn't traverse the internet. This means you can access Amazon S3 without the need to use a NAT gateway or a VPN connection.

WRONG

Option B (creating an S3 bucket in a private subnet) is not a valid solution because S3 buckets do not have subnets.

Option C (creating an S3 bucket in the same AWS Region as the EC2 instances) is not a requirement for meeting the given security regulations.

Option D (configuring a NAT gateway in the same subnet as the EC2 instances) is not a valid solution because it would allow traffic to leave the VPC and travel across the Internet.

upvoted 13 times

✉️  **Charumathi**  2 months ago

Selected Answer: A

You can access Amazon S3 from your VPC using gateway VPC endpoints. After you create the gateway endpoint, you can add it as a target in your route table for traffic destined from your VPC to Amazon S3.

There is no additional charge for using gateway endpoints.

Amazon S3 supports both gateway endpoints and interface endpoints. With a gateway endpoint, you can access Amazon S3 from your VPC, without requiring an internet gateway or NAT device for your VPC, and with no additional cost. 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 1 times

✉️  **awsgeek75** 2 months, 1 week ago

Selected Answer: A

EC2 to S3 without public interne = S3 gateway

B: Cannot be implemented

C: Even if you create EC2 and S3 in same region, without a S3 gateway it will use the public internet

D: Makes no sense, NAT gateway in the subnet as EC2 instance to do what?

upvoted 1 times

✉️  **Ruffyit** 4 months, 4 weeks ago

A gateway endpoint is a VPC endpoint that you can use to connect to Amazon S3 from within your VPC. Traffic between your VPC and Amazon S3 never leaves the Amazon network, so it doesn't traverse the internet. This means you can access Amazon S3 without the need to use a NAT gateway or a VPN connection

upvoted 1 times

 **David_Ang** 5 months, 3 weeks ago

Selected Answer: A

Answer "A" is correct because an endpoint creates a way for the data to travel in the VPC

upvoted 1 times

 **TariqKipkemei** 7 months ago

Selected Answer: A

Prevent traffic from traversing the internet = Gateway VPC endpoint for S3.

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: A

Configure an S3 gateway endpoint

upvoted 1 times

 **tamefi5512** 8 months, 4 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/vpc/latest/privateLink/gateway-endpoints.html>

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

B. Creating an S3 in a private subnet restricts direct internet access to the bucket but does not provide a direct and secure connection between the EC2 and the S3. The application would still need to traverse the internet to access the S3 API.

C. Creating an S3 in the same Region as the EC2 does not inherently prevent traffic from traversing the internet.

D. Configuring a NAT gateway allows outbound internet connectivity for resources in private subnets, but it does not provide a direct and secure connection to the S3 service. The traffic from the EC2 to the S3 API would still traverse the internet.

The most suitable solution is to configure an S3 gateway endpoint (option A). It provides a secure and private connection between the VPC and the S3 service without requiring the traffic to traverse the internet. With an S3 gateway endpoint, the EC2 can access the S3 API directly within the VPC, meeting the security requirement of preventing traffic from traveling across the internet.

upvoted 2 times

 **Bmarodi** 10 months, 1 week ago

Selected Answer: A

Configure an S3 gateway endpoint is answer.

upvoted 1 times

 **gustavtd** 1 year, 2 months ago

Selected Answer: A

S3 Gateway Endpoint is a VPC endpoint,

upvoted 1 times

 **langiac** 1 year, 3 months ago

Selected Answer: A

<https://docs.aws.amazon.com/vpc/latest/privateLink/gateway-endpoints.html>

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 1 times

Question #92

Topic 1

A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.

Which combination of steps should a solutions architect take to accomplish this? (Choose two.)

- A. Configure a VPC gateway endpoint for Amazon S3 within the VPC.
- B. Create a bucket policy to make the objects in the S3 bucket public.
- C. Create a bucket policy that limits access to only the application tier running in the VPC.
- D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.
- E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.

Correct Answer: AC

Community vote distribution

AC (86%)

14%

 **awsgeek75** 2 months, 1 week ago

Selected Answer: AC

A: VPC S3 gateway for direct connection (no public internet) to access S3
 C: Bucket policy to secure access and only allow the VPC application tier to access it

B: Opens up to public
 D: Not secure to copy credentials
 E: NAT instance (obsolete now) is not useful for limiting resource access, it's for subnet connections
 upvoted 3 times

 **rityoui** 3 months, 1 week ago

no one mentioned the translation issue, "limit access to sth" sounds like limit this but allow others, confusing for non-English speaker.
 upvoted 1 times

 **Ruffyit** 4 months, 4 weeks ago

) Configure a VPC gateway endpoint for Amazon S3 within the VPC.
 C) Create a bucket policy that limits access to only the application tier running in the VPC.

The key requirements are secure access to the S3 bucket from EC2 instances in the VPC.

A VPC endpoint for S3 allows connectivity from the VPC to S3 without needing internet access. The bucket policy should limit access only to the VPC by whitelisting the VPC endpoint.

upvoted 1 times

 **David_Ang** 5 months, 3 weeks ago

Selected Answer: AC

These are correct because "A" and "C" ensure secure access and secure connectivity between the S3 and the EC2 instances
 upvoted 2 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: AC

The key requirements are to provide secure access to the S3 bucket only from the application tier EC2 instances inside the VPC.

A VPC gateway endpoint allows private access to S3 from within the VPC without needing internet access. This keeps the traffic secure within the AWS network.

The bucket policy should limit access to only the application tier, not make the objects public. This restricts access to the sensitive data to only the authorized application tier.

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: AC

The correct options are:

- A) Configure a VPC gateway endpoint for Amazon S3 within the VPC.
- C) Create a bucket policy that limits access to only the application tier running in the VPC.

The key requirements are secure access to the S3 bucket from EC2 instances in the VPC.

A VPC endpoint for S3 allows connectivity from the VPC to S3 without needing internet access. The bucket policy should limit access only to the VPC by whitelisting the VPC endpoint.

upvoted 2 times

 **sohailn** 7 months, 2 weeks ago

ac is the correct answer, as per my knowledge people are confused with IAM user we can use IAM role for secure access.

upvoted 1 times

 **tamefi5512** 8 months, 4 weeks ago

Selected Answer: AC

AC is the right answer

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: AC

A. This eliminates the need for the traffic to go over the internet, providing an added layer of security.

B. It is important to restrict access to the bucket and its objects only to authorized entities.

C. This helps maintain the confidentiality of the sensitive user information by limiting access to authorized resources.

D. In this case, since the EC2 instances are accessing the S3 bucket from within the VPC, using IAM user credentials is unnecessary and can introduce additional security risks.

E. a NAT instance to access the S3 bucket adds unnecessary complexity and overhead.

In summary, the recommended steps to provide secure access to the S3 from the application tier running on EC2 inside a VPC are to configure a VPC gateway endpoint for S3 within the VPC (option A) and create a bucket policy that limits access to only the application tier running in the VPC (option C).

upvoted 2 times

 **Bmarodi** 10 months, 1 week ago

Selected Answer: AC

A & C the correct solutions.

upvoted 2 times

 **TillieEhaung** 10 months, 2 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

 **annabellehiro** 1 year ago

Selected Answer: AC

A and C

upvoted 1 times

 **Help2023** 1 year, 1 month ago

Selected Answer: AC

The key part that many miss out on is 'Combination'

The other answers are not wrong but

A works with C and not with the rest as they need an internet connection.

upvoted 2 times

 **vherman** 1 year, 1 month ago

Selected Answer: AC

AC is correct

upvoted 1 times

 **bdp123** 1 year, 1 month ago

Selected Answer: AC

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-private-connection-noauthentication/>

upvoted 2 times

 **remand** 1 year, 2 months ago

Selected Answer: CD

c & D for security. A addresses accessibility which is not a concern here imo

upvoted 2 times

 **pentium75** 3 months ago

"Copy the IAM credentials to the EC2 instance" hell no

upvoted 1 times

 **goodmail** 1 year, 2 months ago

Selected Answer: AC

A & C.

When the question is about security, do not select the answer that storing credential in EC2. This shall be done by using IAM policy + role or Secret Manager.

upvoted 2 times

Question #93

Topic 1

A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability.

The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours, the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes.

A solutions architect must recommend replacement architecture that alleviates the application latency issue. The replacement architecture also must give the development team the ability to continue using the staging environment without delay.

Which solution meets these requirements?

- A. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.
- B. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.
- C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Use the standby instance for the staging database.
- D. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

Correct Answer: B

Community vote distribution



Buruguduystunstugudunstuy Highly Voted 1 year, 3 months ago

Selected Answer: B

The recommended solution is Option B: Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.

To alleviate the application latency issue, the recommended solution is to use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production, and use database cloning to create the staging database on-demand. This allows the development team to continue using the staging environment without delay, while also providing elasticity and availability for the production application.

Therefore, Options A, C, and D are not recommended

upvoted 18 times

MutiverseAgent 8 months, 2 weeks ago

Agree, solution it seems to be the B)

- 1) Because the company wants "elasticity and availability" as the question mentioned, so I think this leaves us in the two questions related to Aurora discarding the RDS Mysql solution.
- 2) According AWS documentation (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Clone.html>) "Aurora cloning is especially useful for quickly setting up test environments using your production data, without risking data corruption"

upvoted 4 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Option A: Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Populating the staging database by implementing a backup and restore process that uses the mysqldump utility is not the recommended solution because it involves taking a full export of the production database, which can cause unacceptable application latency.

Option C: Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Using the standby instance for the staging database is not the recommended solution because it does not give the development team the ability to continue using the staging environment without delay. The standby instance is used for failover in case of a production instance failure, and it is not intended for use as a staging environment.

upvoted 18 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Option D: Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populating the staging database by implementing a backup and restore process that uses the mysqldump utility is not the recommended solution because it involves taking a full export of the production database, which can cause unacceptable application latency.

upvoted 7 times

arashis1993 Highly Voted 4 months, 3 weeks ago

Selected Answer: B

Aura MySQL is very fast in comparison to RDS for creating a clone of DB, you can create even clone of a clone while you still work on your own clone, this will allow the dev team continue working during cloning step.

<https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/>

upvoted 5 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: B

I'll go for B

AD: looks time consuming as mysqldump is like a table dump

C: You cannot use a standby for anything apart from read-only database. This would be an option if dev team was specifically using it for read-only mode.

<https://aws.amazon.com/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/>
upvoted 1 times

 **Ruffyit** 4 months, 4 weeks ago

B. With Aurora, you can create a clone of the production database quickly and efficiently, without the need for time-consuming backup and restore processes. The development team can spin up the staging database on-demand, eliminating delays and allowing them to continue using the staging environment without interruption.

upvoted 1 times

 **Modulopi** 5 months, 4 weeks ago

Selected Answer: B

B is the correct

upvoted 1 times

 **TariqKipkemei** 7 months ago

Selected Answer: C

No mention of cost, so technically both options B & C would work.

C. <https://aws.amazon.com/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/#:~:text=read%20replicas.-,Amazon%20RDS,-now%20offers%20Multi>

B.<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Clone.html#:~:text=cloning%20works.-,Aurora%20cloning,-is%20especially%20useful>

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: B

Option B is the best solution that meets all the requirements:

Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.

The key requirements are to:

Alleviate application latency caused by database exports

Give development immediate access to a staging environment

Aurora Multi-AZ replicas improves availability and provides fast failover.

Database cloning creates an instantly available copy of the production database that can be used for staging. This avoids any export or restoration del

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B

A. Populating the staging database through a backup and restore process using the mysqldump utility would still result in delays and impact application latency.

B. With Aurora, you can create a clone of the production database quickly and efficiently, without the need for time-consuming backup and restore processes. The development team can spin up the staging database on-demand, eliminating delays and allowing them to continue using the staging environment without interruption.

C. Using the standby instance for the staging database would not provide the development team with the ability to use the staging environment without delay. The standby instance is designed for failover purposes and may not be readily available for immediate use.

D. Relying on a backup and restore process using the mysqldump utility would still introduce delays and impact application latency during the data population phase.

upvoted 2 times

 **linux_admin** 12 months ago

Selected Answer: B

With Amazon Aurora MySQL, creating a staging database using database cloning is an easy process. Using database cloning will eliminate the performance issues that occur when a full export is done, and the new database is created. In addition, Amazon Aurora's high availability is provided through Multi-AZ deployment, and read replicas can be used to serve the heavy read traffic without affecting the production database. This solution provides better scalability, elasticity, and availability than the current architecture.

upvoted 4 times

 **alexiscloud** 12 months ago

Answer B:

upvoted 1 times

✉  **bdp123** 1 year, 1 month ago

Selected Answer: B

<https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/>

upvoted 3 times

✉  **john2323** 1 year, 1 month ago

Selected Answer: B

Database cloning is the best answer

upvoted 1 times

✉  **techhb** 1 year, 3 months ago

Selected Answer: B

Database cloning is right answer here.

upvoted 1 times

✉  **career360guru** 1 year, 3 months ago

Option B is right.

You can not access Standby instance for Read in RDS Multi-AZ Deployments.

upvoted 3 times

✉  **aadi7** 1 year, 3 months ago

In a RDS Multi-AZ deployment, you can use the standby instance for read-only purposes, such as running queries and reporting. This is known as a "read replica." You can create one or more read replicas of a DB instance and use them to offload read traffic from the primary instance.

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/>

upvoted 3 times

✉  **aadi7** 1 year, 3 months ago

This is correct, stand by instances cannot be used for read/write and is for failover targets. Read Replicas can be used for that so B is correct.

upvoted 2 times

✉  **333666999** 1 year, 3 months ago

Selected Answer: C

why not C

upvoted 4 times

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

Also the company wants "elasticity and availability" as the question mentioned, so I think this leaves us in the two questions related to Aurora discarding the RDS Mysql solution.

upvoted 1 times

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

Because standby instances are not writable, and at least from my side I occasionally have used the staging database for bug replication. So being able to write might be a thing to consider.

upvoted 1 times

✉  **TTaws** 8 months, 2 weeks ago

You don't need to write anything as they are only pulling the reports. (READ requests)

The Best answer here is C

upvoted 1 times

✉  **DivaLight** 1 year, 4 months ago

Selected Answer: B

Option B

upvoted 1 times

✉  **pSpinelli19** 1 year, 4 months ago

Selected Answer: B

Amazon Aurora Fast Database Cloning is what is required here.

<https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/>

upvoted 1 times

Question #94

Topic 1

A company is designing an application where users upload small files into Amazon S3. After a user uploads a file, the file requires one-time simple processing to transform the data and save the data in JSON format for later analysis. Each file must be processed as quickly as possible after it is uploaded. Demand will vary. On some days, users will upload a high number of files. On other days, users will upload a few files or no files. Which solution meets these requirements with the LEAST operational overhead?

- A. Configure Amazon EMR to read text files from Amazon S3. Run processing scripts to transform the data. Store the resulting JSON file in an Amazon Aurora DB cluster.
- B. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use Amazon EC2 instances to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.
- C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.
- D. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded. Use an AWS Lambda function to consume the event from the stream and process the data. Store the resulting JSON file in an Amazon Aurora DB cluster.

Correct Answer: C

Community vote distribution

C (100%)

✉️  **rjam**  1 year, 4 months ago

Option C
Dynamo DB is a NoSQL-JSON supported
upvoted 13 times

✉️  **rjam** 1 year, 4 months ago

also Use an AWS Lambda - serverless - less operational overhead
upvoted 10 times

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

Selected Answer: C

A. Configuring EMR and an Aurora DB cluster for this use case would introduce unnecessary complexity and operational overhead. EMR is typically used for processing large datasets and running big data frameworks like Apache Spark or Hadoop.
B. While using S3 event notifications and SQS for decoupling is a good approach, using EC2 to process the data would introduce operational overhead in terms of managing and scaling the EC2.
D. Using EventBridge and Kinesis Data Streams for this use case would introduce additional complexity and operational overhead compared to the other options. EventBridge and Kinesis are typically used for real-time streaming and processing of large volumes of data.

In summary, option C is the recommended solution as it provides a serverless and scalable approach for processing uploaded files using S3 event notifications, SQS, and Lambda. It offers low operational overhead, automatic scaling, and efficient handling of varying demand. Storing the resulting JSON file in DynamoDB aligns with the requirement of saving the data for later analysis.
upvoted 7 times

✉️  **TilTil**  6 days, 21 hours ago

Selected Answer: C

B where we use EC2 instances for processing would be ideal in situations where runtime is > 15 minutes. However the question mentions 'simple processing', hence we go for Lambda.
upvoted 1 times

✉️  **awsgeek75** 2 months, 1 week ago

Selected Answer: C

LEAST operational overhead
A: EMR is massive programming effort for this
B: EC2 is considerable overhead
D: Nice solution but why would you use Kinesis as there is no streaming scenario here
C: Simplest and all managed services so least operational overhead compared to other options
upvoted 1 times

✉️  **Ruffyit** 4 months, 4 weeks ago

Option C is the best solution that meets the requirements with the least operational overhead:

Configure Amazon S3 to send event notification to SQS queue

Use Lambda function triggered by SQS to process each file

Store output JSON in DynamoDB

This leverages serverless components like S3, SQS, Lambda, and DynamoDB to provide automated file processing without needing to provision and manage servers.

SQS queues the notifications and Lambda scales automatically to handle spikes and drops in file uploads. No EMR cluster or EC2 Fleet is needed to manage.

upvoted 1 times

Modulopi 5 months, 4 weeks ago

Selected Answer: C

C: Lambdas are made for that

upvoted 1 times

TariqKipkemei 7 months ago

Selected Answer: C

C is best

upvoted 1 times

Guru4Cloud 7 months, 2 weeks ago

Selected Answer: C

Option C is the best solution that meets the requirements with the least operational overhead:

Configure Amazon S3 to send event notification to SQS queue

Use Lambda function triggered by SQS to process each file

Store output JSON in DynamoDB

This leverages serverless components like S3, SQS, Lambda, and DynamoDB to provide automated file processing without needing to provision and manage servers.

SQS queues the notifications and Lambda scales automatically to handle spikes and drops in file uploads. No EMR cluster or EC2 Fleet is needed to manage.

upvoted 1 times

beginnercloud 10 months, 1 week ago

Selected Answer: C

Option C is correct - Dynamo DB is a NoSQL-JSON supported

upvoted 1 times

Abrar2022 10 months, 1 week ago

Selected Answer: C

SQS + LAMDA + JSON >>>>> Dynamo DB

upvoted 1 times

Bmarodi 10 months, 1 week ago

Selected Answer: C

The option C is right answer.

upvoted 1 times

jy190 11 months ago

can someone explain why SQS? it's a poll-based messaging, does it guarantee reacting the event asap?

upvoted 1 times

Zerotn3 1 year, 2 months ago

Selected Answer: C

Dynamo DB is a NoSQL-JSON supported

upvoted 1 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Selected Answer: C

Option C, Configuring Amazon S3 to send an event notification to an Amazon Simple Queue Service (SQS) queue and using an AWS Lambda function to read from the queue and process the data, would likely be the solution with the least operational overhead.

AWS Lambda is a serverless computing service that allows you to run code without the need to provision or manage infrastructure. When a new file is uploaded to Amazon S3, it can trigger an event notification which sends a message to an SQS queue. The Lambda function can then be set up to be triggered by messages in the queue, and it can process the data and store the resulting JSON file in Amazon DynamoDB.

upvoted 3 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Using a serverless solution like AWS Lambda can help to reduce operational overhead because it automatically scales to meet demand and does not require you to provision and manage infrastructure. Additionally, using an SQS queue as a buffer between the S3 event notification and the Lambda function can help to decouple the processing of the data from the uploading of the data, allowing the processing to happen asynchronously and improving the overall efficiency of the system.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C as JSON is supported by DynamoDB. RDS or AuroraDB are not suitable for JSON data.

A - Because this is not a Bigdata analytics usecase.

upvoted 1 times

 **gloritown** 1 year, 3 months ago

Selected Answer: C

CCCCCC

upvoted 1 times

 **AlaN652** 1 year, 3 months ago

Selected Answer: C

Answer C

upvoted 1 times

Question #95

Topic 1

An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.

What should the solutions architect recommend?

- A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
- B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
- C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
- D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Correct Answer: D

Community vote distribution

D (97%)

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

Selected Answer: D

The solutions architect should recommend option D: Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Creating read replicas allows the application to offload read traffic from the source database, improving its performance. The read replicas should be configured with the same compute and storage resources as the source database to ensure that they can handle the read workload effectively.

upvoted 18 times

✉️ **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: D

- A: This will not have any change as you are still reading from same instance as you are writing to
- B: Not possible (<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>)
- C: Why would you do that even if that was possible? No one asked to save on cost
- D: Read replicas are normally for handling read-only traffic

upvoted 2 times

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

Selected Answer: D

In a Multi-AZ deployment, the standby instance is kept in sync with the primary instance and is used for failover purposes only. You cannot read data from the standby instance in a Multi-AZ deployment. If you need to offload read traffic from the primary instance, you can create one or more Read Replicas. Read Replicas are read-only copies of your database that can be used to offload read traffic from the primary instance, which can help improve performance

upvoted 2 times

✉️ **Ruffyt** 4 months, 4 weeks ago

- D. Configuring the read replicas with the same compute and storage resources as the source database ensures that they can handle the read workload efficiently and provide the required performance boost.

upvoted 2 times

✉️ **TariqKipkemei** 7 months ago

Selected Answer: B

Both B and D would work.

Amazon RDS now offers Multi-AZ deployments with readable standby instances (also called Multi-AZ DB cluster deployments). You should consider using Multi-AZ DB cluster deployments with two readable DB instances if you need additional read capacity in your Amazon RDS Multi-AZ deployment and if your application workload has strict transaction latency requirements such as single-digit milliseconds transactions.

<https://aws.amazon.com/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/#:~:text=read%20replicas.,Amazon%20RDS,-now%20offers%20Multi>

upvoted 1 times

✉️ **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: D

The best solution is to create read replicas for the database and configure them with the same compute and storage resources as the source database.

The key requirements are to quickly optimize performance by isolating reads from writes.

Read replicas allow read-only workloads to be directed to one or more replicas of the source RDS instance. This separates reporting or analytics queries from transactional workloads.

The read replicas should have the same compute and storage as the source to provide equivalent performance for reads. Scaling down the replicas would limit read performance.

Using Multi-AZ alone does not achieve read/write separation. The secondary AZ instance is for disaster recovery, not performance.

upvoted 4 times

✉️ **MNotABot** 8 months, 2 weeks ago

Read replica + Same resources as we may need to turn replica to primary in few cases

upvoted 1 times

✉️ **cookieMr** 9 months, 1 week ago

Selected Answer: D

A. In a Multi-AZ deployment, a standby replica of the database is created in a different AZ for high availability and automatic failover purposes. However, serving read requests from the primary AZ alone would not effectively separate read and write traffic. Both read and write traffic would still be directed to the primary database instance, which might not fully optimize performance.

B. The secondary instance in a Multi-AZ deployment is intended for failover and backup purposes, not for actively serving read traffic. It operates in a standby mode and is not optimized for handling read queries efficiently.

C. Configuring the read replicas with half of the compute and storage resources as the source database might not be optimal. It's generally recommended to configure the read replicas with the same compute and storage resources as the source database to ensure they can handle the read workload effectively.

D. Configuring the read replicas with the same compute and storage resources as the source database ensures that they can handle the read workload efficiently and provide the required performance boost.

upvoted 3 times

✉️ **Bmarodi** 10 months, 1 week ago

Selected Answer: D

D meets the requirements.

upvoted 1 times

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

Option C suggests creating read replicas for the database and configuring them with half of the compute and storage resources as the source database. This is a better option as it allows read traffic to be offloaded from the primary database, separating read traffic from write traffic. Configuring the read replicas with half the resources will also save on costs.

upvoted 1 times

✉️ **Charlesleeee** 10 months ago

Err, just curious, what if the production database is 51% full? Your half storage read replica would explode...?

upvoted 4 times

✉️ **Oldman2023** 12 months ago

Can anyone explain why B is not an option?

upvoted 4 times

✉️ **draum010** 12 months ago

CHATGPT says:

To optimize the application's performance and separate read traffic from write traffic, the solutions architect should recommend creating read replicas for the database and configuring them to serve read requests. Option C and D both suggest creating read replicas, but option D is a better choice because it configures the read replicas with the same compute and storage resources as the source database.

Option A and B suggest changing the existing database to a Multi-AZ deployment, which would provide high availability by replicating the database across multiple Availability Zones. However, it would not separate read and write traffic, so it is not the best solution for optimizing application performance in this scenario.

upvoted 4 times

✉️ **caffee** 11 months, 2 weeks ago

Multi-AZ: Synchronous replication occurs, meaning that synchronizing data between DB instances immediately can slow down application's performance. But this method increases High Availability.

Read Replicas: Asynchronous replication occurs, meaning that replicating data in other moments rather than in the writing will maintain application's performance. Although the data won't be HA as Multi-AZ kind of deployment, this method increases Scalability. Good for read heavy workloads.

upvoted 3 times

✉️ **SuketuKohli** 1 year ago

You can create up to 15 read replicas from one DB instance within the same Region. For replication to operate effectively, each read replica should have the same amount of compute and storage resources as the source DB instance. If you scale the source DB instance, also scale the read replicas.

upvoted 2 times

✉️ **dhuno** 10 months, 1 week ago

I think for RDS it is 5 read replicas. 15 is for aurora serverless

upvoted 1 times

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

Selected Answer: D

Option D

upvoted 1 times

✉️  **Wpcorgan** 1 year, 4 months ago

D is correct

upvoted 1 times

✉️  **Nigma** 1 year, 4 months ago

D

<https://www.examtopics.com/discussions/amazon/view/46461-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

✉️  **Hunkie** 1 year, 4 months ago

Selected Answer: D

If you scale the source DB instance, also scale the read replicas.

upvoted 2 times

✉️  **ArielSchivo** 1 year, 5 months ago

Selected Answer: D

D is correct.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html

upvoted 2 times

Question #96

Topic 1

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "10.100.100.0/24"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        }
    ]
}
```

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

Correct Answer: C

Community vote distribution

C (67%)

D (33%)

✉ **Joxtat** 1 year, 2 months ago

What the policy means:

1. Allow termination of any instance if user's source IP address is 10.100.100.254.

2. Deny termination of instances that are not in the us-east-1 Region.

Combining these two, you get: "Allow instance termination in the us-east-1 region if the user's source IP address is 10.100.100.254. Deny termination operation on other regions."

upvoted 53 times

✉ **KMohsoe** 10 months, 2 weeks ago

Nice explanation. Thanks

upvoted 4 times

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

C is correct.

0.0/24, the following five IP addresses are reserved:

0.0: Network address.

0.1: Reserved by AWS for the VPC router.

0.2: Reserved by AWS. The IP address of the DNS server is the base of the VPC network range plus two. ...

0.3: Reserved by AWS for future use.

0.255: Network broadcast address.

upvoted 24 times

✉ **Bmarodi** 10 months, 1 week ago

A good explanation!

upvoted 2 times

 **vip2** Most Recent 1 month, 1 week ago

Selected Answer: C

Clearly the answer is C.

D is 'Deny' 'String NOT equal' == only allow us-east-1

upvoted 3 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: C

Here is how I interpreted this

first part: terminate instance is allowed for the given CIDR block

second part: deny all ec2 actions when region is not us-east-1

so second part is like double negative which means allow for us-east-1 region

You combine both (remember deny always take priority which is why this is written in double negative) and you get:
[allow us-east-region1 to do any action on ec2] when [action is terminate instance and CIDR block is match]

so C is the answer

D is there to confuse you with the double negative

upvoted 1 times

 **pentium75** 3 months ago

Selected Answer: C

Deny takes precedence over Allow. Thus the flow is as follows:

IF region of the EC2 instance is not "us-east-1" -> Deny
ELSE if request is coming from 10.100.100.0/24 -> Allow

ELSE: implicit deny (what is not allowed is denied)

upvoted 3 times

 **Cyberkayu** 3 months, 2 weeks ago

if

IP = 10.100.100.0/24

allow terminate EC2

Else

Deny EC2 termination permission

- with the condition "String NOT equal" to us-east-1

Answer C

upvoted 4 times

 **Bjfikky** 4 months, 1 week ago

Selected Answer: D

The first statement allows users to terminate EC2 instances (ec2:TerminateInstances) from any IP address within the range 10.100.100.0/24. The second statement denies users the ability to perform any EC2 actions (ec2:*) in any region other than us-east-1.

So, the correct interpretation is:

D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254

upvoted 1 times

 **pentium75** 3 months ago

D denies "the ability to perform any actions in any region OTHER than us-east-1". Thus the user CAN terminate instances IN us-east-1. Thus C.

upvoted 1 times

 **sweatheatmn** 5 months ago

Selected Answer: C

C because the explicit deny blocks other regions than us-east-1

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: C

The first statement is a subset of the second statement.

upvoted 1 times

 **prabhjot** 5 months, 3 weeks ago

ans D - This policy denies EC2 instance termination for users with the source IP address 10.100.100.254 in the us-east-1 Region.

upvoted 1 times

 **Subhrangsu** 6 months ago

D is not because of Deny & NOT Equals

upvoted 1 times

 **Valder21** 6 months, 3 weeks ago

I went for C for obvious reasons

Wondering though; this policy also allows to terminate EC2 instances in US-east-1 even if your source IP is not the 10.100.100.254, right? The idea is that since I do not deny this for the other source IP addresses, the Allow action is a obsolete?

upvoted 1 times

 **TariqKipkemei** 7 months ago

Selected Answer: C

Deny all actions on the EC2 instances in the us-east1 region, but let anyone with source IP 10.100.100.254 be able to terminate the EC2 instances.

upvoted 1 times

 **prudhvi08** 7 months, 3 weeks ago

Answer C:

Example 4: Granting access to a specific version of an object

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/amazon-s3-policy-keys.html>

upvoted 1 times

 **RupeC** 8 months, 1 week ago

Selected Answer: D

The effect of the policy is:

D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

The policy allows users to terminate EC2 instances only when their source IP is within the range 10.100.100.0/24.

However, there is a Deny statement that blocks users from terminating any EC2 instance in regions other than us-east-1.

So, when a user tries to terminate an EC2 instance from the IP 10.100.100.254 in the us-east-1 region, the Deny statement will take effect, and the action will be denied. However, if the user tries to terminate an instance from the 10.100.100.0/24 IP range in any region other than us-east-1, the Deny statement will not apply, and the Allow statement will permit the action.

upvoted 5 times

 **JoeGuan** 7 months, 2 weeks ago

The Deny statement 'will not' take effect, because the Deny statement is StringNotEquals to US-East-1. That means that any other region that DOES NOT EQUAL Us-East-1 will be denied, if the region is NOT Us-East-1, then DENY. So Us-East-1 is allowed!

upvoted 3 times

 **Subhrangsu** 6 months ago

oh, ok got it now.

upvoted 1 times

 **MNotABot** 8 months, 2 weeks ago

<https://cidr.xyz/>

upvoted 1 times

 **beginnercloud** 10 months, 1 week ago

Selected Answer: C

Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254. Option C is correct

upvoted 1 times

Question #97

Topic 1

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

- A. Configure Amazon EFS storage and set the Active Directory domain for authentication.
- B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
- C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
- D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Correct Answer: D

Community vote distribution

D (100%)

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

Selected Answer: D

D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Amazon FSx for Windows File Server is a fully managed file storage service that is designed to be used with Microsoft Windows workloads. It is integrated with Active Directory for access control and is highly available, as it stores data across multiple availability zones. Additionally, FSx can be used to migrate data from on-premises Microsoft Windows file servers to the AWS Cloud. This makes it a good fit for the requirements described in the question.

upvoted 20 times

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

Selected Answer: D

A. EFS does not provide native integration with AD for access control. While you can configure EFS to work with AD, it requires additional setup and is not as straightforward as using a dedicated Windows file system like FSx for Windows File Server.

B. It may introduce additional complexity for this use case. Creating an SMB file share using AWS Storage Gateway would require maintaining the gateway and managing the synchronization between on-premises and AWS storage.

C. S3 does not natively provide the SMB file protocol required for MS SharePoint and Windows shared file storage. While it is possible to mount an S3 as a volume using 3rd-party tools or configurations, it is not the recommended.

D. FSx for Windows File Server is a fully managed, highly available file storage service that is compatible with MSWindows shared file storage requirements. It provides native integration with AD, allowing for seamless access control and authentication using existing AD user accounts.

upvoted 6 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>

"When you create a file system with Amazon FSx, you join it to your Active Directory domain to provide user authentication and file- and folder-level access control."

upvoted 1 times

 **Ruffyit** 4 months, 4 weeks ago

D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Amazon FSx for Windows File Server is a fully managed file storage service that is designed to be used with Microsoft Windows workloads. It is integrated with Active Directory for access control and is highly available, as it stores data across multiple availability zones. Additionally, FSx can be used to migrate data from on-premises Microsoft Windows file servers to the AWS Cloud. This makes it a good fit for the requirements described in the question.

upvoted 1 times

 **TariqKipkemei** 7 months ago

Selected Answer: D

Microsoft Windows shared file storage = Amazon FSx for Windows File Server

upvoted 2 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: D

The best solution that satisfies the requirements is D) Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

The key requirements are:

Shared Windows file storage for SharePoint

High availability

Integrated Active Directory authentication

upvoted 1 times

✉ **cheese929** 11 months ago

Selected Answer: D

D is correct. FSx is for windows and supports AD authentication

upvoted 1 times

✉ **kakka22** 11 months, 1 week ago

Why not B? Migrating the workload? Maybe is needed a hybrid cloud solution

upvoted 1 times

✉ **gx2222** 11 months, 3 weeks ago

Selected Answer: D

One solution that can satisfy the mentioned requirements is to use Amazon FSx for Windows File Server. Amazon FSx is a fully managed service that provides highly available and scalable file storage for Windows-based applications. It is designed to be fully integrated with Active Directory, which allows you to use your existing domain users and groups to control access to your file shares.

Amazon FSx provides the ability to migrate data from on-premises file servers to the cloud, using tools like AWS DataSync, Robocopy or PowerShell. Once the data is migrated, you can continue to use the same tools and processes to manage and access the file shares as you would on-premises.

Amazon FSx also provides features such as automatic backups, data encryption, and native multi-Availability Zone (AZ) deployments for high availability. It can be easily integrated with other AWS services, such as Amazon S3, Amazon EFS, and AWS Backup, for additional functionality and backup options.

upvoted 2 times

✉ **psr83** 1 year, 3 months ago

Selected Answer: D

FSx is for Windows

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

✉ **xeun88** 1 year, 3 months ago

I'm going for D as the answer because FSx is compatible with windows

upvoted 1 times

✉ **kajal1206** 1 year, 3 months ago

Selected Answer: D

Answer is D

upvoted 1 times

✉ **Wpcorgan** 1 year, 4 months ago

D is correct

upvoted 1 times

✉ **TonyghostR05** 1 year, 4 months ago

Windows only available for using FSx

upvoted 3 times

✉ **Nigma** 1 year, 4 months ago

D. Windows is the keyword

<https://www.examtopics.com/discussions/amazon/view/29780-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

✉ **Nigma** 1 year, 4 months ago

EFS is for Linux

FSx is for Windows

upvoted 6 times

✉ **Hunkie** 1 year, 4 months ago

Selected Answer: D

DDDDDDDD

upvoted 1 times

Question #98

Topic 1

An image-processing company has a web application that users use to upload images. The application uploads the images into an Amazon S3 bucket. The company has set up S3 event notifications to publish the object creation events to an Amazon Simple Queue Service (Amazon SQS) standard queue. The SQS queue serves as the event source for an AWS Lambda function that processes the images and sends the results to users through email.

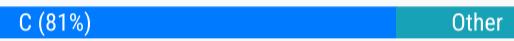
Users report that they are receiving multiple email messages for every uploaded image. A solutions architect determines that SQS messages are invoking the Lambda function more than once, resulting in multiple email messages.

What should the solutions architect do to resolve this issue with the LEAST operational overhead?

- A. Set up long polling in the SQS queue by increasing the ReceiveMessage wait time to 30 seconds.
- B. Change the SQS standard queue to an SQS FIFO queue. Use the message deduplication ID to discard duplicate messages.
- C. Increase the visibility timeout in the SQS queue to a value that is greater than the total of the function timeout and the batch window timeout.
- D. Modify the Lambda function to delete each message from the SQS queue immediately after the message is read before processing.

Correct Answer: A

Community vote distribution



✉ **Six_Fingered_Jose** 1 year, 5 months ago

Selected Answer: C

answer should be C,
users get duplicated messages because -> lambda polls the message, and starts processing the message.
However, before the first lambda can finish processing the message, the visibility timeout runs out on SQS, and SQS returns the message to the poll, causing another Lambda node to process that same message.
By increasing the visibility timeout, it should prevent SQS from returning a message back to the poll before Lambda can finish processing the message

upvoted 49 times

✉ **Ello2023** 1 year, 2 months ago

I am confused. If the email has been sent many times already why would they need more time?
I believe SQS Queue Fifo will keep in order and any duplicates with same ID will be deleted. Can you tell me where i am going wrong? Thanks
upvoted 4 times

✉ **Robrobtutu** 11 months, 2 weeks ago

Increasing the visibility timeout would give time to the lambda function to finish processing the message, which would make it disappear from the queue, and therefore only one email would be send to the user.
If the visibility timeout ends while the lambda function is still processing the message, the message will be returned to the queue and there another lambda function would pick it up and process it again, which would result in the user receiving two or more emails about the same thing.

upvoted 4 times

✉ **aadityaravi8** 9 months ago

I agree with your answer explanation
upvoted 1 times

✉ **Abdou1604** 7 months, 2 weeks ago

i agree because the issue is multiple received email for an image uploaded
upvoted 1 times

✉ **MrAWS** 1 year, 2 months ago

I tend to agree with you. See my comments above.
upvoted 2 times

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

I agree it seems solution is C, as thought the SQS FIFO makes sense deduplication id would make NO sense as the system who put messages in the queue is S3 events; and as far as I know S3 do not send duplicated events. Also, the question mention that users are complaining about receiving multiple emails for each email, which is different to say they are receiving occasionally a repeated email; so my guess is SQS FIFO is not needed.

upvoted 1 times

✉ **JoeGuan** 7 months, 2 weeks ago

The FIFO SQS is for solving a different problem, where items in the queue require order. You cannot simply switch from a standard queue to fifo queue. Duplicate emails are a common issue with a standard queue. The documentation consistently reminds us that duplicate emails can occur, and the solution is not to create a FIFO queue, but rather adjust the configuration parameters accordingly.

upvoted 3 times

 **PLN6302** 7 months ago

amazon s3 doesn't support fifo queues

upvoted 2 times

 **brushek**  1 year, 5 months ago

Selected Answer: C

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

this is important part:

Immediately after a message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The minimum is 0 seconds. The maximum is 12 hours.

upvoted 15 times

 **Uzbekistan**  4 days, 3 hours ago

Selected Answer: B

Given the requirement to resolve the issue of multiple email messages being sent to users with the least operational overhead, the most appropriate solution is:

B. Change the SQS standard queue to an SQS FIFO queue. Use the message deduplication ID to discard duplicate messages.

Explanation:

SQS FIFO Queue: FIFO (First-In-First-Out) queues in SQS ensure that the order in which messages are sent and received is strictly preserved and that each message is processed only once. By switching to an SQS FIFO queue, you can prevent the Lambda function from processing duplicate messages.

upvoted 1 times

 **vip2** 1 month, 1 week ago

Selected Answer: C

'Visibility Timeout' is suitable(better) solution to solve the issue.

upvoted 1 times

 **shwelin** 1 month, 1 week ago

I will stick with "B", the correct answer.

upvoted 2 times

 **0xE8D4A51000** 2 months, 1 week ago

Selected Answer: B

All answers are wrong, the answer B

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: C

In this setup the only way to get multiple emails is when same image is processed multiple times. This only happens when another Lambda starts processing while the previous one hasn't finished processing.

Increasing the SQS queue timeout to be greater than Lambda timeout will ensure that other Lambda can't see the SQS message before previous Lambda finishes processing or times out.

So C is best answer

A: Long polling won't fix anything

B: FIFO is nice idea but how will the Lambda function know it has got a duplicate message?

D: Wrong as in case of Lambda timeout that message is lost without being processed

upvoted 1 times

 **Ruffyit** 4 months, 4 weeks ago

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

this is important part:

Immediately after a message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The minimum is 0 seconds. The maximum is 12 hours

upvoted 3 times

 **lqw** 5 months, 2 weeks ago

Selected Answer: C

least operational overheads

upvoted 1 times

 **prabhjot** 5 months, 3 weeks ago

ans B - Option A (long polling), Option C (increasing visibility timeout), and Option D (deleting messages immediately) do not address the root cause of the problem, which is the duplication of messages in the queue.

upvoted 2 times

 **vijaykamal** 6 months ago

Long polling is incorrect...it just means that SQS queue is connected after specific interval instead of looking for messages in queue in very short interval...long polling saves money but does not help to remove duplicate.

Correct Answer: C

upvoted 1 times

 **hieulam** 6 months, 1 week ago

Selected Answer: A

I think A is correct.

<https://aws.amazon.com/blogs/developer/polling-messages-from-a-amazon-sqs-queue/#:~:text=When%20disabling,more%20API%20calls>.

upvoted 1 times

 **kwang312** 7 months ago

D is an incorrect answer because Lambda automatically deletes message from the queue when finish process

upvoted 1 times

 **TariqKipkemei** 7 months ago

Selected Answer: C

Immediately after a message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents all consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The minimum is 0 seconds. The maximum is 12 hours.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html#:~:text=SQS%20sets%20a-,visibility%20timeout,-%2C%20a%20period%20of>

upvoted 1 times

 **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

I would go with the C.

upvoted 1 times

 **Olaunfazed** 9 months ago

Answer is B.

B. Change the SQS standard queue to an SQS FIFO queue. Use the message deduplication ID to discard duplicate messages.

By changing the SQS standard queue to an SQS FIFO (First-In-First-Out) queue, you can ensure that messages are processed in the order they are received and that each message is processed only once. FIFO queues provide exactly-once processing and eliminate duplicates.

Using the message deduplication ID feature of SQS FIFO queues, you can assign a unique identifier (such as the S3 object key) to each message. SQS will check the deduplication ID of incoming messages and discard duplicate messages with the same deduplication ID. This ensures that only unique messages are processed by the Lambda function.

This solution requires minimal operational overhead as it mainly involves changing the queue type and using the deduplication ID feature, without requiring modifications to the Lambda function or adjusting timeouts.

upvoted 4 times

 **dangvanduc90** 6 months, 2 weeks ago

compare with C, SQS FIFO must take time than C, B is important when you concern about ordering

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

A. Long polling doesn't directly address the issue of multiple invocations of the Lambda for the same message. Increasing the ReceiveMessage may not completely prevent duplicate invocations.

B. Changing the queue type from standard to FIFO requires additional considerations and changes to the application architecture. It may involve modifying the event configuration and handling message deduplication IDs, which can introduce operational overhead.

D. Deleting messages immediately after reading them may lead to message loss if the Lambda encounters an error or fails to process the image successfully. It does not guarantee message processing and can result in data loss.

C. By setting the visibility timeout to a value greater than the total time required for the Lambda to process the image and send the email, you ensure that the message is not made visible to other consumers during processing. This prevents duplicate invocations of the Lambda for the same message.

upvoted 2 times

Question #99

Topic 1

A company is implementing a shared storage solution for a gaming application that is hosted in an on-premises data center. The company needs the ability to use Lustre clients to access data. The solution must be fully managed.

Which solution meets these requirements?

- A. Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- B. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- C. Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: D

Community vote distribution



123jh10 Highly Voted 1 year, 5 months ago

Selected Answer: D

Answer is D.

Lustre in the question is only available as FSx

<https://aws.amazon.com/fsx/lustre/>

upvoted 25 times

Buruguduystunstugudunstuy Highly Voted 1 year, 3 months ago

Selected Answer: D

Option D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Amazon FSx for Lustre is a fully managed file system that is designed for high-performance workloads, such as gaming applications. It provides a high-performance, scalable, and fully managed file system that is optimized for Lustre clients, and it is fully integrated with Amazon EC2. It is the only option that meets the requirements of being fully managed and able to support Lustre clients.

upvoted 12 times

awsgeek75 Most Recent 2 months, 1 week ago

Selected Answer: D

D: Lustre is key requirement

AB: No support for Lustre

C: Cannot just configure EFS to support Lustre file system

upvoted 1 times

Ruffyt 4 months, 4 weeks ago

Option D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Amazon FSx for Lustre is a fully managed file system that is designed for high-performance workloads, such as gaming applications. It provides a high-performance, scalable, and fully managed file system that is optimized for Lustre clients, and it is fully integrated with Amazon EC2. It is the only option that meets the requirements of being fully managed and able to support Lustre clients.

upvoted 1 times

TariqKipkemei 7 months ago

Selected Answer: D

Lustre clients = Amazon FSx for Lustre file system

upvoted 1 times

Guru4Cloud 7 months, 2 weeks ago

Selected Answer: D

The correct solution is D) Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

The key requirements are:

Shared storage solution

Support Lustre clients

Fully managed service

Amazon FSx for Lustre provides a fully managed file system that is optimized for Lustre workloads. It allows Lustre clients to seamlessly connect to the file system.

upvoted 2 times

 **RupeC** 8 months, 1 week ago

Selected Answer: A

Sorry, but I disagree with everyone. The question states "a gaming application that is hosted in an on-premises data center". Option D does not address this and cannot to my knowledge address it. Thus:

A. Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.

By using AWS Storage Gateway in file gateway mode, you can extend your on-premises data center storage into the AWS cloud. The file share created on AWS Storage Gateway can use the necessary client protocol (such as Lustre), which would allow the Lustre clients in your on-premises data center to access the data stored on AWS Storage Gateway.

This solution enables you to use Lustre clients to access data, while still keeping the gaming application hosted in your on-premises data center. AWS Storage Gateway provides a fully managed solution for this hybrid scenario, allowing seamless integration between on-premises and AWS cloud storage.

upvoted 4 times

 **David_Ang** 5 months, 3 weeks ago

mate if you have an aws service that is meant to be used for this task, there is simply not discussion, is more simple, is more cheap and better option

upvoted 1 times

 **JoeGuan** 7 months, 2 weeks ago

So, I think that the FSx File Gateway is currently only available for Windows? I don't think Lustre is part of this offering yet as of 8/8/2023

upvoted 1 times

 **pentium75** 3 months ago

"The file share created on AWS Storage Gateway can use the necessary client protocol (such as Lustre)", no it can use only NFS or SMB. But NOT Lustre.

upvoted 2 times

 **james2033** 8 months, 2 weeks ago

Selected Answer: D

Content of "Amazon FSx for Lustre" at this link <https://aws.amazon.com/fsx/lustre/>. Focus at image, section: "On-premises clients".

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: D

A. Lustre client access is not supported by AWS Storage Gateway file gateway.

B. Creating a Windows file share on an EC2 Windows instance is suitable for Windows-based file sharing, but it does not provide the required Lustre client access. Lustre is a high-performance parallel file system primarily used in high-performance computing (HPC) environments.

C. EFS does not natively support Lustre client access. Although EFS is a managed file storage service, it is designed for general-purpose file storage and is not optimized for Lustre workloads.

D. Amazon FSx for Lustre is a fully managed file system optimized for high-performance computing workloads, including Lustre clients. It provides the ability to use Lustre clients to access data in a managed and scalable manner. By choosing this option, the company can benefit from the performance and manageability of Amazon FSx for Lustre while meeting the requirement of Lustre client access.

upvoted 2 times

 **Musti35** 11 months, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/fsx/lustre/>?
nc1=h_ls#:~:text=Amazon%20FSx%20for%20Lustre%20provides%20fully%20managed%20shared%20storage%20with%20the%20scalability%20and%20performance%20of%20the%20popular%20Lustre%20file%20system.

upvoted 1 times

 **jdr75** 11 months, 3 weeks ago

Selected Answer: D

Option D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

BUT the onprem server couldn't view and have good perf with the EFS, so the question is an absurd !

upvoted 1 times

 **fkie4** 1 year ago

Selected Answer: D

seriously? it spells out "Lustre" for you

upvoted 1 times

 **CaoMengde09** 1 year, 1 month ago

D is the most logical solution. But still the app is OnPrem so AWS Fx for Lustre is not enough to connect the storage to the app, we'll need a File Gateway to use with the FSx Lustre

upvoted 2 times

 **Chalamalli** 1 year, 1 month ago

D is correct

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

D is correct

upvoted 1 times

Question #100

Topic 1

A company's containerized application runs on an Amazon EC2 instance. The application needs to download security certificates before it can communicate with other business applications. The company wants a highly secure solution to encrypt and decrypt the certificates in near real time. The solution also needs to store data in highly available storage after the data is encrypted.

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

- A. Create AWS Secrets Manager secrets for encrypted certificates. Manually update the certificates as needed. Control access to the data by using fine-grained IAM access.
- B. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operations. Store the function in an Amazon S3 bucket.
- C. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon S3.
- D. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

Correct Answer: D

Community vote distribution



✉️ **Chunslı** 1 year, 5 months ago

C makes a better sense. Between C (S3) and D (EBS), S3 is highly available with LEAST operational overhead.
upvoted 41 times

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

Agree, also the data in EBS will be accessible only to the EC2 instance and that is not as available as S3 would be.
upvoted 4 times

✉️ **MXB05** 1 year, 5 months ago

Selected Answer: C

Correct Answer is C: EBS is not highly available
upvoted 20 times

✉️ **FNJ1111** 1 year, 2 months ago

Per AWS: "Amazon EBS volumes are designed to be highly available, reliable, and durable"

<https://aws.amazon.com/ebs/features/>
upvoted 2 times

✉️ **Ello2023** 1 year, 2 months ago

EBS is Highly Available as it stores in multi AZ and S3 is regional.
upvoted 1 times

✉️ **oguz11** 1 year, 2 months ago

EBS also has Multi-AZ capability, but it does not replicate the data across multiple availability zones by default. When Multi-AZ is enabled, it creates a replica of the EBS volume in a different availability zone and automatically failover to the replica in case of a failure. However, this requires additional configuration and management. In comparison, Amazon S3 automatically replicates data across multiple availability zones without any additional configuration. Therefore, storing the data on Amazon S3 provides a simpler and more efficient solution for high availability.
upvoted 9 times

✉️ **dkw2342** 3 weeks, 4 days ago

This is false. There is no AWS-provided functionality that will replicate EBS volumes across AZs. There are 3rd-party solutions to this, but that's not what's being asked here.

EBS is only replicated WITHIN an AZ by default.
upvoted 1 times

✉️ **pentium75** 3 months ago

S3 is also highly available. Within the region, but still. Multi-AZ = HA.
upvoted 2 times

✉️ **JayBee65** 1 year, 3 months ago

Yes it is!
upvoted 1 times

 **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: C

The language is confusing over here so I'm going by process of elimination

A: Wrong because manual operation and fine grained IAM is overhead

B: What?

D: Between C and D S3 is more HA than EFS so C wins

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Sorry meant EBS, not EFS for D

D: Between C and D, S3 is more HA than EBS. So C wins

upvoted 1 times

 **ignajtolandstrong** 2 months, 4 weeks ago

Selected Answer: D

I would select D.

you can mount a single Amazon Elastic Block Store (EBS) volume to multiple Docker containers running on the same Amazon Elastic Compute Cloud (EC2) instance.

you can store data from a container running on Amazon Elastic Compute Cloud (EC2) to an Amazon Simple Storage Service (S3) bucket. One way to do this is to use the aws s3 cp command in the command line of the EC2 instance.

upvoted 1 times

 **pentium75** 3 months ago

Selected Answer: C

A - does not mention storing the encrypted data at all (though that is a requirement), also involves manual action which is surely NOT "least operational effort"

B - Doesn't make any sense

C - Yes, S3 meets the requirements and is easy to access from containerized app

D - EBS volumes are mounted to the container host, but data is created on containers

upvoted 2 times

 **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: A

A is OK

secrets manager:

- is highly available

- you can store custom secrets in it like certificate

- automatically encrypts secrets at rest, and can be configured for encryption in transit

- downloading certificate from it is less operational overhead than decrypting it manually with KMS key

arguments against it that this is more manual than C and D? this manual step is necessary measure and can't be omitted in other options

C and D have this "store the encrypted data in..." to store encrypted certificate you have to: log in to instance, get kms key, get certificate, encrypt it, and load that data this is more operational overhead

upvoted 1 times

 **pentium75** 3 months ago

"Least operational overhead" and "manually" (as in A) usually don't go together. Also, A does not say anything about storing the data (which is a requirement).

"C and D have this 'store the encrypted data in'" yes, exactly, the encrypted data, NOT the certificate. You encrypt data with the certificate, and you want to store THAT encrypted data.

upvoted 2 times

 **David_Ang** 5 months, 3 weeks ago

Selected Answer: C

"C" is more correct because S3 is more efficient and cheaper to store data like certificates, like this case. Also Option D involves using Amazon Elastic Block Store (Amazon EBS) volumes, which is not typically used for storing certificates and may introduce unnecessary complexity and operational overhead.

upvoted 1 times

 **Abitek007** 5 months, 3 weeks ago

confused between EBS and S3, both are HA, but location?

upvoted 1 times

 **joshik** 6 months ago

C. when it comes to availability, Amazon S3 is generally more highly available than Amazon EBS because S3 replicates data across multiple AZs by default, providing greater resilience to failures. However, the choice between S3 and EBS depends on your specific use case and whether you need block storage for EC2 instances (EBS) or object storage for storing and retrieving data (S3).

upvoted 1 times

 **Ramdi1** 6 months, 2 weeks ago

Selected Answer: D

I selected D, even though S3 has high availability to 11 9's. The question started with EC2 Instance. EBS provides block level storage that is attached to EC2 Instances. They are also designed for High Availability.

upvoted 1 times

✉ **Guru4Cloud** 7 months, 2 weeks ago

Selected Answer: C

Option C is the best solution that meets all the requirements with the least operational overhead:

Use AWS KMS customer managed key for encryption
Allow EC2 instance role access to use the KMS key
Store encrypted data in Amazon S3

upvoted 1 times

✉ **mr_D3v1n3** 8 months ago

All data within EBS is stored in equally sized blocks. This system offers some performance advantages over traditional storage, and generally boasts lower latency, too. This would meet the near real time requirement over the S3 option

upvoted 1 times

✉ **james2033** 8 months, 2 weeks ago

Selected Answer: C

A: Missing encrypt/decrypt process. B: "Store the function in an Amazon S3 bucket" made meaningless. D: Amazon Elastic Block Store (Amazon EBS) for clone all of hard disk, CD/DVD. The context of question requires near real-time, it need save small parts, not a big part. --> Choose C (with S3, AWS Key Management Service - AWS KMS).

See <https://docs.aws.amazon.com/kms/index.html> . Decrypt process https://docs.aws.amazon.com/latest/APIReference/API_Decrypt.html .

upvoted 1 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: C

- A. Manual - no no no!
- B. External (python) library - no no no!
- C. yeap.
- D. S3 over EBS (see answer C)

upvoted 3 times

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

I will go for D, as mentioned in the question ' an EC2 instance' , ' near real-time' , 'LEAST operational overhead' all refer to EBS rather than S3.

upvoted 3 times

✉ **jaswantn** 1 month, 2 weeks ago

near real time is the key that goes with EBS if we compare with S3 in this situation.

upvoted 1 times

✉ **bgsanata** 10 months, 2 weeks ago

The correct answer is D...

Using a containerized applications in EC2 mean it's easier to use EBS. S3 require extra work to be done and the question is about Least operational overhead.

upvoted 1 times

✉ **studynoplay** 10 months, 3 weeks ago

Selected Answer: C

The moment you see storage, think S3. It is default unless there is a very specific requirement where S3 does not fit which will be explicitly described in the question

upvoted 2 times

Question #101

Topic 1

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable Internet access for the private subnets?

- A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
- B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
- C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
- D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress-only Internet gateway.

Correct Answer: A

Community vote distribution

A (97%)

✉ **Gil80** 1 year, 4 months ago

Selected Answer: A

NAT Instances - OUTDATED BUT CAN STILL APPEAR IN THE EXAM!

However, given that A provides the newer option of NAT Gateway, then A is the correct answer.

B would be correct if NAT Gateway wasn't an option.

upvoted 12 times

✉ **Shrestwt** 11 months, 1 week ago

NAT instance or NAT Gateway always created in public subnet to provide internet access to private subnet. In option B. they are creating NAT Instance in private subnet which is not correct.

upvoted 13 times

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

Selected Answer: A

The correct answer is option A.

To enable Internet access for the private subnets, the solutions architect should create three NAT gateways, one for each public subnet in each Availability Zone (AZ). NAT gateways allow private instances to initiate outbound traffic to the Internet but do not allow inbound traffic from the Internet to reach the private instances.

The solutions architect should then create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ. This will allow instances in the private subnets to access the Internet through the NAT gateways in the public subnets.

upvoted 6 times

✉ **ronin201** 4 months, 4 weeks ago

in Azure there is 1 NAT GW multi AZ, 1 per network, I think this is example for AWS to change

upvoted 1 times

✉ **pentium75** 3 months ago

But in AWS a NAT GW is attached to a subnet, and a subnet resides in a single AZ. Can't create multi-AZ NAT GW without changing whole architecture. You CAN use one NAT GW from multiple subnets in multiple AZs I think, but then it would not be HA.

upvoted 1 times

✉ **Ruffyit** 4 months, 4 weeks ago

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-example-private-subnets-nat.html>

upvoted 2 times

✉ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

The best solution is to create a NAT gateway in each public subnet (one per availability zone), and update the route tables for the private subnets to send internet traffic to the NAT gateway.

NAT gateways allow private subnets to access the internet for things like software updates, without exposing those instances directly to the

internet. An egress-only internet gateway would allow outbound access, but also allow inbound internet traffic, which is not desired for the private subnets.

upvoted 3 times

 **james2033** 8 months, 1 week ago

Selected Answer: A

"Egress" means outbound connection, remove D. "Second gateway", remove C.

Now has only A and B. The difference between A versus B is "1 NAT gateway, 1 for public subnet in each AZ" (A) and "1 NAT gateway, 1 for private subnet in each AZ" (B).

Choose A.

upvoted 3 times

 **cookieMr** 9 months, 1 week ago

By creating a NAT gateway in each public subnet, the private subnets can route their Internet-bound traffic through the NAT gateways. This allows EC2 in the private subnets to download software updates and access other resources on the Internet.

Additionally, a separate private route table should be created for each AZ. The private route tables should have a default route that forwards non-VPC traffic (0.0.0.0/0) to the corresponding NAT gateway in the same AZ. This ensures that the private subnets use the appropriate NAT gateway for Internet access.

B is incorrect because NAT instances require manual management and configuration compared to NAT gateways, which are a fully managed service. NAT instances are also being deprecated in favor of NAT gateways.

C is incorrect because creating a second internet gateway on a private subnet is not a valid solution. Internet gateways are associated with public subnets and cannot be directly associated with private subnets.

D is incorrect because egress-only internet gateways are used for IPv6 traffic.

upvoted 5 times

 **Jeeva28** 10 months ago

NAT Gateway will be created Public Subnet and Provide access to Private Subnet

upvoted 1 times

 **cheese929** 11 months ago

Selected Answer: A

A is correct.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-example-private-subnets-nat.html>

upvoted 2 times

 **Heric** 11 months, 1 week ago

Selected Answer: A

Now NAT Instances is avoided by AWS. Then choose the NAT Gateway

upvoted 3 times

 **alexiscloud** 12 months ago

A: NAT Gateway

upvoted 1 times

 **Rudraman** 1 year ago

Selected Answer: A

NAT Gateway - AWS-managed NAT, higher bandwidth, high availability, no administration

upvoted 1 times

 **RODCCN** 1 year ago

You should create 3 NAT gateways, but not in the public subnet. So, even NAT instance is already deprecated, is the right answer in this case, since it's relate to create in a private subnet, not public.

upvoted 2 times

 **Ben2008** 1 year ago

Refer:

<https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-scenarios.html#public-nat-gateway-overview>

Should be A.

upvoted 2 times

 **erik29** 1 year, 2 months ago

aaaaaa

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: A

Networking 101, A is only right option

upvoted 2 times

 **career360guru** 1 year, 3 months ago

Option A

NAT gateway needs to be configured within each VPC's in Public Subnet.

upvoted 1 times

Question #102

Topic 1

A company wants to migrate an on-premises data center to AWS. The data center hosts an SFTP server that stores its data on an NFS-based file system. The server holds 200 GB of data that needs to be transferred. The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system.

Which combination of steps should a solutions architect take to automate this task? (Choose two.)

- A. Launch the EC2 instance into the same Availability Zone as the EFS file system.
- B. Install an AWS DataSync agent in the on-premises data center.
- C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for the data.
- D. Manually use an operating system copy command to push the data to the EC2 instance.
- E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

Correct Answer: AB

Community vote distribution



✉️ **123jh10** 1 year, 5 months ago

Selected Answer: AB

A. Launch the EC2 instance into the same Availability Zone as the EFS file system.
 Makes sense to have the instance in the same AZ the EFS storage is.
 B. Install an AWS DataSync agent in the on-premises data center.
 The DataSync will move the data to the EFS, which already uses the EC2 instance (see the info provided). No more things are required...
 C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for the data.
 This secondary EBS volume isn't required... the data should be moved on to EFS...
 D. Manually use an operating system copy command to push the data to the EC2 instance.
 Potentially possible (instead of A), BUT the "automate this task" premise goes against any "manually" action. So, we should keep A.
 E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.
 I don't get the relationship between DataSync and the configuration for SFTP "on-prem"! Nonsense.
 So, answers are A&B

upvoted 50 times

✉️ **RBSK** 1 year, 3 months ago

will A,B work without E?

upvoted 3 times

✉️ **Lalo** 1 year, 1 month ago

CORRECT ANSWER: B&E

Steps 4 &5

https://aws.amazon.com/datasync/getting-started/?nc1=h_ls

upvoted 13 times

✉️ **Cizzla7049** 1 year, 4 months ago

E is correct

<https://aws.amazon.com/blogs/storage/migrating-storage-with-aws-datasync/>

upvoted 4 times

✉️ **happpiee** 3 weeks, 6 days ago

Use AWS Transfer Family instead of DataSync for SFTP. So E seems incorrect.

When do I use AWS DataSync and when do I use AWS Transfer Family?

A: If you currently use SFTP to exchange data with third parties, AWS Transfer Family provides a fully managed SFTP, FTPS, FTP, and AS2 transfer directly into and out of Amazon S3, while reducing your operational burden.

If you want an accelerated and automated data transfer between NFS servers, SMB file shares, Hadoop clusters, self-managed or cloud object storage, AWS Snowcone, Amazon S3, Amazon EFS, and Amazon FSx, you can use AWS DataSync. DataSync is ideal for customers who need online migrations for active data sets, timely transfers for continuously generated data, or replication for business continuity.

upvoted 1 times

✉️ **Iconique** 6 months ago

Just go to AWS Console, to DataSync and choose "Create Location Configuration". Locations configurations are endpoints used in DataSync task. A location can be the source endpoint of the task, e.g. a NFS on-premise filesystem. So E is helping in the automation process. A is not even part of this automation process, it is a solution already agreed to have EC2 with EFS, how you connect EC2 to EFS is not part of the solution!

upvoted 3 times

 **Buruguduystunstugudunstuy**  1 year, 3 months ago

Selected Answer: BE

Answer and HOW-TO

- B. Install an AWS DataSync agent in the on-premises data center.
- E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

To automate the process of transferring the data from the on-premises SFTP server to an EC2 instance with an EFS file system, you can use AWS DataSync. AWS DataSync is a fully managed data transfer service that simplifies, automates, and accelerates transferring data between on-premises storage systems and Amazon S3, Amazon EFS, or Amazon FSx for Windows File Server.

To use AWS DataSync for this task, you should first install an AWS DataSync agent in the on-premises data center. This agent is a lightweight software application that you install on your on-premises data source. The agent communicates with the AWS DataSync service to transfer data between the data source and target locations.

upvoted 44 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Next, you should use AWS DataSync to create a suitable location configuration for the on-premises SFTP server. A location represents a data source or a data destination in an AWS DataSync task. You can create a location for the on-premises SFTP server by specifying the IP address, the path to the data, and the necessary credentials to access the data.

Once you have created the location configuration for the on-premises SFTP server, you can use AWS DataSync to transfer the data to the EC2 instance with the EFS file system. AWS DataSync handles the data transfer process automatically and efficiently, transferring the data at high speeds and minimizing downtime.

upvoted 15 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Explanation of other options

- A. Launch the EC2 instance into the same Availability Zone as the EFS file system.

This option is not wrong, but it is not directly related to automating the process of transferring the data from the on-premises SFTP server to the EC2 instance with the EFS file system. Launching the EC2 instance into the same Availability Zone as the EFS file system can improve the performance and reliability of the file system, as it reduces the latency between the EC2 instance and the file system. However, it is not necessary for automating the data transfer process.

upvoted 9 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

- C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for the data.

This option is incorrect because Amazon EBS is a block-level storage service that is designed for use with Amazon EC2 instances. It is not suitable for storing large amounts of data that need to be accessed by multiple EC2 instances, like in the case of the NFS-based file system on the on-premises SFTP server. Instead, you should use Amazon EFS, which is a fully managed, scalable, and distributed file system that can be accessed by multiple EC2 instances concurrently.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

- D. Manually use an operating system copy command to push the data to the EC2 instance.

This option is not wrong, but it is not the most efficient or automated way to transfer the data from the on-premises SFTP server to the EC2 instance with the EFS file system. Manually transferring the data using an operating system copy command would require manual intervention and would not scale well for large amounts of data. It would also not provide the same level of performance and reliability as a fully managed service like AWS DataSync.

upvoted 3 times

 **Risin42**  4 weeks ago

Selected Answer: AB

AWS DataSync does not support SFTP

upvoted 1 times

 **Ikki77** 4 weeks, 1 day ago

Selected Answer: AE

The most appropriate combination of steps to automate the task of migrating the on-premises SFTP server to an Amazon EC2 instance using Amazon EFS is:

- A. Launch the EC2 instance into the same Availability Zone as the EFS file system.
- E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

Explanation:

A. Launching the EC2 instance into the same Availability Zone as the EFS file system ensures optimal performance and low-latency access to the file system.

E. AWS DataSync can be used to automate and accelerate the transfer of data between on-premises systems and AWS. Creating a suitable location configuration for the on-premises SFTP server with AWS DataSync facilitates the migration process.

Therefore, options A and E together provide an efficient and automated approach to migrate the data.

upvoted 1 times

 **nntuan** 1 month ago

My choice is B and E.

Data Sync is used to transfer data between on-premises and AWS. It is required to deploy AWS Data Sync Agent in on-premises and configure the location FROM/TO in AWS Data Sync.

upvoted 1 times

 **app12** 2 months, 1 week ago

Apparently it's not B, as it says:

"Install" an AWS DataSync agent in the on-premises data center.

You actually don't install it.

You deploy it as a vm or EC2.

So I guess it's the terminology that hints at "E"

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

The question is confusing and misleading!!!

This part of question remains unanswered: "The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system" and A doesn't actually make sense. BE doesn't fulfil this requirement. AB doesn't work without a location.

I think something is missing in the dump

upvoted 1 times

 **data_cloud_aws** 2 months, 2 weeks ago

Selected Answer: BE

It's already given EC2 with EFS opted for the solution.

Which combination of steps should a solutions architect take to automate this task?

BE

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Are you saying the question is about automating the transfer and not migrating the SFTP server?

upvoted 1 times

 **Priyapani** 2 months, 2 weeks ago

Correct answer BE

A is not correct. EFS is region specific not AZ

upvoted 1 times

 **SaurabhTiwari1** 3 months, 1 week ago

Selected Answer: BE

BE is correct

upvoted 1 times

 **djgodzilla** 3 months, 1 week ago

Selected Answer: AB

Data Sync is agent based solution that allows to transfer between on-premises NFS/SMB shares and AWS, between AWS storage services and between different Clouds. it supports EFS,S3, and Fsx.. it requires an agent installation on-prem

upvoted 1 times

 **Cyberkayu** 3 months, 2 weeks ago

A because the statement in the question "The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system."

B answer is explained in every comment

upvoted 1 times

 **MiniYang** 4 months ago

Selected Answer: AE

Installing the AWS DataSync agent on the local data center, although it can be an efficient way, may be regarded as wasteful in this case, because the SFTP server already has a secure transport method, and DataSync is mainly used to simplify Data transfer in cross-domain transfer environment (local data center to AWS)Installing the AWS DataSync agent on the local data center, although it can be an efficient way, may be regarded as wasteful in this case, because the SFTP server already has a secure transport method, and DataSync is mainly used to simplify Data transfer in cross-domain transfer environment (local data center to AWS) and A. This ensures that EC2 instances and EFS file systems run in the same Availability Zone to maximize performance and reduce latency.

upvoted 3 times

 **t0nx** 4 months ago

A and B

answer on the FAQ, SFTP has nothing to do with DataSync

Q: When do I use AWS DataSync and when do I use AWS Transfer Family?

A: If you currently use SFTP to exchange data with third parties, AWS Transfer Family provides a fully managed SFTP, FTPS, FTP, and AS2 transfer directly into and out of Amazon S3, while reducing your operational burden.

<https://aws.amazon.com/datasync/faqs/>

upvoted 2 times

 **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: BE

BE combination allow migration using datasync, architecture already is defined in the question.
A is wrong because it's not said EFS uses single AZ mode, by default it works in multi-AZ mode

upvoted 1 times

 **axelrodb** 6 months, 2 weeks ago

Selected Answer: BD

BE is the correct answer

upvoted 1 times

 **SuperDuperPooperScooper** 7 months, 1 week ago

<https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-associate-saa-c03/view/11/#>

upvoted 1 times

Question #103

Topic 1

A company has an AWS Glue extract, transform, and load (ETL) job that runs every day at the same time. The job processes XML data that is in an Amazon S3 bucket. New data is added to the S3 bucket every day. A solutions architect notices that AWS Glue is processing all the data during each run.

What should the solutions architect do to prevent AWS Glue from reprocessing old data?

- A. Edit the job to use job bookmarks.
- B. Edit the job to delete data after the data is processed.
- C. Edit the job by setting the NumberOfWorkers field to 1.
- D. Use a FindMatches machine learning (ML) transform.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **123jh10**  1 year, 5 months ago

Selected Answer: A

This is the purpose of bookmarks: "AWS Glue tracks data that has already been processed during a previous run of an ETL job by persisting state information from the job run. This persisted state information is called a job bookmark. Job bookmarks help AWS Glue maintain state information and prevent the reprocessing of old data."

<https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html>

upvoted 43 times

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

Selected Answer: A

A. Job bookmarks in Glue allow you to track the last-processed data in a job. By enabling job bookmarks, Glue keeps track of the processed data and automatically resumes processing from where it left off in subsequent job runs.

B. Results in the permanent removal of the data from the S3, making it unavailable for future job runs. This is not desirable if the data needs to be retained or used for subsequent analysis.

C. It would only affect the parallelism of the job but would not address the issue of reprocessing old data. It does not provide a mechanism to track the processed data or skip already processed data.

D. It is not directly related to preventing Glue from reprocessing old data. The FindMatches transform is used for identifying and matching duplicate or matching records in a dataset. While it can be used in data processing pipelines, it does not address the specific requirement of avoiding reprocessing old data in this scenario.

upvoted 8 times

✉️  **awsgeek75**  2 months, 1 week ago

Selected Answer: A

B: Glue can delete DataSet but this option is too vague to consider or too open to mean anything

C: Won't help with repeated ETL. This property affects parallelism

D: Too vague

upvoted 1 times

✉️  **Ruffyit** 4 months, 4 weeks ago

<https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html>

upvoted 2 times

✉️  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

The best solution is to edit the AWS Glue job to use job bookmarks.

Job bookmarks allow AWS Glue ETL jobs to track which data has already been processed during previous runs. This prevents reprocessing of old data.

Deleting the data after processing would cause the data to be lost and unavailable for future processing. Reducing the number of workers may improve performance but does not prevent reprocessing of old data. Using a FindMatches ML transform is used for record matching, not preventing reprocessing.

So the solutions architect should enable job bookmarks in the AWS Glue job configuration. This will allow the ETL job to keep track of processed data and only transform the new data added since the last run.

upvoted 1 times

✉️  **bedwal2020** 11 months ago

Selected Answer: A

Job bookmark to make sure that the glue job will not process already processed files.
upvoted 1 times

 **Heric** 11 months, 1 week ago

Selected Answer: A

Job bookmarks are used in AWS Glue ETL jobs to keep track of the data that has already been processed in a previous job run. With bookmarks enabled, AWS Glue will read the bookmark information from the previous job run and will only process the new data that has been added to the data source since the last job run. This saves time and reduces costs by eliminating the need to reprocess old data.

Therefore, a solutions architect should edit the AWS Glue ETL job to use job bookmarks so that it will only process new data added to the S3 bucket since the last job run.

upvoted 2 times

 **linux_admin** 11 months, 4 weeks ago

Selected Answer: A

Job bookmarks enable AWS Glue to track the data that has been processed in a previous run of the job. With job bookmarks enabled, AWS Glue will only process new data that has been added to the S3 bucket since the previous run of the job, rather than reprocessing all data every time the job runs.

upvoted 2 times

 **gustavtd** 1 year, 2 months ago

Delete files in S3 freely is not good. so B is not correct,

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: A

A is correct

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: A

Option A. Edit the job to use job bookmarks.

Job bookmarks in AWS Glue allow the ETL job to track the data that has been processed and to skip data that has already been processed. This can prevent AWS Glue from reprocessing old data and can improve the performance of the ETL job by only processing new data. To use job bookmarks, the solutions architect can edit the job and set the "Use job bookmark" option to "True". The ETL job will then use the job bookmark to track the data that has been processed and skip data that has already been processed in subsequent runs.

upvoted 3 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

Option A

upvoted 1 times

 **SilentMilli** 1 year, 3 months ago

Selected Answer: A

It's obviously A. Bookmarks serve this purpose

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 2 times

 **LeGlopier** 1 year, 5 months ago

Selected Answer: A

A

<https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html>

upvoted 3 times

Question #104

Topic 1

A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website.

Which actions should the solutions architect take to protect the website from such an attack? (Choose two.)

- A. Use AWS Shield Advanced to stop the DDoS attack.
- B. Configure Amazon GuardDuty to automatically block the attackers.
- C. Configure the website to use Amazon CloudFront for both static and dynamic content.
- D. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
- E. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization.

Correct Answer: AC

Community vote distribution



✉️ **alvarez100** Highly Voted 1 year, 5 months ago

Selected Answer: AC

I think it is AC, reason is they require a solution that is highly available. AWS Shield can handle the DDoS attacks. To make the solution HA you can use cloud front. AC seems to be the best answer imo.
AB seem like redundant answers. How do those answers make the solution HA?
upvoted 26 times

✉️ **attila9778** 1 year, 4 months ago

A - AWS Shield Advanced
C - (protecting this option) IMO: AWS Shield Advanced has to be attached. But it can not be attached directly to EC2 instances.
According to the docs: <https://aws.amazon.com/shield/>
It requires to be attached to services such as CloudFront, Route 53, Global Accelerator, ELB or (in the most direct way using) Elastic IP (attached to the EC2 instance)
upvoted 25 times

✉️ **Buruguduystunstugudunstuy** Highly Voted 1 year, 2 months ago

Selected Answer: AC

Option A. Use AWS Shield Advanced to stop the DDoS attack.

It provides always-on protection for Amazon EC2 instances, Elastic Load Balancers, and Amazon Route 53 resources. By using AWS Shield Advanced, the solutions architect can help protect the website from large-scale DDoS attacks.

Option C. Configure the website to use Amazon CloudFront for both static and dynamic content.

CloudFront is a content delivery network (CDN) that integrates with other Amazon Web Services products, such as Amazon S3 and Amazon EC2, to deliver content to users with low latency and high data transfer speeds. By using CloudFront, the solutions architect can distribute the website's content across multiple edge locations, which can help absorb the impact of a DDoS attack and reduce the risk of downtime for the website.

upvoted 13 times

✉️ **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: AC

A: For DDoS attacks
C: For scalable available site

B: Irrelevant
D: How would Lambda identify the attacker IP even if this was possible (ACL has a limit of 40 rules each way)
E: Scaling is not an issue here
upvoted 2 times

✉️ **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: AC

A - use aws shield advanced for DDoS protection, but it cannot be used with EC2 instance if it's not using EIP, which is not mentioned
C - but it can be used with CloudFront distribution
thus AC is the answer
upvoted 1 times

✉️ **Ruffyit** 4 months, 4 weeks ago

DDoS attack will choose the AWS Shield Advanced
CloudFront have attached the WAF

upvoted 1 times

 **Devsin2000** 5 months, 4 weeks ago

Selected Answer: AE

A - no brainer

E = "must design a highly available infrastructure". I am not sure if CloudFront addresses this requirement.

upvoted 1 times

 **pentium75** 3 months ago

Is CloudFront not HA? Answer E uses Spot instances which might be unavailable, thus are NEVER an option for HA.

upvoted 2 times

 **sidharthwader** 3 weeks, 4 days ago

You are right if it was On demand instances we could think of E

upvoted 1 times

 **LoXoL** 2 months, 2 weeks ago

pentium75 is right.

upvoted 1 times

 **TariqKipkemei** 7 months ago

Selected Answer: AC

Mitigate a large-scale DDoS attack = AWS Shield Advanced

Downtime is not acceptable for the website = high availability = Amazon CloudFront

upvoted 1 times

 **mtmayer** 7 months, 1 week ago

Selected Answer: D

yeah , AWS Shield Advanced can be used directly on EC2.....

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-protections-by-resource-type.html>

upvoted 1 times

 **pentium75** 3 months ago

Why D then?

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: AC

Cloud front supports SHIELD ADVANCED integration

upvoted 2 times

 **diabloexodia** 8 months, 2 weeks ago

Cloud front supports SHIELD ADVANCED integration

upvoted 1 times

 **Aash24** 8 months, 3 weeks ago

Selected Answer: D

D should be the one here

upvoted 3 times

 **pentium75** 3 months ago

"Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs"?????

upvoted 2 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: AC

A. AWS Shield Advanced provides advanced DDoS protection for AWS resources, including EC2. It includes features such as real-time threat intelligence, automatic protection, and DDoS cost protection.

C. CloudFront is a CDN service that can help mitigate DDoS attacks. By routing traffic through CloudFront, requests to the website are distributed across multiple edge locations, which can absorb and mitigate DDoS attacks more effectively. CloudFront also provides additional DDoS protection features, such as rate limiting, SSL/TLS termination, and custom security policies.

B. While GuardDuty can detect and provide insights into potential malicious activity, it is not specifically designed for DDoS mitigation.

D. Network ACLs are not designed to handle high-volume traffic or DDoS attacks efficiently.

E. Spot Instances are a cost optimization strategy and may not provide the necessary availability and protection against DDoS attacks compared to using dedicated instances with DDoS protection mechanisms like Shield Advanced and CloudFront.

upvoted 3 times

 **Heric** 11 months, 1 week ago

Selected Answer: AC

Key word:

DDoS attack will choose the AWS Shield Advanced

Cloudfront have attached the WAF
upvoted 2 times

✉ **jdr75** 11 months, 3 weeks ago

Selected Answer: AC

A & C
but no fully understand why cloudfront is opted.
The customer does not need it, and it's not exactly cheap.
Yes it could serve the cached content to the attacker, alighting the job in backend, but as I said it's not cheap, and the OOTB AWS Shield is free and can cope with the attack (as far as it won't be waf-style-attack).
upvoted 1 times

✉ **pentium75** 3 months ago

Because AWS Shield Advanced can't be directly attached to an EC2 instance. Yes, it says everything that 'AWS Shield Advanced can protect EC2 instances', but it still needs CloudFront inbetween.

upvoted 3 times

✉ **Khushna** 1 year, 1 month ago

Selected Answer: AC

DDos is better with shield and Cloudfront also provide protection for ddos
upvoted 1 times

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

AC
"AWS Shield Advanced is available globally on all Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 edge locations worldwide. You can protect your web applications hosted anywhere in the world by deploying Amazon CloudFront in front of your application. Your origin servers can be Amazon Simple Storage Service (S3), Amazon EC2, Elastic Load Balancing, or a custom server outside of AWS."
<https://aws.amazon.com/shield/faqs/>

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

A and C as your will need to configure Cloudfront to activate AWS Advance Shield
upvoted 1 times

Question #105

Topic 1

A company is preparing to deploy a new serverless workload. A solutions architect must use the principle of least privilege to configure permissions that will be used to run an AWS Lambda function. An Amazon EventBridge (Amazon CloudWatch Events) rule will invoke the function. Which solution meets these requirements?

- A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.
- B. Add an execution role to the function with lambda:InvokeFunction as the action and Service: lambda.amazonaws.com as the principal.
- C. Add a resource-based policy to the function with lambda:* as the action and Service: events.amazonaws.com as the principal.
- D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service: events.amazonaws.com as the principal.

Correct Answer: D

Community vote distribution

D (97%)

✉ 123jh10 **Highly Voted** 1 year, 5 months ago

Selected Answer: D

Best way to check it... The question is taken from the example shown here in the documentation:
<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-use-resource-based.html#eb-lambda-permissions>

upvoted 34 times

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

Selected Answer: D

The correct solution is D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service: events.amazonaws.com as the principal.

The principle of least privilege requires that permissions are granted only to the minimum necessary to perform a task. In this case, the Lambda function needs to be able to be invoked by Amazon EventBridge (Amazon CloudWatch Events). To meet these requirements, you can add a resource-based policy to the function that allows the InvokeFunction action to be performed by the Service: events.amazonaws.com principal. This will allow Amazon EventBridge to invoke the function, but will not grant any additional permissions to the function.

upvoted 20 times

✉ Buruguduystunstugudunstuy 1 year, 3 months ago

Why other options are wrong

Option A is incorrect because it grants the lambda:InvokeFunction action to any principal (*), which would allow any entity to invoke the function and goes beyond the minimum permissions needed.

Option B is incorrect because it grants the lambda:InvokeFunction action to the Service: lambda.amazonaws.com principal, which would allow any Lambda function to invoke the function and goes beyond the minimum permissions needed.

Option C is incorrect because it grants the lambda:* action to the Service: events.amazonaws.com principal, which would allow Amazon EventBridge to perform any action on the function and goes beyond the minimum permissions needed.

upvoted 19 times

✉ awsgEEK75 **Most Recent** 2 months, 1 week ago

Selected Answer: D

This is a good example article with nice learning material.

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-run-lambda-schedule.html>

upvoted 1 times

✉ chasingsummer 3 months, 2 weeks ago

Selected Answer: D

Good explanation from ChatGPT:

In order to adhere to the principle of least privilege when configuring permissions for an AWS Lambda function invoked by an Amazon EventBridge (CloudWatch Events) rule, the most appropriate solution would be:

D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service: events.amazonaws.com as the principal.

This solution involves attaching a resource-based policy to the Lambda function. It specifies that the only entity allowed to invoke the Lambda function is the Amazon EventBridge service (represented by the principal events.amazonaws.com) and restricts the action to only invoking the function (lambda:InvokeFunction). This aligns with the principle of least privilege by granting the necessary permissions explicitly to the service that needs them, without providing overly permissive access.

upvoted 2 times

 **MiniYang** 4 months ago

Selected Answer: B

Is anyone can explain why B is can't be a good choice? The option adds the execution role to the function, with lambda:InvokeFunction as the action and Service: lambda.amazonaws.com as the body. This restricts the Lambda function to only the Lambda service, providing an effective layer of security. and fully complies with the principle of least privilege

upvoted 2 times

 **pentium75** 3 months ago

Because the question is about the permission 'to run the function' (permission for the administrator to invoke it), while B is about execution permissions (permission for the function to access resources).

upvoted 1 times

 **Evonne_HY** 6 months, 1 week ago

why not choose B, an execution role is attached to lambda and a policy is attached to an execution role

upvoted 1 times

 **Georgeyp** 6 months ago

B would be the wrong choice as the both roles are granted to lambda, however the question requires Eventbridge to call the Lambda function.

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

lambda:InvokeFunction is the action needed to invoke the Lambda function.

Service: events.amazonaws.com is the principal (the AWS service) that is allowed to invoke the Lambda function. In this case, you're explicitly allowing CloudWatch Events to invoke the function.

upvoted 1 times

 **MNotABot** 8 months, 2 weeks ago

D

* is BIG NO. And we are talking about policy --> hence D

upvoted 2 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: D

In this solution, a resource-based policy is added to the Lambda function, which allows the specified principal (events.amazonaws.com) to invoke the function. The lambda:InvokeFunction action provides the necessary permission for the Amazon EventBridge rule to trigger the Lambda function.

Option A is incorrect because it assigns the lambda:InvokeFunction action to all principals (*), which grants permission to invoke the function to any entity, which is broader than necessary.

Option B is incorrect because it assigns the lambda:InvokeFunction action to the specific principal "lambda.amazonaws.com," which is the service principal for AWS Lambda. However, the requirement is for the EventBridge service principal to invoke the function.

Option C is incorrect because it assigns the lambda:* action to the specific principal "events.amazonaws.com," which is the service principal for Amazon EventBridge. However, it grants broader permissions than necessary, allowing any Lambda function action, not just lambda:InvokeFunction.

upvoted 2 times

 **Abrar2022** 10 months, 1 week ago

Option C is incorrect, the reason is that, firstly, lambda:* allows Amazon EventBridge to perform any action on the function and this is beyond the minimum permissions needed.

upvoted 1 times

 **Rahulbit34** 10 months, 3 weeks ago

Since its for Lamda which is a resource, resource policy is the trick

upvoted 2 times

 **bdp123** 1 year, 1 month ago

Selected Answer: D

<https://docs.aws.amazon.com/eventbridge/latest/userguide/resource-based-policies-eventbridge.html#lambda-permissions>

upvoted 1 times

 **gustavtd** 1 year, 2 months ago

Selected Answer: D

The definition scope of D is the smallest, so is it

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: D

events.amazonaws.com is principal for eventbridge

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

  **wly_al** 1 year, 3 months ago

least privilege meant the role cannot be "*". answer B only mention lambda. so the answer was D

upvoted 1 times

  **ocbn3wby** 1 year, 4 months ago**Selected Answer: D**

My answer was D, as this is the most specific answer.

And then there's this guy's answer (123jhl0) which provides more details.

upvoted 1 times

Question #106

Topic 1

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year. Which solution meets these requirements and is the MOST operationally efficient?

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

Correct Answer: D

Community vote distribution



✉️ **123jh10** 1 year, 5 months ago

Selected Answer: D

The MOST operationally efficient one is D.

Automating the key rotation is the most efficient.

Just to confirm, the A and B options don't allow automate the rotation as explained here:

<https://aws.amazon.com/kms/faqs/#:~:text=You%20can%20choose%20to%20have%20AWS%20KMS%20automatically%20rotate%20KMS,KMS%20custom%20key%20store%20feature>

upvoted 17 times

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

In addition you cannot log key usage in B, for A I am not certain

upvoted 1 times

✉️ **ocbn3wby** 1 year, 4 months ago

Thank you for the explanation.

upvoted 1 times

✉️ **cookieMr** 9 months, 1 week ago

Selected Answer: D

SSE-KMS provides a secure and efficient way to encrypt data at rest in S3. SSE-KMS uses KMS to manage the encryption keys securely. With SSE-KMS, encryption keys can be automatically rotated using KMS key rotation feature, which simplifies the key management process and ensures compliance with the requirement to rotate keys every year.

Additionally, SSE-KMS provides built-in audit logging for encryption key usage through CloudTrail, which captures API calls related to the management and usage of KMS keys. This meets the requirement for logging key usage for auditing purposes.

Option A (SSE-C) requires customers to provide their own encryption keys, but it does not provide key rotation or built-in logging of key usage. Option B (SSE-S3) uses Amazon S3 managed keys for encryption, which simplifies key management but does not provide key rotation or detailed key usage logging.

Option C (SSE-KMS with manual rotation) uses AWS KMS keys but requires manual rotation, which is less operationally efficient than the automatic key rotation available with option D.

upvoted 6 times

✉️ **Karun3294** 1 month ago

I got this question in exam today (FEB 21, 2024)

upvoted 4 times

✉️ **awsgeek75** 2 months, 1 week ago

Selected Answer: D

I'll go for D as SSS-S3 has unpublished scheduled of rotation which may or may not be "each year".

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

upvoted 1 times

✉️ **rcpttryk** 3 months, 4 weeks ago

Selected Answer: B

SSE-S3 can be used for logging in cloudtrail since January 5, 2023

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

upvoted 1 times

✉️ **pentium75** 3 months ago

But "keys must be rotated every year". I understand that SSE-S3 rotates the keys "regularly" but you have no influence on the schedule.

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

The correct answer is D. Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation.

SSE-KMS is the most secure way to encrypt data in Amazon S3. It uses AWS KMS, which is a highly secure key management service that is managed by AWS. AWS KMS logs all key usage, so the company can meet its compliance requirements. AWS KMS also rotates keys automatically, so the company does not have to worry about manually rotating keys.

upvoted 3 times

 **SilentMilli** 1 year, 2 months ago

Selected Answer: D

Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation meets the requirements and is the most operationally efficient solution. This option allows you to use AWS KMS to automatically rotate the keys every year, which simplifies key management. In addition, key usage is logged for auditing purposes, and the data is encrypted at rest to meet compliance requirements.

upvoted 2 times

 **Zerotn3** 1 year, 2 months ago

Selected Answer: B

AWS API Gateway is a fully managed service that makes it easy to create, publish, maintain, monitor, and secure APIs at any scale. You can use API Gateway to create a REST API that exposes the location data as an API endpoint, allowing you to access the data from your analytics platform.

AWS Lambda is a serverless compute service that lets you run code in response to events or HTTP requests. You can use Lambda to write the code that retrieves the location data from your data store and returns it to API Gateway as a response to API requests. This allows you to scale the API to handle a large number of requests without the need to provision or manage any infrastructure.

upvoted 2 times

 **pentium75** 3 months ago

This question is about server-side encryption, not API Gateway

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: D

The most operationally efficient solution that meets the requirements listed would be option D: Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation.

SSE-KMS allows you to use keys that are managed by the AWS Key Management Service (KMS) to encrypt your data at rest. KMS is a fully managed service that makes it easy to create and control the encryption keys used to encrypt your data. With automatic key rotation enabled, KMS will automatically create a new key for you on a regular basis, typically every year, and use it to encrypt your data. This simplifies the key rotation process and reduces the operational burden on your team.

In addition, SSE-KMS provides logging of key usage through AWS CloudTrail, which can be used for auditing purposes.

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Why other options are wrong

Option A: Server-side encryption with customer-provided keys (SSE-C) would require you to manage the encryption keys yourself, which can be more operationally burdensome.

Option B: Server-side encryption with Amazon S3 managed keys (SSE-S3) does not allow for key rotation or logging of the key usage.

Option C: Server-side encryption with AWS KMS keys (SSE-KMS) with manual rotation would require you to manually initiate the key rotation process, which can be more operationally burdensome compared to automatic rotation.

upvoted 3 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

 **Berny** 1 year, 3 months ago

You can choose to have AWS KMS automatically rotate KMS keys every year, provided that those keys were generated within AWS KMS HSMs. Automatic key rotation is not supported for imported keys, asymmetric keys, or keys generated in a CloudHSM cluster using the AWS KMS custom key store feature. If you choose to import keys to AWS KMS or asymmetric keys or use a custom key store, you can manually rotate them by creating a new KMS key and mapping an existing key alias from the old KMS key to the new KMS key.

upvoted 1 times

 **PavelTech** 1 year, 3 months ago

Can anybody correct me if I'm wrong, KMS does not offer automatic rotations but SSE-KMS only allows automatic rotation once in 3 years thus if we want rotation every year we need to rotate it manually?

upvoted 2 times

 **JayBee65** 1 year, 3 months ago

You're wrong :) "All AWS managed keys are automatically rotated every year. You cannot change this rotation schedule."
<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk>

upvoted 1 times

 PS_R 1 year, 4 months ago

Selected Answer: D

Agree Also, SSE-S3 cannot be audited.

upvoted 2 times

Question #107

Topic 1

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3.
- B. Use Amazon API Gateway with AWS Lambda.
- C. Use Amazon QuickSight with Amazon Redshift.
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

Correct Answer: D

Community vote distribution



✉ **ArielSchivo** Highly Voted 1 year, 5 months ago

Selected Answer: B

API Gateway is needed to get the data so option A and C are out.

"The company wants to use these data points in its existing analytics platform" so there is no need to add Kinesis. Option D is also out. This leaves us with option B as the correct one.

upvoted 80 times

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

You are right, but it clearly say "store data".
AWS Lambda don't store data, Kinesis could.

upvoted 4 times

✉ **ces26015** 1 year, 2 months ago

i dont understand the use of a lambda function here, maybe if there would be need to transform the data, can you explain?

upvoted 5 times

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

B might work but D works better. B requieres API gateway + lambda for data input & output, whereas D is a broader solution, as Kinesis Data Analytics APIs can be used to extract and process data better than API Gateway + Lambdas. Also, Kinesis is highly recommended for telemetry data which is the question scenario. @See Kinesys flexible API (<https://aws.amazon.com/documentation-overview/kinesis-data-analytics/>)

upvoted 5 times

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

Also by using kinesis the analytics platform will have a storing buffer to take & process data through the kinesys API. The lambda aproach in the B scenario is to wide and leaves many loose ends.

upvoted 2 times

✉ **bullrem** 1 year, 2 months ago

AWS Lambda is a serverless compute service that can be used to run code in response to specific events, such as changes to data in an Amazon S3 bucket or updates to a DynamoDB table. It could be used to process the location data, but it doesn't provide storage solution. Therefore, it would not be the best option for storing and retrieving location data in this scenario.

upvoted 9 times

✉ **Six_Fingered_Jose** Highly Voted 1 year, 5 months ago

Selected Answer: D

I dont understand why you will vote B?

how are you going to store data with just lambda?

> Which action meets these requirements for storing and retrieving location data

In this use case there will obviously be a ton of data and you want to get real-time location data of the bicycles, and to analyze all these info kinesis is the one that makes most sense here.

upvoted 55 times

✉ **a070112** 1 year, 3 months ago

Lambda isn't storing the data themselves. It's triggering the data store to the company's "existing data analytics platform"

upvoted 8 times

✉ **kmluy73** 1 year, 3 months ago

Real-time analytics on Kinesis Data Streams & Firehose using SQL, not store db ...

upvoted 3 times

 **Six_Fingered_Jose** 1 year, 5 months ago

<https://aws.amazon.com/blogs/aws/real-time-hotspot-detection-in-amazon-kinesis-analytics/>
upvoted 5 times

 **UWSFish** 1 year, 5 months ago

I don't think you need to worry about storing data. The question states there is an existing platform.
upvoted 4 times

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

We need API Gateway for rest APIs, so A and C are out.

Among B and D, there is an existing analytics platform so no need for Kinesis. Also, Kinesis Data Analytics relies on data source: either Kinesis Data Firehose or Kinesis Data Streams. It cannot work directly with API Gateway, so option D is out.

That leaves B).

upvoted 2 times

 **danwantstolearn** 1 month, 1 week ago

Selected Answer: D

D because B mentions no way to store data.

upvoted 1 times

 **farnamjam** 1 month, 3 weeks ago

Selected Answer: B

Comparison to other options:

A. Athena and S3: While storing data in S3 and querying it with Athena is cost-effective, it wouldn't provide real-time data access needed for the API.

C. QuickSight and Redshift: QuickSight and Redshift are excellent for analytics, but wouldn't directly expose data through the API. You'd still need a Lambda function to act as an intermediary.

D. API Gateway and Kinesis Data Analytics: Kinesis Data Analytics is suitable for real-time streaming analysis, but it wouldn't directly provide a REST API endpoint. You'd need additional setup like API Gateway or Lambda for API access.

upvoted 2 times

 **rvca231** 2 months ago

Selected Answer: B

Kinesis Data Analytics requires a Kinesis Data Streams or Kinesis Data Firehose as input streams, so you cannot directly connect it to API Gateway, therefore B is the answer

upvoted 5 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: D

A: Athena on S3 is query

B: API + Lambda is just API

C: Analytics and reporting

D: API and analytics with storage

D is the correct answer

upvoted 1 times

 **pdragon1981** 2 months, 2 weeks ago

Selected Answer: D

I would go for option D, use of gateway API is needed and also is necessary to store the data so the unique option available is D, lambda can't store data

upvoted 1 times

 **data_cloud_aws** 2 months, 2 weeks ago

Selected Answer: D

Keywords : API , Storing

D

upvoted 1 times

 **SaurabhTiwari1** 3 months, 1 week ago

Selected Answer: B

B is correct

B. Use Amazon API Gateway with AWS Lambda.

This option allows the company to create, deploy, and manage a RESTful API to expose the required endpoints. AWS Lambda can be used to process the incoming requests and perform CRUD operations. The processed data can then be stored in a database like Amazon DynamoDB. This architecture would be serverless, scalable, and cost-effective. It would also allow real-time tracking of bicycles during peak operating hours. The other options do not provide the same level of real-time processing and flexibility for this specific use case.

upvoted 1 times

 **pentium75** 3 months ago

"The processed data can then be stored in a database like Amazon DynamoDB" -> but B does not mention a database, though 'storing data' is part of the requirement.

upvoted 1 times

 **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: A

I'm going with A

<https://docs.aws.amazon.com/athena/latest/ug/what-is.html>

"Athena helps you analyze unstructured, semi-structured, and structured data stored in Amazon S3."

It provides REST API for interacting with it https://docs.aws.amazon.com/athena/latest/APIReference/API_Operations.html
you can access data points via sql queries

B: doesn't mention how data will be stored

C: QuickSight don't provide api for accessing data points from data sources

D: you can integrate API Gateway with Amazon Kinesis but it's very limited API, I don't see a possibility to read a data point from it
https://docs.aws.amazon.com/kinesisanalytics/latest/dev/API_Operations.html

upvoted 3 times

 **pentium75** 3 months ago

"Athena helps you analyze" .. But we don't want to analyze. We want to retrieve and store the data and make it available to an existing analytics platform via REST API.

upvoted 1 times

 **slimen** 4 months, 3 weeks ago

Selected Answer: B

they do have an analytic platform, adding kinesis = more money + more operational overhead

upvoted 1 times

 **ZZNZ** 5 months, 1 week ago

Selected Answer: B

"The company wants to use these data points in its existing analytics platform"

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: D

If you choose the lambda function, where does it pull data from?

upvoted 1 times

 **slimen** 4 months, 3 weeks ago

the data is being sent to API gateway using REST

API GW will send data to Lambda

Lambda will send data to the existing analytic platform

they have an analytic platform already, Kinesis is not needed

upvoted 1 times

 **pentium75** 3 months ago

Nothing is SENT via API GW, the stem tells us that they want to RETRIEVE the stored data via REST API (= API GW). The "existing analytic platform" will use this REST API; Lambda will not "send" anything there.

upvoted 1 times

 **MOSHE** 5 months, 3 weeks ago

Selected Answer: D

Using Amazon API Gateway with AWS Lambda: This combination allows for creating a serverless REST API. AWS Lambda can process the data, but it doesn't inherently store it. It would need an additional data storage service.

Using Amazon API Gateway with Amazon Kinesis Data Analytics: This combination allows for real-time analysis of streaming data, and the data can be exposed via a REST API using Amazon API Gateway. Amazon Kinesis Data Analytics can process and analyze the streaming data in real-time, making it a suitable choice for the scenario described. Moreover, Amazon Kinesis Data Analytics can ingest data and not only store the data points but can expose them as REST API, which aligns with the requirements of the scenario1.

upvoted 2 times

 **Ramdi1** 5 months, 3 weeks ago

Selected Answer: D

i think the answer is D because of the storing data requirement

upvoted 1 times

 **vijaykamal** 6 months ago

Selected Answer: D

Lambda does not store the information and since real time tracking is needed for peak hrs., Kinesis would work better

upvoted 1 times

Question #108

Topic 1

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems. Which design should a solutions architect recommend?

- A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume.
- B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume.
- C. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics. Use AWS Lambda functions to update the targets.
- D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues. Use AWS Lambda functions to update the targets.

Correct Answer: C

Community vote distribution



✉️ **romko** 1 year, 4 months ago

Selected Answer: A

Interesting point that Amazon RDS event notification doesn't support any notification when data inside DB is updated.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.overview.html
So subscription to RDS events doesn't give any value for Fanout = SNS => SQS

B is out because FIFO is not required here.

A is left as correct answer

upvoted 81 times

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

D is connect
RDS event notification by RDS stream or advance audit DML so it is possible
upvoted 1 times

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

The key is "Fanned out" due to "Multiple target systems" need to update
upvoted 2 times

✉️ **JayBee65** 1 year, 3 months ago

Please provide reference for this claim: " event notification by RDS stream or advance audit DML"
upvoted 2 times

✉️ **nauman001** 12 months ago

Listing the Amazon RDS event notification categories.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.ListingCategories.html:
upvoted 1 times

✉️ **ruqui** 10 months, 1 week ago

I don't think A is a valid solution ... how do you send the data to multiple targets using a single SQS?
upvoted 17 times

✉️ **Vic_d_gr8** 1 year, 4 months ago

Amazon RDS uses the SNS to provide notification when an Amazon event occurs
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.html
upvoted 2 times

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

Selected Answer: A

RDS events only provide operational events such as DB instance events, DB parameter group events, DB security group events, and DB snapshot events. What we need in the scenario is to capture data-modifying events (INSERT, DELETE, UPDATE) which can be achieved thru native functions or stored procedures.

upvoted 11 times

✉️ **BlueVolcano1** 1 year, 2 months ago

I agree with it requiring a native function or stored procedure, but can they in turn invoke a Lambda function? I have only seen this being possible with Aurora, but not RDS - and I'm not able to find anything googling for it either. I guess it has to be possible, since there's no other option that fits either.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html>

upvoted 1 times

✉ **BlueVolcano1** 1 year, 2 months ago

To add to that though, A also states to only use SQS (no SNS to SQS fan-out), which doesn't seem right as the message needs to go to multiple targets?

upvoted 5 times

✉ **dkw2342** **Most Recent** 3 weeks, 4 days ago

To sum up: There seems to be sth wrong with this question.

D: Sounds plausible, but RDS events only provide operational events, e.g. shutdown, failover, config change.

C: see D, also makes no sense since fanout is SNS -> SQS

B: No mention of FIFO requirement.

A: Invoking an AWS Lambda function is possible, albeit only from Postgres-flavored RDS[1]. However, this solution lacks fanout architecture (SNS -> multiple SQS) to enable multiple consumers as required.

[1] <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/PostgreSQL-Lambda.html>

upvoted 1 times

✉ **lki77** 4 weeks, 1 day ago

The most suitable design for the scenario described is:

D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues. Use AWS Lambda functions to update the targets.

This design leverages RDS event notifications to trigger a fan-out mechanism through Amazon SNS. Subsequently, AWS Lambda functions can be used to process these messages and update the multiple target systems efficiently. This approach allows for decoupling the components and provides flexibility in managing the integration with different target systems.

upvoted 1 times

✉ **shwelin** 1 month, 1 week ago

Answer is C , multiple subscribers.

upvoted 1 times

✉ **wyejay** 1 month, 3 weeks ago

Option A: Triggering a Lambda function directly from RDS updates isn't straightforward without using an intermediary service like SNS or SQS to handle the messaging.

Option B: While SQS FIFO queues ensure order, they aren't necessary unless the application requires strict order in processing sales data, and they don't inherently support multiple targets without additional configuration.

Option C: RDS event notifications typically signal RDS instance events (like backups or maintenance) rather than data-level changes within the database.

upvoted 1 times

✉ **thewalker** 1 month, 3 weeks ago

Selected Answer: D

D is the right option

When asked Amazon Q: Can I create an event notification for a delete row action for a table in the RDS Database?

The answer was:

Yes, it is possible to create an event notification for delete row actions in an RDS database table.

When a row is deleted from an RDS database table, it will trigger a "Delete" event. You can subscribe to these events by creating an Amazon RDS event notification subscription.

Hence, for the remaining architecture, D is the best way forward.

upvoted 3 times

✉ **06042022** 2 months ago

Selected Answer: D

Fanout->SNS->SQS

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Selected Answer: A

From language perspective A looks better than D but the implementation in D is much closer to what A should be. It is confusing either way.

upvoted 1 times

✉ **SohamSLP** 3 months ago

Wouldn't we want to process orders in FIFO manner?

upvoted 1 times

 **sirasdf** 1 month ago

If you understood FIFO you would ask that question.

upvoted 1 times

 **pentium75** 3 months ago

Why should we?

upvoted 2 times

 **djgodzilla** 3 months, 1 week ago

Selected Answer: A

AWS RDS Event Categories and Messages

Amazon RDS generates several different events. The key event categories include :

DB instance created/deleted/restarted/shutdown

Maintenance , patching , backup & Recovery

Configuration changes, snapshot actions

<https://dzone.com/articles/how-can-i-know-what-happens-inside-amazon-rds>

upvoted 1 times

 **Fizbo** 4 months ago

Selected Answer: A

RDS events only provide operational events such as DB instance events, DB parameter group events, DB security group events, and DB snapshot events. What we need in the scenario is to capture data-modifying events i.e delete. Usually, you can do it through a native function or stored procedure

upvoted 1 times

 **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: B

RDS event notification can't send notifications about state of tables

If this data is about selling automobile and target systems process this sale FIFO queue would be desired to avoid duplicates

Multiple consumers can process single message from queue

upvoted 1 times

 **slimen** 4 months, 3 weeks ago

the question not very clear, 2 points to consider:

- record delete
- send to multiple systems

if you go for A you will violate the 2nd point as SQS wan't send to multiple targets at the same time

is you go dor D you violate the 1st point as the RDS events doesn't intercept database level changes instead it intercept the changes of the resource itself:

DB instance

DB snapshot

DB parameter group

DB security group

RDS Proxy

Custom engine version

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.overview.html

so I'm a bit confused here!!

upvoted 5 times

 **liux99** 4 months, 3 weeks ago

RDS event is database level event, not table level event, so record delete is not considered as event, C, D are out. FIFO queue is not required here, B is out. A is the only possible right answer.

upvoted 1 times

 **wearrexdzw3123** 4 months, 3 weeks ago

In my opinion, there is no complete solution provided, whether it is d or a

upvoted 2 times

 **tom_cruise** 4 months, 3 weeks ago

Selected Answer: A

"If you don't delete the message, Amazon SQS will deliver it again when it receives another receive request."

<https://aws.amazon.com/sqs/faqs/#:~:text=If%20you%20don't%20delete,No.>

upvoted 1 times

Question #109

Topic 1

A company needs to store data in Amazon S3 and must prevent the data from being changed. The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects. Only specific users in the company's AWS account can have the ability to delete the objects.

What should a solutions architect do to meet these requirements?

- A. Create an S3 Glacier vault. Apply a write-once, read-many (WORM) vault lock policy to the objects.
- B. Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Set a retention period of 100 years. Use governance mode as the S3 bucket's default retention mode for new objects.
- C. Create an S3 bucket. Use AWS CloudTrail to track any S3 API events that modify the objects. Upon notification, restore the modified objects from any backup versions that the company has.
- D. Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Add a legal hold to the objects. Add the s3:PutObjectLegalHold permission to the IAM policies of users who need to delete the objects.

Correct Answer: D

Community vote distribution

D (79%) B (21%)

✉️  **123jh10**  1 year, 5 months ago

Selected Answer: D

A - No as "specific users can delete"
 B - No as "nonspecific amount of time"
 C - No as "prevent the data from being change"
 D - The answer: "The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed." <https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html>
 upvoted 32 times

✉️  **PassNow1234** 1 year, 3 months ago

The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed.

Correct

upvoted 1 times

✉️  **Chunsli**  1 year, 5 months ago

typo -- 10 delete the objects => TO delete the objects
 upvoted 17 times

✉️  **oddnoises** 6 months ago

they were trying to speak in binary lol
 upvoted 3 times

✉️  **reviewmine** 1 month, 1 week ago

HAHAHA
 upvoted 1 times

✉️  **awsgeek75**  2 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>
 A: WORM doesn't allow delete by some users
 C: Irrelevant
 D: Permission only allows putting legal hold on objects. Not a complete solution
 B: Closest apart from 100 years as question is asking for indefinite. Governance allows modification by some users
 upvoted 1 times

✉️  **pentium75** 3 months ago

Selected Answer: B

"With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the objects if necessary."

D is wrong because it applies Object Lock AND Legal Hold, which are two different things that achieve similar results. 'Adding the s3:PutObjectLegalHold permission' to user's policies would allow them to remove the Legal Hold but NOT the Object Lock. (Also, it would probably make more sense to add the permissions to the bucket policy, not the "IAM policies of users".)

upvoted 3 times

 **LoXoL** 2 months, 2 weeks ago

Isn't Legal Hold a subcategory of Object Lock? Object Lock itself doesn't imply anything imho: you should go either for a Retention Mode OR Legal Hold. Why would you go for B if they ask "for a nonspecific amount of time"? Open to change my mind.

upvoted 1 times

 **Abitek007** 5 months, 2 weeks ago

Selected Answer: D

I only picked this because of restricted users who can delete, and the easiest way of achieving this is them assuming the role

upvoted 1 times

 **TariqKipkemei** 6 months, 4 weeks ago

Selected Answer: D

"The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects" = A legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed.

s3:PutObjectLegalHold permission is required in your IAM role to add or remove legal hold from objects.

upvoted 2 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed.

upvoted 1 times

 **RupeC** 8 months, 1 week ago

Selected Answer: D

My understanding is that the s3:PutObjectLegalHold permission allows certain users to apply or remove the legal hold on objects in the S3 bucket. However, having the permission to apply or remove the legal hold does not necessarily mean users can override the hold set by another user.

Once the legal hold is set on an object, it is in effect until the hold is removed by the user who applied it or an admin with the necessary permissions. Other users, even if they have the s3:PutObjectLegalHold permission, won't be able to remove the hold unless they are granted access by the user who originally applied it.

upvoted 2 times

 **omoakin** 10 months, 1 week ago

I go with option B as they still need some specific users to be able to make changes so Gov mode is the best choice and 100 yrs is like infinity as well haha

upvoted 3 times

 **KZM** 1 year ago

Selected Answer: D

The correct answer is D.

upvoted 1 times

 **Whericanstart** 1 year ago

Selected Answer: D

Option B specifies a retention period of 100 years which contradicts what the question asked for.....

"The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects"

Setting the retention period of 100 years is specific and the company wants new data/objects to remain unchanged for nonspecific amount of time.

Correct answer is D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html>

upvoted 3 times

 **slackbot** 7 months, 1 week ago

FFS 100 years = indefinitely. no company has a policy of keeping data for more than 10 years.

having specific admins run 2 additional commands every time they want to modify an object, is really in sync with nowadays automation processes.

instead of commenting each letter from the question, start thinking. if you were to decide, would you make your users always run commands before modifying or would you rather allow them to directly modify?

upvoted 1 times

 **bdp123** 1 year, 1 month ago

Selected Answer: D

"The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed." <https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html>

upvoted 1 times

 **Yelizaveta** 1 year, 1 month ago

Selected Answer: D

retention period of 100 Years prevents the object to be deleted before the retention period expires, so it's not a good fit.
upvoted 1 times

 **nadir_kh** 1 year, 2 months ago

it is B.

Once a legal hold is enabled, regardless of the object's retention date or retention mode, the object version cannot be deleted until the legal hold is removed.

Question says: "Specific users must have ability to delete objects"

upvoted 5 times

 **MutiverseAgent** 8 months, 2 weeks ago

If users have the policy s3:PutObjectLegalHold then they can remove the legal hold before deleting.

upvoted 1 times

 **John_Zhuang** 1 year, 2 months ago

Selected Answer: D

While S3 bucket governance mode does allow certain users with permissions to alter retention/delete objects, the 100 years in Option B makes it invalid.

Correct answer is option D.

"With Object Lock you can also place a legal hold on an object version. Like a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed."

<https://aws.amazon.com/s3/features/object-lock/>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html#object-lock-legal-holds>

upvoted 1 times

 **aba2s** 1 year, 2 months ago

Selected Answer: D

With Object Lock, you can also place a legal hold on an object version. Like a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed. Legal holds can be freely placed and removed by any user who has the s3:PutObjectLegalHold permission.

B - No as "nonspecific amount of time" otherwise B will meet the requirement with legal hold attached.

upvoted 1 times

 **FNJ1111** 1 year, 2 months ago

Wouldn't D require s3:GetBucketObjectLockConfiguration IAM permission? If so, D is incomplete and wouldn't meet the requirement.
(from the link shared above)

upvoted 1 times

Question #110

Topic 1

A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website.

The company needs to reduce coupling within the application and improve website performance. A solutions architect must design the most operationally efficient process for image uploads.

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

- A. Configure the application to upload images to S3 Glacier.
- B. Configure the web server to upload the original images to Amazon S3.
- C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL.
- D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image.
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

Correct Answer: BD

Community vote distribution



Buruguduystunstugudunstuy Highly Voted 1 year, 3 months ago

Selected Answer: CD

To meet the requirements of reducing coupling within the application and improving website performance, the solutions architect should consider taking the following actions:

C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a pre-signed URL. This will allow the application to upload images directly to S3 without having to go through the web server, which can reduce the load on the web server and improve performance.

D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image. This will allow the application to resize images asynchronously, rather than having to do it synchronously during the upload request, which can improve performance.

upvoted 39 times

jdr75 11 months, 3 weeks ago

presigned URL is for download the data from S3, not for uploads, so the user does not upload anything. C is no correct.

upvoted 10 times

mauroicardi 1 week, 4 days ago

A user who does not have AWS credentials to upload a file can use a presigned URL to perform the upload.

<https://boto3.amazonaws.com/v1/documentation/api/latest/guide/s3-presigned-urls.html>

upvoted 1 times

EricYu2023 11 months, 1 week ago

Presigned URL can be used for upload.

upvoted 8 times

PoisonBlack 11 months ago

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

upvoted 5 times

AF_1221 10 months, 4 weeks ago

Preassigned URL is for upload or download for temporary time and for specific users outside the company

upvoted 3 times

AF_1221 10 months, 4 weeks ago

but for temporary purpose not for permanent

upvoted 3 times

tuso 1 month, 3 weeks ago

So? You only need a presigned URL for the moment you upload the image, not forever

upvoted 1 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Why other options are wrong

Option A, Configuring the application to upload images to S3 Glacier, is not relevant to improving the performance of image uploads.

Option B, Configuring the webserver to upload the original images to Amazon S3, is not a recommended solution as it would not reduce coupling within the application or improve performance.

Option E, Creating an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images, is not a recommended solution as it would not be able to resize images in a timely manner and would not improve performance.

upvoted 4 times

 **MutiverseAgent** 8 months, 2 weeks ago

About your comments regarding option B)... But if images are being saved directly to S3 instead of the EBS/SSD storage of E2 instances as they originally were, the new approach will reduce coupling and improve performance. Also you have to consider the security concerns about presign URLs as the question does not mention if users are public or private.

upvoted 1 times

 **Yelizaveta** 1 year, 1 month ago

Here it means to decouple the processes, so that the web server don't have to do the resizing, so it doesn't slow down. The customers access the web server, so the web server have to be involved in the process, and how the others already wrote, the pre-signed URL is not the right solution because, of the explanation you can read in the other comments.

And additional! "Configure the application to upload images directly from EACH USER'S BROWSER to Amazon S3 through the use of a pre-signed URL"

I am not an expert, but I can't imagine that you can store an image that an user uploads in his browser etc.

upvoted 6 times

 **fkie4**  1 year ago

Selected Answer: BD

Why would anyone vote C? signed URL is for temporary access. also, look at the vote here:

<https://www.examtopics.com/discussions/amazon/view/82971-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 26 times

 **MikeJANG**  1 month, 2 weeks ago

Selected Answer: CD

GPT4

option B would offload the storage to S3 but still involves the web server in the upload process, which does not fully address the performance issues.

upvoted 1 times

 **sirasdf** 1 month ago

GPT4 is wrong. It does address the performance issue with the image processing will be done by lambda and not on the server

upvoted 1 times

 **MikeJANG** 1 month, 2 weeks ago

GPT4

option B would offload the storage to S3 but still involves the web server in the upload process, which does not fully address the performance issues.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: CD

C: presigned URL can be used to upload images to S3 <https://docs.aws.amazon.com/AmazonS3/latest/userguide/PresignedUrlUploadObject.html>

D: scalable event processing for image resizing using lambda

A: Glacier?

B: Can work and maybe improves the performance also as the webserver is not resizing the image (if D is used in combination with this). However,

C is better

E: Irrelevant

upvoted 1 times

 **bujuman** 2 months, 2 weeks ago

Selected Answer: CD

B could be excluded because of these two points:

- During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3.
- Users are experiencing slow upload requests to the website.

upvoted 1 times

 **Wang87** 2 months, 3 weeks ago

Selected Answer: AD

C is out of question as URL is not generated by user and highest validity is 7 days. So if user needs to access same file after 7 days it would be very troublesome.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

How is S3 glacier going to help with uploads?

upvoted 1 times

Cyberkayu 3 months, 2 weeks ago

based on decoupling requirement, Answer B still go thru Web server before drop the file into S3.

Answer CD

upvoted 1 times

pentium75 3 months ago

It's about decoupling upload and scaling process, the upload can still go through the web server, that's what a web server is for.

upvoted 1 times

slimen 4 months, 3 weeks ago

Selected Answer: BD

pre-signed URL is temporary

decoupling means preventing server from uploading and doing the resizing at the same time

so separating the processing into 2 parts (upload, then notify, then resize) is considered decoupling

upvoted 3 times

xplusfb 5 months, 1 week ago

Selected Answer: BD

C section seriously nonsense. many logical args given for BD I'll not write again.

upvoted 1 times

baggam 6 months, 1 week ago

Selected Answer: CD

CD is correct

upvoted 1 times

numark 6 months, 2 weeks ago

This is a social media company, so random users are uploading images. These are not employees. The signed URL has to be sent to the user and they only have a certain amount of time to use it. That's a disaster for a social media company. No way C is the answer. Lambda all the way.

upvoted 4 times

MarcusLEK 6 months, 3 weeks ago

Selected Answer: BD

while technically it's possible to upload with pre-signed URLs, it's also worth mentioning that pre-signed URLs have a time validity, so I think it might not be suitable to long term use.

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

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-presigned-url.html#:~:text=User%20Guide,-Expiration%20time%20for%20presigned%20URLs,-A%20presigned%20URL>

upvoted 4 times

judyda 6 months, 3 weeks ago

Selected Answer: CD

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/PresignedUrlUploadObject.html

upvoted 1 times

KawtarZ 6 months, 4 weeks ago

C is not correct. the pre-signed URLs are for download only, not upload.

upvoted 1 times

Iconique 6 months ago

wrong, they both for upload/download.

upvoted 2 times

TariqKipkemei 6 months, 4 weeks ago

Selected Answer: CD

Main requirement is decoupling and improve performance for which option C&D suit best.

You may use presigned URLs to allow someone to upload an object to your Amazon S3 bucket.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/PresignedUrlUploadObject.html#:~:text=You%20may%20use-,presigned%20URLs,-to%20allow%20someone>

Technically option D would work, but with the overhead of EC2/HDD/SDD.

upvoted 1 times

slimen 4 months, 3 weeks ago

pre-signed URL is temporary

decoupling means preventing server from uploading and doing the resizing at the same time

so separating the processing into 2 parts (upload, then notify, then resize) is considered decoupling

upvoted 1 times

mtmayer 7 months, 1 week ago

Selected Answer: CD

CD is much more efficient.

upvoted 1 times

 **pentium75** 3 months ago

But the application would need to request individual presigned URLs for each upload as these are temporary, this is quite an overhead.

upvoted 2 times

Question #111

Topic 1

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity.

Which architecture offers the HIGHEST availability?

- A. Add a second ActiveMQ server to another Availability Zone. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- B. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.
- D. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.

Correct Answer: D*Community vote distribution*

D (98%)

 **123jh10**  1 year, 5 months ago

Selected Answer: D

Answer is D as the "HIGHEST available" and less "operational complex"
 The "Amazon RDS for MySQL with Multi-AZ enabled" option excludes A and B
 The "Auto Scaling group" is more available and reduces operational complexity in case of incidents (as remediation it is automated) than just adding one more instance. This excludes C.

C and D to choose from based on
 D over C since is configured
 upvoted 19 times

 **awsgeek75**  2 months, 1 week ago

Selected Answer: D

D: Managed and auto-scaling, resilient and HA service for each tier. This is well-architected too.
 upvoted 2 times

 **Ruffyit** 4 months, 4 weeks ago

Using Amazon MQ with active/standby brokers provides highly available message queuing across AZs.

Adding an Auto Scaling group for consumer EC2 instances across 2 AZs provides highly available processing.

Using RDS MySQL with Multi-AZ provides a highly available database.

This architecture provides high availability for all components of the system - queue, processing, and database.
 upvoted 2 times

 **prabhjot** 5 months, 3 weeks ago

Ans is C - C. Option C uses Amazon MQ with active/standby brokers, adds an additional consumer EC2 instance, and uses Amazon RDS for MySQL with Multi-AZ enabled. Amazon RDS Multi-AZ automatically replicates your database to another AZ and provides automated failover. This ensures high availability for both the messaging system and the database. Option D- bring More scalability rather HA
 upvoted 2 times

 **pentium75** 3 months ago

D automates replacement of failed instances, thus it has higher availability than C.
 upvoted 2 times

 **TariqKipkemei** 6 months, 4 weeks ago

Selected Answer: D

HIGHEST availability. Definitely option D.
 upvoted 2 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

The key reasons are:

Amazon MQ active/standby brokers across AZs for queue high availability

Auto Scaling group with consumer EC2 instances across AZs for redundant processing

RDS MySQL with Multi-AZ for database high availability

This combines the HA capabilities of MQ, EC2 and RDS to maximize fault tolerance across all components. The auto scaling also provides flexibility to scale processing capacity as needed.

upvoted 2 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

D is the correct answer.

Using Amazon MQ with active/standby brokers provides highly available message queuing across AZs.

Adding an Auto Scaling group for consumer EC2 instances across 2 AZs provides highly available processing.

Using RDS MySQL with Multi-AZ provides a highly available database.

This architecture provides high availability for all components of the system - queue, processing, and database.

upvoted 2 times

 **james2033** 8 months, 1 week ago

Selected Answer: D

Keyword Amazon RDS, has C and D. Then D has "Auto Scaling group", choose D.

upvoted 2 times

 **MNotABot** 8 months, 2 weeks ago

D

With 3 options with Amazon MQ --> A is odd one out / Then ASG with M-AZ was an easy choice

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: D

Amazon MQ with active/standby brokers configured across two AZ ensures high availability for the message broker. In case of a failure in one AZ, the other AZ's broker can take over seamlessly.

Adding an ASG for the consumer EC2 instances across two AZ provides redundancy and automatic scaling based on demand. If one consumer instance becomes unavailable or if the message load increases, the ASG can automatically launch additional instances to handle the workload.

Using RDS for MySQL with Multi-AZ enabled ensures high availability for the database. Multi-AZ automatically replicates the database to a standby instance in another AZ. If a failure occurs, RDS automatically fails over to the standby instance without manual intervention.

This architecture combines high availability for the message broker (Amazon MQ), scalability and redundancy for the consumer EC2 instances (ASG), and high availability for the database (RDS Multi-AZ). It offers the highest availability with low operational complexity by leveraging managed services and automated failover mechanisms.

upvoted 2 times

 **Kostya** 9 months, 1 week ago

Selected Answer: D

Correct answer D

upvoted 1 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: D

to achieve ha + low operational complexity, the solution architect has to choose option D, which fulfill these requirements.

upvoted 1 times

 **Abrar2022** 10 months ago

Auto scaling and Multi-AZ enabled for high availability.

upvoted 1 times

 **Erbug** 1 year ago

you can find some details about Amazon MQ active/standby broker for high availability <https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/active-standby-broker-deployment.html>

upvoted 1 times

 **Abdel42** 1 year, 1 month ago

Selected Answer: D

D as the Auto Scaling group offer the highest availability between all solutions

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: D

Option D offers the highest availability because it addresses all potential points of failure in the system:

Amazon MQ with active/standby brokers configured across two Availability Zones ensures that the message queue is available even if one Availability Zone experiences an outage.

An Auto Scaling group for the consumer EC2 instances across two Availability Zones ensures that the consumer application is able to continue processing messages even if one Availability Zone experiences an outage.

Amazon RDS for MySQL with Multi-AZ enabled ensures that the database is available even if one Availability Zone experiences an outage.
upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option A addresses some potential points of failure, but it does not address the potential for the consumer application to become unavailable due to an Availability Zone outage.

Option B addresses some potential points of failure, but it does not address the potential for the database to become unavailable due to an Availability Zone outage.

Option C addresses some potential points of failure, but it does not address the potential for the consumer application to become unavailable due to an Availability Zone outage.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 2 times

Question #112

Topic 1

A company hosts a containerized web application on a fleet of on-premises servers that process incoming requests. The number of requests is growing quickly. The on-premises servers cannot handle the increased number of requests. The company wants to move the application to AWS with minimum code changes and minimum development effort.

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

- A. Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Use an Application Load Balancer to distribute the incoming requests.
- B. Use two Amazon EC2 instances to host the containerized web application. Use an Application Load Balancer to distribute the incoming requests.
- C. Use AWS Lambda with a new code that uses one of the supported languages. Create multiple Lambda functions to support the load. Use Amazon API Gateway as an entry point to the Lambda functions.
- D. Use a high performance computing (HPC) solution such as AWS ParallelCluster to establish an HPC cluster that can process the incoming requests at the appropriate scale.

Correct Answer: A

Community vote distribution

A (100%)

✉  **123jh10**  1 year, 5 months ago

Selected Answer: A

Less operational overhead means A: Fargate (no EC2), move the containers on ECS, autoscaling for growth and ALB to balance consumption.
 B - requires configure EC2
 C - requires add code (developpers)
 D - seems like the most complex approach, like re-architecting the app to take advantage of an HPC platform.
 upvoted 16 times

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

Selected Answer: A

key = LEAST operational overhead

Fargate a serverless service fully managed by aws

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html#:~:text=AWS%20Fargate%20is,optimize%20cluster%20packing>.

upvoted 1 times

✉  **Ruffyt** 4 months, 4 weeks ago

Less operational overhead means A: Fargate (no EC2), move the containers on ECS, autoscaling for growth and ALB to balance consumption.
 upvoted 1 times

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

Selected Answer: A

LEAST operational overhead = AWS Fargate

upvoted 1 times

✉  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

A is the best solution to meet the requirements with the least operational overhead. The key reasons are:

AWS Fargate removes the need to provision and manage servers. Fargate will automatically scale the application based on demand. This removes a significant operational burden.
 Using ECS along with Fargate provides a managed orchestration layer to easily run and scale the containerized application.
 The Application Load Balancer handles distribution of traffic without additional effort.
 No code changes are required to move the application to Fargate. The containers can run as-is.
 upvoted 2 times

✉  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

A is the correct answer.

AWS Fargate removes the need to provision and manage servers, allowing you to focus on deploying and running applications. Fargate will scale compute capacity up and down automatically based on application load. This removes the operational overhead of managing servers.

upvoted 1 times

✉  **james2033** 8 months, 1 week ago

Selected Answer: A

Existing: "containerized web-app", "minimum code changes + minimum development effort" --> AWS Fargate + Amazon Elastic Container Services (ECS). Easy question.

upvoted 1 times

 **MNotABot** 8 months, 2 weeks ago

A
Fargate, ECS, ASG, ALB....What else one will need for a nice sleep?
upvoted 2 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: A
Option A (AWS Fargate on Amazon ECS with Service Auto Scaling) is the best choice as it provides a serverless and managed environment for your containerized web application. It requires minimal code changes, offers automatic scaling, and utilizes an Application Load Balancer for request distribution.

Option B (Amazon EC2 instances with an Application Load Balancer) requires manual management of EC2 instances, resulting in more operational overhead compared to option A.

Option C (AWS Lambda with API Gateway) may require significant code changes and restructuring, introducing complexity and potentially increasing development effort.

Option D (AWS ParallelCluster) is not suitable for a containerized web application and involves significant setup and configuration overhead.

upvoted 3 times

 **Jeeva28** 10 months ago

Selected Answer: A
AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers. This removes the need to choose server types, decide when to scale your clusters, or optimize cluster packing.
upvoted 1 times

 **studynoplay** 10 months, 3 weeks ago

Selected Answer: A
Least Operational Overhead = Serverless
upvoted 1 times

 **airraid2010** 1 year ago

Selected Answer: A
AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers on clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale of virtual machines to run containers.

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html>
upvoted 1 times

 **Chalamalli** 1 year, 1 month ago

A is correct
upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: A
The best solution to meet the requirements with the least operational overhead is Option A: Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Use an Application Load Balancer to distribute the incoming requests.
upvoted 3 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A
Option A has minimum operational overhead and almost no application code changes.
upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

A is correct
upvoted 1 times

 **Six_Fingered_Jose** 1 year, 5 months ago

Selected Answer: A
Agreed with A,
lambda will work too but requires more operational overhead (more chores)

with A, you are just moving from an on-prem container to AWS container
upvoted 3 times

Question #113

Topic 1

A company uses 50 TB of data for reporting. The company wants to move this data from on premises to AWS. A custom application in the company's data center runs a weekly data transformation job. The company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible.

The data center does not have any available network bandwidth for additional workloads. A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud.

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

- A. Use AWS DataSync to move the data. Create a custom transformation job by using AWS Glue.
- B. Order an AWS Snowcone device to move the data. Deploy the transformation application to the device.
- C. Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. Create a custom transformation job by using AWS Glue.
- D. Order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Copy the data to the device. Create a new EC2 instance on AWS to run the transformation application.

Correct Answer: C

Community vote distribution

C (71%)

D (29%)

✉️  **123jh10**  1 year, 5 months ago

Selected Answer: C

A. Use AWS DataSync to move the data. Create a custom transformation job by using AWS Glue. - No BW available for DataSync, so "asap" will be weeks/months (?)
 B. Order an AWS Snowcone device to move the data. Deploy the transformation application to the device. - Snowcone will just store 14TB (SSD configuration).
 C. Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. Create a custom transformation job by using AWS Glue. - SnowBall can store 80TB (ok), takes around 1 week to move the device (faster than A), and AWS Glue allows to do ETL jobs. This is the answer.
 D. Order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Copy the data to the device. Create a new EC2 instance on AWS to run the transformation application. - Same as C, but the ETL job requires the deployment/configuration/maintenance of an EC2 instance, while Glue is serverless. This means D has more operational overhead than C.

upvoted 58 times

✉️  **remand** 1 year, 1 month ago

I disagree on D. transformation job is already in place.so, all you have to do is deploy and run on ec2.
 C takes more effort to build Glue process, like reinventing the wheel . this is unnecessary

upvoted 7 times

✉️  **jdr75** 11 months, 3 weeks ago

I agree. When it said "with least Operational overhead" , it does not takes in account "migration activities" neccesary to reach the "final photo/scenario". In "operational overhead" schema, you're situated in a "final scenario" and you've only take into account how do you operate it, and if the operation of that scheme is ALIGHTED (least effort to operate than original scenario), that's the desired state.

upvoted 3 times

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

Selected Answer: D

Why C? This answer misses the part between SnowBall and AWS Glue.
 D at least provides a full-step solution that copies data in snowball device, and installs the custom application in device's EC2 to do the transformation job.

upvoted 13 times

✉️  **happpieee** 3 weeks, 5 days ago

AWS Glue is not part of SnowBall Edge AWS services it can run within. Check it out here :
<https://docs.aws.amazon.com/snowball/latest/developer-guide/whatisedge.html>

upvoted 1 times

✉️  **pentium75** 3 months ago

Because AWS Glue means less "operational (!) overhead" than running an EC2 instance.

upvoted 4 times

✉️  **vip2**  1 month, 1 week ago

Selected Answer: C

Using an EC2 instance instead of a managed service like AWS Glue will include more operational overhead for the organization.

upvoted 2 times

 **cajilaxu** 1 month, 3 weeks ago

Selected Answer: C

C is right Answer!!

Get Up-To-Date <https://www.pinterest.com/pin/937522847419120352>

upvoted 2 times

 **Femmyte** 1 month, 3 weeks ago

Selected Answer: D

The answer is D because of the following key points

1. A custom application in the company's data center runs a weekly data transformation job. Which means that the company already has an application that runs the transformation.
2. A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud. This shows that the only responsibility of the architect is to transfer the data and configure the existing application to run on the EC2 the architect is going to deploy.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: C

A: Cannot be done because no bandwidth

B: Snowcone is probably to small

D: Doable by EC2 is overhead for transformation when Glue is an option

C: Is correct as Snowball Edge Storage Optimised device is good for storage and Glue can transform once the data is available

upvoted 1 times

 **bujuman** 2 months, 2 weeks ago

Selected Answer: C

C best suit for:

ETL jobs with LEAST operational overhead.

For my understanding, we need here to avoid operation or maintenance burden of the solution

upvoted 1 times

 **Shalen** 3 months, 4 weeks ago

Selected Answer: D

we use snowball to copy 50 PB

"The company plans to pause the application until the data transfer is complete "

and least overhead " hence C would be reinventing the wheel

upvoted 1 times

 **slimen** 4 months, 3 weeks ago

Selected Answer: D

which is faster?

- setup a glue cluster and adapt it to do the same analytical stuff as the original app

- simply run the same app in an EC2 instance?

upvoted 1 times

 **mach2022** 4 months, 3 weeks ago

How are we going to run the custom application using glue? that means more time to adapt the process instead of just running the app in ec2

upvoted 1 times

 **GB_12345** 5 months, 1 week ago

Selected Answer: D

Not A. AWS DataSync requires an internet connection & the question states no available bandwidth

Not B. SnowCone only has a max of 14 TB with an SSD, and the data is 50 TB

Not C. Snowball Edge doesn't support Glue

Supported services: <https://docs.aws.amazon.com/snowball/latest/developer-guide/whatisedge.html>

So the answer must be D, as Snowball Edge Storage Optimized does support EC2 & can store 80 TB for the version that supports compute resources

upvoted 5 times

 **TariqKipkemei** 6 months, 4 weeks ago

Selected Answer: C

Snowball Edge has storage and compute capabilities, can be used to support workload in offline locations.

Technically option D will work but with the overhead of EC2, negating the requirement for LEAST ops.

upvoted 1 times

 **slimen** 4 months, 3 weeks ago

which is faster?

- setup a glue cluster and adapt it to do the same analytical stuff as the original app

- simply run the same app in an EC2 instance?

upvoted 1 times

✉  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: C

The Snowball Edge Storage Optimized device allows transferring a large amount of data without using network bandwidth. Once the data is copied to the Snowball, AWS Glue can be used to create a custom ETL job to transform the data, avoiding the need to reconfigure the existing on-premises application. This meets the requirements to transfer the data with minimal operational overhead and configure the data transformation job to run in AWS.

upvoted 1 times

✉  **james2033** 8 months, 1 week ago

Selected Answer: C

AWS Glue for ETL (Extract, Transform, Load) <https://docs.aws.amazon.com/glue/latest/dg/how-it-works.html> is good for this case (transformation). Keyword "50 TB", "AWS Snowball". Choose C. Easy question.

upvoted 2 times

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

Selected Answer: C

A - no bandwidth, option out
B - snowcone SSD has max 14TB of capacity
C - is correct one here
D - cannot use Compute optimized as max capacity for this snowball is 39.5TB, and only that's why ;-)
<https://docs.aws.amazon.com/snowball/latest/developer-guide/device-differences.html>

upvoted 4 times

✉  **rcarmin** 8 months, 2 weeks ago

D answer says Snowball Edge STORAGE Optimized, which supports 80TB. 39.5TB is for the Snowball Edge COMPUTE Optimized.
upvoted 3 times

✉  **live_reply_developers** 8 months, 4 weeks ago

Selected Answer: D

"A custom application in the company's data center runs a weekly data transformation job."

"A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud."

LEAST operational overhead -> just take app and put on EC2, instead of configuring Glue
upvoted 1 times

✉  **rcarmin** 8 months, 2 weeks ago

IMHO, that's the least CONFIGURATION overhead, not operational. After you configure Glue, the operation should be easier than maintaining the EC2 and the transformation job.
upvoted 2 times

✉  **cookieMr** 9 months, 1 week ago

Option A (AWS DataSync with AWS Glue) involves using AWS DataSync for data transfer, which requires available network bandwidth. Since the data center has no additional network bandwidth, this option is not suitable.

Option B (AWS Snowcone device with deployment) is designed for smaller workloads and may not have enough storage capacity for transferring 50 TB of data. Additionally, deploying the transformation application on the Snowcone device could introduce complexity and operational overhead.

Option D (AWS Snowball Edge with EC2 compute) involves transferring the data using a Snowball Edge device and then creating a new EC2 instance in AWS to run the transformation application. This option adds additional complexity and operational overhead of managing an EC2 instance.

In comparison, option C offers a straightforward and efficient approach. The Snowball Edge Storage Optimized device can handle the large data transfer without relying on network bandwidth. Once the data is transferred, AWS Glue can be used to create the transformation job, ensuring the continuity of the application's processing in the AWS Cloud.

upvoted 4 times

✉  **rcarmin** 8 months, 2 weeks ago

My thoughts exactly. I think people are misunderstanding CONFIG for OPERATION overhead.

upvoted 2 times

Question #114

Topic 1

A company has created an image analysis application in which users can upload photos and add photo frames to their images. The users upload images and metadata to indicate which photo frames they want to add to their images. The application uses a single Amazon EC2 instance and Amazon DynamoDB to store the metadata.

The application is becoming more popular, and the number of users is increasing. The company expects the number of concurrent users to vary significantly depending on the time of day and day of week. The company must ensure that the application can scale to meet the needs of the growing user base.

Which solution meets these requirements?

- A. Use AWS Lambda to process the photos. Store the photos and metadata in DynamoDB.
- B. Use Amazon Kinesis Data Firehose to process the photos and to store the photos and metadata.
- C. Use AWS Lambda to process the photos. Store the photos in Amazon S3. Retain DynamoDB to store the metadata.
- D. Increase the number of EC2 instances to three. Use Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volumes to store the photos and metadata.

Correct Answer: A

Community vote distribution

C (100%)

✉️  **MXB05**  1 year, 5 months ago

Selected Answer: C

Do not store images in databases ;)... correct answer should be C
upvoted 38 times

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

Selected Answer: C

Solution C offloads the photo processing to Lambda. Storing the photos in S3 ensures scalability and durability, while keeping the metadata in DynamoDB allows for efficient querying of the associated information.

Option A does not provide an appropriate solution for storing the photos, as DynamoDB is not suitable for storing large binary data like images.

Option B is more focused on real-time streaming data processing and is not the ideal service for processing and storing photos and metadata in this use case.

Option D involves manual scaling and management of EC2 instances, which is less flexible and more labor-intensive compared to the serverless nature of Lambda. It may not efficiently handle the varying number of concurrent users and can introduce higher operational overhead.

In conclusion, option C provides the best solution for scaling the application to meet the needs of the growing user base by leveraging the scalability and durability of Lambda, S3, and DynamoDB.

upvoted 9 times

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

Selected Answer: C

Max size for DDB entry is 400KB.
upvoted 1 times

✉️  **aptx4869** 4 months, 4 weeks ago

Selected Answer: C

Images (Object) should go in S3 and metadata should go in database (DynamoDB)
upvoted 1 times

✉️  **Ruffyit** 4 months, 4 weeks ago

Solution C offloads the photo processing to Lambda. Storing the photos in S3 ensures scalability and durability, while keeping the metadata in DynamoDB allows for efficient querying of the associated information.

upvoted 1 times

✉️  **Ferna** 5 months ago

Selected Answer: C

Solution C
upvoted 1 times

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

Selected Answer: C

i think is only a confusion of the admin, because it has more sense to store the photos in a S3 bucket is logic.
upvoted 1 times

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

Selected Answer: C

A does not store data.
upvoted 1 times

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

Selected Answer: C

I stopped at option C
upvoted 1 times

✉ **sand44** 7 months ago

Selected Answer: C

c is correct
upvoted 1 times

✉ **Abdou1604** 7 months, 1 week ago

DynamoDB can technically store images as binary data (BLOBs)
upvoted 1 times

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

Selected Answer: C

Why one would store photos in DB
upvoted 2 times

✉ **MNotABot** 8 months, 2 weeks ago

This one is in exam
upvoted 7 times

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

Selected Answer: C

Option C is the best.
upvoted 1 times

✉ **MostafaWardany** 10 months, 1 week ago

Selected Answer: C

C is the correct answer, A can't store images in DB
upvoted 1 times

✉ **cheese929** 11 months ago

Selected Answer: C

Go for C which is able to scale
upvoted 1 times

✉ **TheAbsoluteTruth** 11 months, 4 weeks ago

Selected Answer: C

La opción A no es la solución más adecuada para manejar la carga potencialmente alta de usuarios simultáneos, ya que las instancias de Lambda tienen un límite de tiempo de ejecución y la carga alta puede causar un retraso significativo en la respuesta de la aplicación. Además, no se proporciona una solución escalable para almacenar las imágenes.

La opción C proporciona una solución escalable para el procesamiento y almacenamiento de imágenes y metadatos. La aplicación puede utilizar AWS Lambda para procesar las fotos y almacenar las imágenes en Amazon S3, que es un servicio de almacenamiento escalable y altamente disponible. Los metadatos pueden almacenarse en DynamoDB, que es un servicio de base de datos escalable y de alto rendimiento que puede manejar una gran cantidad de solicitudes simultáneas.

upvoted 3 times

✉ **cookieMr** 9 months, 1 week ago

Si Señior Siarra!

upvoted 1 times

Question #115

Topic 1

A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.

A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.

Which change to the network architecture should a solutions architect recommend to meet this requirement?

- A. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.
- B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.
- C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.
- D. Remove the internet gateway from the VPC. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

Option A (creating a NAT gateway) would not meet the requirement since it still involves sending traffic to S3 over the internet. NAT gateway is used for outbound internet connectivity from private subnets, but it doesn't provide a private route for accessing S3.

Option B (configuring security groups) focuses on controlling outbound traffic using security groups. While it can restrict outbound traffic, it doesn't provide a private route for accessing S3.

Option D (setting up Direct Connect) involves establishing a dedicated private network connection between the on-premises environment and AWS. While it offers private connectivity, it is more suitable for hybrid scenarios and not necessary for achieving private access to S3 within the VPC.

In summary, option C provides a straightforward solution by moving the EC2 instances to private subnets, creating a VPC endpoint for S3, and linking the endpoint to the route table for private subnets. This ensures that file transfer traffic between the EC2 instances and S3 remains within the private network without going over the internet.

upvoted 10 times

✉️  **Ruffyit**  4 months, 4 weeks ago

C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.

upvoted 1 times

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

Selected Answer: C

Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.

upvoted 1 times

✉️  **sand444** 7 months ago

Selected Answer: C

link VPC endpoint in route tables ---- EC2 instance to communicate S3 with a private connection in VPC

upvoted 1 times

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

Selected Answer: C

According to the well-designed framework, option C is the safest and most efficient option.

upvoted 3 times

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

Selected Answer: C

The correct answer is C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.

To meet the new requirement of transferring files over a private route, the EC2 instances should be moved to private subnets, which do not have direct access to the internet. This ensures that the traffic for file transfers does not go over the internet.

To enable the EC2 instances to access Amazon S3, a VPC endpoint for Amazon S3 can be created. VPC endpoints allow resources within a VPC to

communicate with resources in other services without the traffic being sent over the internet. By linking the VPC endpoint to the route table for the private subnets, the EC2 instances can access Amazon S3 over a private connection within the VPC.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option A (Create a NAT gateway) would not work, as a NAT gateway is used to allow resources in private subnets to access the internet, while the requirement is to prevent traffic from going over the internet.

Option B (Configure the security group for the EC2 instances to restrict outbound traffic) would not achieve the goal of routing traffic over a private connection, as the traffic would still be sent over the internet.

Option D (Remove the internet gateway from the VPC and set up an AWS Direct Connect connection) would not be necessary, as the requirement can be met by simply creating a VPC endpoint for Amazon S3 and routing traffic through it.

upvoted 1 times

 **Kayamables** 1 year, 2 months ago

How about the question of moving the instances across subnets. Because according to AWS you can't do it.

<https://aws.amazon.com/premiumsupport/knowledge-center/move-ec2-instance/#:~:text=It%27s%20not%20possible%20to%20move,%2C%20Availability%20Zone%2C%20or%20VPC.>

Kindly clarify. Maybe I miss something.

upvoted 1 times

 **pentium75** 3 months ago

You can't just change the subnet in instance settings, but this article mentions how you CAN move the instance manually.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

 **ocbn3wby** 1 year, 3 months ago

C is correct.

There is no requirement for public access from internet.

Application must be moved in Private subnet. This is a prerequisite in using VPC endpoints with S3

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 4 times

 **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

 **Jtic** 1 year, 4 months ago

Selected Answer: C

Use VPC endpoint

upvoted 1 times

 **Jtic** 1 year, 4 months ago

Selected Answer: C

User VPC endpoint and make the EC2 private

upvoted 1 times

 **Jtic** 1 year, 4 months ago

Use VPC endpoint

upvoted 1 times

 **backbencher2022** 1 year, 4 months ago

Selected Answer: C

VPC endpoint is the best choice to route S3 traffic without traversing internet. Option A alone can't be used as NAT Gateway requires an Internet gateway for outbound internet traffic. Option B would still require traversing through internet and option D is also not a suitable solution

upvoted 3 times

Question #116

Topic 1

A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome. The company is redesigning its website and wants a new solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security.

Which combination of changes will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Configure Amazon CloudFront in front of the website to use HTTPS functionality.
- B. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality.
- C. Create and deploy an AWS Lambda function to manage and serve the website content.
- D. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled.
- E. Create the new website. Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

Correct Answer: AD*Community vote distribution*

palermo777 Highly Voted 1 year, 5 months ago

A -> We can configure CloudFront to require HTTPS from clients (enhanced security)
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to-cloudfront.html>
D -> storing static website on S3 provides scalability and less operational overhead, then configuration of Application LB and EC2 instances (hence E is out)

B is out since AWS WAF Web ACL does not provide HTTPS functionality, but to protect HTTPS only.
upvoted 32 times

Six_Fingered_Jose Highly Voted 1 year, 5 months ago

Selected Answer: AD

agree with A and D

static website -> obviously S3, and S3 is super scalable
CDN -> CloudFront obviously as well, and with HTTPS security is enhanced.

B does not make sense because you are not replacing the CDN with anything,
E works too but takes too much effort and compared to S3, S3 still wins in term of scalability. plus why use EC2 when you are only hosting static website

upvoted 7 times

aussiehoa 10 months, 3 weeks ago

does not need to have any dynamic content available
upvoted 1 times

Lalo 9 months, 2 weeks ago

Amazon CloudFront is for Securely deliver content with low latency and high transfer speeds
But what about the SQL injection XSS attacks? we use WAF and also use HTTPS
<https://www.f5.com/glossary/web-application-firewall-waf#:~:text=A%20WAF%20protects%20your%20web,and%20what%20traffic%20is%20safe.>
WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app.
Answer is WAF Not Cloudfront

upvoted 1 times

David_Ang Most Recent 5 months, 2 weeks ago

Selected Answer: AD

these answers are the most common use case for real companies, is like the answers that have more sense
upvoted 1 times

tom_cruise 5 months, 2 weeks ago

Selected Answer: AD

Web Application Firewall creates rules to block attacks, but it does not create HTTPS. It can only allow HTTPS inbound traffic.
upvoted 1 times

TariqKipkemei 6 months, 4 weeks ago

Selected Answer: AD

Scalability, enhanced security and less operational overhead = CloudFront with HTTPS
Scalability and less operational overhead = S3 bucket with static website hosting

upvoted 2 times

✉ **cookieMr** 9 months, 1 week ago

Selected Answer: AD

A. Amazon CloudFront provides scalable content delivery with HTTPS functionality, meeting security and scalability requirements.

D. Deploying the website on an Amazon S3 bucket with static website hosting reduces operational overhead by eliminating server maintenance and patching.

Why other options are incorrect:

B. AWS WAF does not provide HTTPS functionality or address patching and maintenance.

C. Using AWS Lambda introduces complexity and does not directly address patching and maintenance.

E. Managing EC2 instances and an Application Load Balancer increases operational overhead and does not minimize patching and maintenance tasks.

In summary, configuring Amazon CloudFront for HTTPS and deploying on Amazon S3 with static website hosting provide security, scalability, and reduced operational overhead.

upvoted 1 times

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

Selected Answer: AD

AD

A for enhanced security D for static content

upvoted 1 times

✉ **studynoplay** 10 months, 3 weeks ago

Selected Answer: AD

LEAST operational overhead = Serverless

<https://aws.amazon.com/serverless/>

upvoted 2 times

✉ **angolateoria** 10 months, 4 weeks ago

AD misses the operational part, how can the app work without a lambda function, an EC2 instance or something?

upvoted 1 times

✉ **darn** 11 months, 1 week ago

Selected Answer: AD

people do not seem to get the LEAST OPERATIONAL OVERHEAD statement, many people keep voting for options that bring far too Op work

upvoted 1 times

✉ **channn** 11 months, 3 weeks ago

Selected Answer: AD

A for enhanced security

D for static content

upvoted 2 times

✉ **Erbug** 1 year ago

Since Amazon S3 is unlimited and you pay as you go so it means there will be no limit to scale as long as your data is going to grow, so D is one of the correct answers and another correct answer is A, because of this:

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

so my answer is AD.

upvoted 1 times

✉ **ManOnTheMoon** 1 year, 1 month ago

I vote A & C for the reason being least operational overhead.

upvoted 1 times

✉ **Yelizaveta** 1 year, 1 month ago

Selected Answer: AD

Here a perfect explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>

upvoted 2 times

✉ **Abdel42** 1 year, 1 month ago

Selected Answer: AD

Simple and secure

upvoted 1 times

✉ **remand** 1 year, 2 months ago

Selected Answer: AD

- D. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled.
A. Configure Amazon CloudFront in front of the website to use HTTPS functionality.

By deploying the website on an S3 bucket with static website hosting enabled, the company can take advantage of the high scalability and cost-efficiency of S3 while also reducing the operational overhead of managing and patching a CMS.

By configuring Amazon CloudFront in front of the website, it will automatically handle the HTTPS functionality, this way the company can have a secure website with very low operational overhead.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: CD

KEYWORD: LEAST operational overhead

D. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled.

C. Create and deploy an AWS Lambda function to manage and serve the website content.

Option D (using Amazon S3 with static website hosting) would provide high scalability and enhanced security with minimal operational overhead because it requires little maintenance and can automatically scale to meet increased demand.

Option C (using an AWS Lambda function) would also provide high scalability and enhanced security with minimal operational overhead. AWS Lambda is a serverless compute service that runs your code in response to events and automatically scales to meet demand. It is easy to set up and requires minimal maintenance.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Why other options are not correct?

Option A (using Amazon CloudFront) and Option B (using an AWS WAF web ACL) would provide HTTPS functionality but would require additional configuration and maintenance to ensure that they are set up correctly and remain secure.

Option E (using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer) would provide high scalability, but it would require more operational overhead because it involves managing and maintaining EC2 instances.

upvoted 1 times

 **pentium75** 3 months ago

You're asked for a "combination of changes", not for two alternatives. D already covers the hosting part, now we need the security which is A.

upvoted 1 times

Question #117

Topic 1

A company stores its application logs in an Amazon CloudWatch Logs log group. A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in near-real time. Which solution will meet this requirement with the LEAST operational overhead?

- A. Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
- B. Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
- C. Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery streams sources. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.
- D. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

Correct Answer: C

Community vote distribution



Six_Fingered_Jose Highly Voted 1 year, 5 months ago

Selected Answer: A

answer is A

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

> You can configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in NEAR REAL-TIME through a CloudWatch Logs subscription

least overhead compared to kinesis

upvoted 80 times

HayLLIHuK 1 year, 2 months ago

Zerotn3 is right! There should be a Lambda for writing into ES

upvoted 1 times

UWSFish 1 year, 5 months ago

Great link. Convinced me

upvoted 5 times

Zerotn3 1 year, 2 months ago

Option A (Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service)) is not a suitable option, as a CloudWatch Logs subscription is designed to send log events to a destination such as an Amazon Simple Notification Service (Amazon SNS) topic or an AWS Lambda function. It is not designed to write logs directly to Amazon Elasticsearch Service (Amazon ES).

upvoted 4 times

kucyk 1 year, 1 month ago

that is not true, you can stream logs from CloudWatch Logs directly to OpenSearch

upvoted 7 times

Buruguduystunstugudunstuy Highly Voted 1 year, 3 months ago

Selected Answer: C

The correct answer is C: Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery stream source. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.

This solution uses Amazon Kinesis Data Firehose, which is a fully managed service for streaming data to Amazon OpenSearch Service (Amazon Elasticsearch Service) and other destinations. You can configure the log group as the source of the delivery stream and Amazon OpenSearch Service as the destination. This solution requires minimal operational overhead, as Kinesis Data Firehose automatically scales and handles data delivery, transformation, and indexing.

upvoted 17 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Option A: Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service) would also work, but it may require more operational overhead as you would need to set up and manage the subscription and ensure that the logs are delivered in near-real time.

Option B: Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service) would also work, but it may require more operational overhead as you would need to set up and manage the Lambda function and ensure that it scales to handle the incoming logs.

Option D: Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service) would also work, but it may require more operational overhead as you would need to install and configure the Kinesis Agent on each application server and set up and manage the Kinesis Data Streams.

upvoted 2 times

 **ocbn3wby** 1 year, 1 month ago

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 1 times

 **Lalo** 9 months, 2 weeks ago

ANSWER A

<https://docs.aws.amazon.com/opensearch-service/latest/developerguide/integrations.html>

You can use CloudWatch or Kinesis, but in the Kinesis description it never says real time, however in the Cloudwatch description it does say Real time ""You can load streaming data from CloudWatch Logs to your OpenSearch Service domain by using a CloudWatch Logs subscription . For information about Amazon CloudWatch subscriptions, see Real-time processing of log data with subscriptions.""

upvoted 2 times

 **CloudLearner01** Most Recent 3 weeks, 2 days ago

A is correct

You can configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in near real-time through a CloudWatch Logs subscription.

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 1 times

 **vip2** 1 month, 1 week ago

Selected Answer: A

You can configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in near real-time through a CloudWatch Logs subscription. This is the solution that requires the least operational overhead.

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 1 times

 **eyob911** 1 month, 2 weeks ago

A,

You can configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in near real-time through a CloudWatch Logs subscription

upvoted 1 times

 **Varun_SP** 2 months ago

Selected Answer: C

Amazon Kinesis Data Firehose can automatically deliver logs from CloudWatch Logs to Amazon OpenSearch Service without requiring you to manage and configure additional components or write custom code. It simplifies the process and reduces operational overhead

upvoted 1 times

 **bujuman** 2 months, 2 weeks ago

Selected Answer: C

Following these key words:

- near-real time.
- LEAST operational overhead and the fact that CloudWatch loggroup support OpenSearch Service subscription filter

upvoted 1 times

 **pentium75** 3 months ago

Selected Answer: A

Since the scenario perfectly fits this description: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 2 times

 **SaurabhTiwari1** 3 months, 1 week ago

Selected Answer: A

The solution that will meet the requirement with the least operational overhead is:

Option A: Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

This option allows you to directly stream logs from CloudWatch to OpenSearch Service (Elasticsearch Service) in near-real time without the need for additional services or resources, thus minimizing operational overhead. The other options involve additional services (Lambda, Kinesis Data Firehose, Kinesis Data Streams) and would therefore require more operational management.

upvoted 1 times

 **Marco_St** 4 months ago

Selected Answer: A

A, C can both support near-real-time logs transfer to OpenSearch. But it depends on the current needs. Based on the context of question, Option A is the best one.

For Option C: This Kinesis Data Firehose offers additional benefits like easy scaling, built-in failure handling, and potential for data transformation if needed. But these are not required by the question. It only requires LEAST overhead-operation and near-real-time transfer then A is straightforward.

upvoted 1 times

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

Selected Answer: C

You need real time buffer like Kinesis, otherwise you are going to lose data.

upvoted 1 times

✉ **SohamSLP** 3 months ago

Pretty sure A supports near-real-time transfer

upvoted 1 times

✉ **cheroh_tots** 2 weeks, 5 days ago

They both do, but C has the least operational overhead.

upvoted 1 times

✉ **mhka1988** 5 months, 1 week ago

Selected Answer: A

It is possible to configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in near realtime through a CloudWatch Logs subscription which implies less ops overhead.

upvoted 1 times

✉ **OlehKom** 5 months, 2 weeks ago

Selected Answer: C

"A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in !!!near-real time!!!!."

Amazon Kinesis Data Firehose captures and loads data in near real time. It loads new data into Amazon S3, Amazon Redshift, and Amazon OpenSearch Service within 60 seconds after the data is sent to the service. As a result, you can access new data sooner and react to business and operational events faster.

upvoted 2 times

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

Selected Answer: C

You need kinesis as a buffer in between, otherwise, the logs will be lost if anything goes wrong.

upvoted 1 times

✉ **mohamoha** 5 months, 2 weeks ago

Selected Answer: A

You can configure a CloudWatch Logs log group to stream data it receives to Amazon OpenSearch Service cluster in near real-time through a CloudWatch Logs subscription.

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 2 times

✉ **JKevin778** 6 months ago

Selected Answer: C

100% C.

CloudWatch logs cannot be send to OpenSearch directly, need KDS or KDF works in the middle.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/SubscriptionFilters.html>

upvoted 1 times

✉ **hootani** 6 months, 2 weeks ago

Selected Answer: C

The answer is C

upvoted 1 times

Question #118

Topic 1

A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totaling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.

Which storage solution meets these requirements MOST cost-effectively?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon OpenSearch Service (Amazon Elasticsearch Service)
- D. Amazon S3

Correct Answer: D

Community vote distribution



✉️ **Azure55** 4 months, 3 weeks ago

Selected Answer: D

the cost of S3 < EFS < EBS

upvoted 13 times

✉️ **cookieMr** 9 months, 1 week ago

Selected Answer: D

Amazon S3 (Simple Storage Service) is a highly scalable and cost-effective storage service. It is well-suited for storing large amounts of data, such as the 900 TB of text documents mentioned in the scenario. S3 provides high durability, availability, and performance.

Option A (Amazon EBS) is block storage designed for individual EC2 instances and may not scale as seamlessly and cost-effectively as S3 for large amounts of data.

Option B (Amazon EFS) is a scalable file storage service, but it may not be the most cost-effective option compared to S3, especially for the anticipated storage size of 900 TB.

Option C (Amazon OpenSearch Service) is a search and analytics service and may not be suitable as the primary storage solution for the text documents.

In summary, Amazon S3 is the recommended choice as it offers high scalability, cost-effectiveness, and durability for storing the large repository of text documents required by the web application.

upvoted 6 times

✉️ **theochan** 2 months, 1 week ago

Option A : EBS can't be multi-AZ

Option B: EFS is expensive

Option C: ElasticSearch is not for storing

upvoted 3 times

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

Selected Answer: D

D is the only real solution here. S3 is the cheapest option for storage and it can scale indefinitely.

upvoted 3 times

✉️ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

MOST cost-effective = S3 (unless explicitly stated in the requirements)

upvoted 2 times

✉️ **Jeeva28** 10 months ago

Selected Answer: D

900 in the question to divert our Thinking. When you have keyword least in question S3 will be only thing we should look

upvoted 1 times

✉️ **Abrar2022** 10 months ago

EFS and S3 meet the requirements but S3 is a better option because it is cheaper.

upvoted 1 times

✉️ **studynoplay** 10 months, 3 weeks ago

Selected Answer: D

MOST cost-effective = S3 (unless explicitly stated in the requirements)
upvoted 2 times

 **Robrobtutu** 11 months, 1 week ago

Selected Answer: D

S3 is the cheapest and most scalable.
upvoted 1 times

 **jdr75** 11 months, 3 weeks ago

Selected Answer: C

Now in OpenSearch you can reach at 3 PB so option C is better.
With S3 in an intensive scenario the costs of retrieving the buckets could be high.
Yes OpenSearch is NOT cheap but this has to be analysed carefully.
So, I opt "C" to increase the discussion.

With UltraWarm, you can retain up to 3 PB of data on a single Amazon OpenSearch Service cluster, while reducing your cost per GB by nearly 90% compared to the warm storage tier. You can also easily query and visualize the data in your Kibana interface (version 7.10 and earlier) or OpenSearch Dashboards. Analyze both your recent (weeks) and historical (months or years) log data without spending hours or days restoring archived logs.

<https://aws.amazon.com/es/opensearch-service/features/>
upvoted 2 times

 **Dr_Chomp** 11 months, 3 weeks ago

EFS is a good option but expensive alongside S3 and customer concerned about cost - thus: S3 (D)
upvoted 2 times

 **frenzoid** 1 year ago

I wonder why people choose S3, yet S3 max capacity is 5TB 😳.
upvoted 2 times

 **frenzoid** 1 year ago

My bad, the 5TB limit is for individual files. S3 has virtually unlimited storage capacity.
upvoted 6 times

 **Help2023** 1 year, 1 month ago

Selected Answer: D

A. It is Not a block storage
B. It is Not a file storage
C. Opensearch is useful but can only accommodate up to 600TiB and is mainly for search and analytics.
D. S3 is more cost effective than all and can handle all objects like Block, File or Text.
upvoted 4 times

 **remand** 1 year, 2 months ago

Selected Answer: D

D. Amazon S3

Amazon S3 is an object storage service that can store and retrieve large amounts of data at any time, from anywhere on the web. It is designed for high durability, scalability, and cost-effectiveness, making it a suitable choice for storing a large repository of text documents. With S3, you can store and retrieve any amount of data, at any time, from anywhere on the web, and you can scale your storage up or down as needed, which will help to meet the demand of the web application. Additionally, S3 allows you to choose between different storage classes, such as standard, infrequent access, and archive, which will enable you to optimize costs based on your specific use case.

upvoted 1 times

 **SilentMilli** 1 year, 2 months ago

Selected Answer: D

The most cost-effective storage solution for a web application that needs to scale to meet high demand and store a large repository of text documents would be Amazon S3. Amazon S3 is an object storage service that is designed for durability, availability, and scalability. It can store and retrieve any amount of data from anywhere on the internet, making it a suitable choice for storing a large repository of text documents. Additionally, Amazon S3 is designed to be highly scalable and can easily handle periods of high demand without requiring any additional infrastructure or maintenance.

upvoted 2 times

 **gustavtd** 1 year, 2 months ago

Selected Answer: D

Is there anything cheaper than S3?
upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: D

D. Amazon S3 is the most cost-effective storage solution that meets the requirements described.

Amazon S3 is an object storage service that is designed to store and retrieve large amounts of data from anywhere on the web. It is highly scalable, highly available, and cost-effective, making it an ideal choice for storing a large repository of text documents that will experience periods of high

demand. S3 is a standalone storage service that can be accessed from anywhere, and it is designed to handle large numbers of objects, making it well-suited for storing the 900 TB repository of text documents described in the scenario. It is also designed to handle high levels of demand, making it suitable for handling periods of high demand.

upvoted 1 times

Question #119

Topic 1

A global company is using Amazon API Gateway to design REST APIs for its loyalty club users in the us-east-1 Region and the ap-southeast-2 Region. A solutions architect must design a solution to protect these API Gateway managed REST APIs across multiple accounts from SQL injection and cross-site scripting attacks.

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

- A. Set up AWS WAF in both Regions. Associate Regional web ACLs with an API stage.
- B. Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules.
- C. Set up AWS Shield in both Regions. Associate Regional web ACLs with an API stage.
- D. Set up AWS Shield in one of the Regions. Associate Regional web ACLs with an API stage.

Correct Answer: A

Community vote distribution

B (69%)

A (31%)

✉ **Gil80** 1 year, 4 months ago

Selected Answer: B

If you want to use AWS WAF across accounts, accelerate WAF configuration, automate the protection of new resources, use Firewall Manager with AWS WAF

upvoted 33 times

✉ **slimen** 4 months, 3 weeks ago

they didn't mention multiple accounts! only 2 regions

upvoted 2 times

✉ **baku98** 3 months, 2 weeks ago

B is wrong: AWS Firewall Manager cannot create security policies across regions.

Q: Can I create security policies across regions? No, AWS Firewall Manager security policies are region specific. Each Firewall Manager policy can only include resources available in that specified AWS Region. You can create a new policy for each region where you operate.

[https://aws.amazon.com/firewall-](https://aws.amazon.com/firewall-manager/faqs/#:~:text=No%20AWS%20Firewall%20Manager%20security,in%20that%20specified%20AWS%20Region.)

manager/faqs/#:~:text=No%20AWS%20Firewall%20Manager%20security,in%20that%20specified%20AWS%20Region.

upvoted 2 times

✉ **mauroicardi** 1 week, 4 days ago

AWS Firewall Manager is integrated with AWS Organizations so you can enable AWS WAF rules, AWS Shield Advanced protections, VPC security groups, AWS Network Firewalls, and Amazon Route 53 Resolver DNS Firewall rules across multiple AWS accounts and resources from a single place.

upvoted 1 times

✉ **pentium75** 3 months ago

That's why B says that you "set up AWS Firewall Manager IN BOTH REGIONS". Still you can "centrally configure" WAF per region, so that you don't have to attach WAF to every individual API.

upvoted 4 times

✉ **Nigma** 1 year, 4 months ago

B

Using AWS WAF has several benefits. Additional protection against web attacks using criteria that you specify. You can define criteria using characteristics of web requests such as the following:

Presence of SQL code that is likely to be malicious (known as SQL injection).

Presence of a script that is likely to be malicious (known as cross-site scripting).

AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for a variety of protections.

<https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

upvoted 16 times

✉ **JayBee65** 1 year, 3 months ago

Q: Can I create security policies across regions?

No, AWS Firewall Manager security policies are region specific. Each Firewall Manager policy can only include resources available in that specified AWS Region. You can create a new policy for each region where you operate.

So you could not centrally (i.e. in one place) configure policies, you would need to do this in each region

upvoted 2 times

✉ **pentium75** 3 months ago

"Centrally" on the Firewall Manager per region, as opposed to individually for every single API.

upvoted 1 times

 **TilTil** Most Recent 6 days, 12 hours ago

Selected Answer: A
WAF deals well with the types of attacks mentioned. XSS and SQL Injection are both app level attacks hence needs a WAF.

upvoted 1 times

 **sirasdf** 1 month ago

B

Option A involves setting up AWS WAF in both regions and associating regional web ACLs with an API stage. While this can provide the necessary protection, it requires more manual configuration in each region, potentially leading to more administrative effort, especially if there are updates or changes needed to be made across multiple regions.

Therefore, Option B is likely to require the least amount of administrative effort.

upvoted 1 times

 **killbots** 1 month, 3 weeks ago

Selected Answer: A
Original architecture does not have WAFs. B assumes there are WAFs already in place and why would you want to deploy a Firewall Manager to manage 1 Firewall? it adds unnecessary administrative tasks and costs for a tool that is not needed. You would want that if you were managing 10+ Firewalls not just one. A makes the most sense.

upvoted 3 times

 **thewalker** 1 month, 3 weeks ago

Selected Answer: B

B is the answer

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: B

B is basically A but with least admin overhead.

upvoted 1 times

 **1Alpha1** 3 months ago

Selected Answer: A

Are AWS firewall Manager security policies region specific?

Q: Can I create protection policies across regions? No, Amazon Firewall Manager protection policies are region specific. Each Firewall Manager policy can only include resources available in that specified Amazon Web Services Region. You can create a new policy for each region where you operate.

upvoted 1 times

 **djgodzilla** 3 months ago

AW FW manager demo:

<https://youtu.be/fwFHTxtSN2M>

upvoted 1 times

 **Murtadhaceit** 3 months, 3 weeks ago

Selected Answer: A

For "SQL injection and cross-site scripting attacks" use AWS WAF:

<https://aws.amazon.com/waf/features/>

upvoted 2 times

 **pentium75** 3 months ago

Y, but WAF is also involved in B, just centrally configured by Firewall Manager

upvoted 1 times

 **slimen** 4 months, 3 weeks ago

Selected Answer: A

the question mentioned 2 regions not 2 accounts

WAF is more suitable here with less effort than Firewall Manager!

upvoted 2 times

 **cosmiccliff** 4 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html#:~:text=AWS%20Firewall%20Manager%20simplifies,new%20accounts%20and%20resources.>

upvoted 1 times

 **ronin201** 4 months, 3 weeks ago

One question for those who voted for B, how WAF manager protect APIGW from SQL injection and etc w/o WAF. WAF manager is not FW!!!

upvoted 1 times

✉ **pentium75** 3 months ago

B specifically says that you use Firewall Manager to configure WAF, and protecting from SQL injection is exactly what WAF does.
upvoted 1 times

✉ **Abitek007** 5 months, 2 weeks ago

Selected Answer: A

you can as well use Firewall Manager, but the question says least operational overhead
upvoted 2 times

✉ **pentium75** 3 months ago

No, it says "least administrative effort".
upvoted 2 times

✉ **Valder21** 6 months, 3 weeks ago

Selected Answer: A

SQL injection, cross-site scripting = WAF
upvoted 2 times

✉ **pentium75** 3 months ago

WAF is also in B
upvoted 3 times

✉ **Hassao0** 6 months, 3 weeks ago

A is Right Option
<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-aws-waf.html>
upvoted 1 times

✉ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

B is the correct answer.

Using AWS Firewall Manager to centrally configure AWS WAF rules provides the least administrative effort compared to the other options.

Firewall Manager allows centralized administration of AWS WAF rules across multiple accounts and Regions. WAF rules can be defined once in Firewall Manager and automatically applied to APIs in all the required Regions and accounts.

upvoted 1 times

Question #120

Topic 1

A company has implemented a self-managed DNS solution on three Amazon EC2 instances behind a Network Load Balancer (NLB) in the us-west-2 Region. Most of the company's users are located in the United States and Europe. The company wants to improve the performance and availability of the solution. The company launches and configures three EC2 instances in the eu-west-1 Region and adds the EC2 instances as targets for a new NLB.

Which solution can the company use to route traffic to all the EC2 instances?

- A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.
- B. Create a standard accelerator in AWS Global Accelerator. Create endpoint groups in us-west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups.
- C. Attach Elastic IP addresses to the six EC2 instances. Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instances. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.
- D. Replace the two NLBs with two Application Load Balancers (ALBs). Create an Amazon Route 53 latency routing policy to route requests to one of the two ALBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

Correct Answer: A*Community vote distribution*

dokaedu Highly Voted 1 year, 4 months ago

B is the correct one for self manage DNS

If need to use Route53, ALB (layer 7) needs to be used as end points for 2 regions x 3 EC2s, if it the case answer would be the option 4
upvoted 17 times

MutiverseAgent 8 months, 2 weeks ago

After reading the discussion I think the right answer is B, as the service they use is DNS it does not make sense using a cloudfront distribution for this. The scenario would be different if the service were HTTP/HTTPS.

upvoted 3 times

MutiverseAgent 8 months, 2 weeks ago

Just to complete my previous comment. If the scenario were that the company uses HTTP/HTTPS service, then the correct answer (as the original dokaedu message mentions) would be option D)

upvoted 1 times

RNess 5 months, 1 week ago

Why I need replace NLB to ALB?

upvoted 2 times

pentium75 3 months ago

Who said that?

upvoted 2 times

LeGlopier Highly Voted 1 year, 5 months ago

Selected Answer: B

for me it is B

upvoted 12 times

rityoui Most Recent 3 weeks, 3 days ago

Selected Answer: B

i choose a previous until i checked google that tells me "DNS is an Application-layer protocol"

upvoted 1 times

thewalker 1 month, 3 weeks ago

Selected Answer: A

A seems the right answer.

upvoted 1 times

pentium75 3 months ago

Selected Answer: B

Not A: CloudFront is not for DNS

Not C: Involves CloudFront which is not needed, otherwise would work but ignore the NLBs

Not D: ALB can't handle DNS

Leaves B

upvoted 2 times

 **SaurabhTiwari1** 3 months, 1 week ago

Selected Answer: B

Keyword-

AWS global accelerator = Super cop (who direct the traffic and give you the best way to reach your destination)

Geolocation is use for showing web content as you want to show your web content to particular country or continent.
Geolocation has nothing to do with traffic.

upvoted 1 times

 **SaurabhTiwari1** 3 months, 1 week ago

Route 53 geolocation has nothing to do with traffic in the sense that it does not affect the amount or speed of traffic that reaches your resources. It only affects how Route 53 responds to DNS queries based on the location of your users.

upvoted 1 times

 **Masakichen** 4 months ago

Option B. Create a standard accelerator in AWS Global Accelerator. Establish endpoint groups in us-west-2 and eu-west-1. Add two NLBs as endpoints of the endpoint group.

AWS Global Accelerator is a network service that can provide a global traffic management solution. By creating a standard accelerator in AWS Global Accelerator, you can guide user traffic to the endpoint closest to them, thereby improving the performance and availability of the application. In this case, you can establish endpoint groups in the us-west-2 and eu-west-1 regions, and add two NLBs as endpoints. In this way, no matter where the user is located, their requests will be routed to the EC2 instance closest to them, thereby improving the performance and availability of DNS resolution. In addition, this design can also provide flexibility and scalability to handle a large amount of traffic. Therefore, this solution can meet your needs.

upvoted 4 times

 **Ruffyit** 4 months, 4 weeks ago

Global Accelerator: AWS Global Accelerator is designed to improve the availability and performance of applications by using static IP addresses (Anycast IPs) and routing traffic over the AWS global network infrastructure.

Endpoint Groups: By creating endpoint groups in both the us-west-2 and eu-west-1 Regions, the company can effectively distribute traffic to the NLBs in both Regions. This improves availability and allows traffic to be directed to the closest Region based on latency.

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: B

Key: route traffic to all the EC2 instances

upvoted 2 times

 **Hassao0** 6 months, 3 weeks ago

B. Create a standard accelerator in AWS Global Accelerator. Create endpoint groups in us-west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups.

Here's why this option is the most suitable:

Global Accelerator: AWS Global Accelerator is designed to improve the availability and performance of applications by using static IP addresses (Anycast IPs) and routing traffic over the AWS global network infrastructure.

Endpoint Groups: By creating endpoint groups in both the us-west-2 and eu-west-1 Regions, the company can effectively distribute traffic to the NLBs in both Regions. This improves availability and allows traffic to be directed to the closest Region based on latency.

upvoted 3 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

B is the best solution to route traffic to all the EC2 instances across regions.

The key reasons are:

AWS Global Accelerator allows routing traffic to endpoints in multiple AWS Regions. It uses the AWS global network to optimize availability and performance.

Creating an accelerator with endpoint groups in us-west-2 and eu-west-1 allows traffic to be distributed across both regions.

Adding the NLBs in each region as endpoints allows the traffic to be routed to the EC2 instances behind them.

This provides improved performance and availability compared to just using Route 53 geolocation routing.

upvoted 3 times

 **MNotABot** 8 months, 2 weeks ago

B

route requests to one of the two NLBs --> hence AD out / Attach Elastic IP addresses --> who will pay for it?

upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B

Option B offers a global solution by utilizing Global Accelerator. By creating a standard accelerator and configuring endpoint groups in both Regions, the company can route traffic to all the EC2 across multiple regions. Adding the two NLBs as endpoints ensures that traffic is distributed effectively.

Option A does not directly address the requirement of routing traffic to all EC2 instances. It focuses on routing based on geolocation and using CloudFront as a distribution, which may not achieve the desired outcome.

Option C involves managing Elastic IP addresses and routing based on geolocation. However, it may not provide the same level of performance and availability as AWS Global Accelerator.

Option D focuses on ALBs and latency-based routing. While it can be a valid solution, it does not utilize AWS Global Accelerator and may require more configuration and management compared to option B.

upvoted 3 times

 **beginnercloud** 9 months, 2 weeks ago

Selected Answer: B

Correctly is B.

if it is self-managed DNS, you cannot use Route 53. There can be only 1 DNS service for the domain.

upvoted 3 times

 **studynoplay** 10 months, 3 weeks ago

Selected Answer: B

For self-managed DNS solution:

<https://aws.amazon.com/blogs/security/how-to-protect-a-self-managed-dns-service-against-ddos-attacks-using-aws-global-accelerator-and-aws-shield-advanced/>

upvoted 2 times

 **studynoplay** 10 months, 3 weeks ago

Selected Answer: B

Re-wording the correct explanations here:

if it is self-managed DNS, you cannot use Route 53. There can be only 1 DNS service for the domain. If the question didn't mention self-managed DNS and asked for optimal solution, then D is correct.

upvoted 4 times

 **Yadav_Sanjay** 10 months, 4 weeks ago

Using self managed DNS - other three options talking about Route 53 so B can only B answer

upvoted 1 times

Question #121

Topic 1

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

- A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
- B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
- C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.
- D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

Correct Answer: A

Community vote distribution

A (81%)

Other

✉️  **123jh10**  1 year, 5 months ago

Selected Answer: A

"You can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created. However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance."

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>

upvoted 53 times

✉️  **Futurebones** 10 months, 1 week ago

How can A guarantee future encryption?

upvoted 3 times

✉️  **Smart** 8 months ago

Once DB is encrypted, newer snapshots and read replicas will also be encrypted.

upvoted 5 times

✉️  **JoeGuan** 7 months, 2 weeks ago

I agree, there is no reason to copy all of the snapshots and encrypt them all. You just need one encrypted snapshot, moving forward they will all be encrypted. C is close but I think there is no reason to copy all the snapshots plural. There is a wizard to go through and select the snapshot to encrypt. "In the Amazon RDS console navigation pane, choose Snapshots, and select the DB snapshot you created. For Actions, choose Copy Snapshot. Provide the destination AWS Region and the name of the DB snapshot copy in the corresponding fields. Select the Enable Encryption checkbox. For Master Key, specify the KMS key identifier to use to encrypt the DB snapshot copy. Choose Copy Snapshot. For more information, see Copying a snapshot in the Amazon RDS documentation". What if you had 30 snapshots? You just need to do it once.

upvoted 3 times

✉️  **Guru4Cloud** 7 months, 1 week ago

In simple terms, you double the effort of your work and spending money by creating unnecessary snapshots... so A is the best choice

upvoted 1 times

✉️  **SinghJagdeep**  3 months ago

Selected Answer: A

Correct. Please visit for more details.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>

upvoted 1 times

✉️  **ansagr** 3 months, 2 weeks ago

Selected Answer: A

AWS RDS does not support direct restoration of an encrypted snapshot to an existing unencrypted DB instance. When you restore a snapshot, it creates a new DB instance with the same configuration as the original instance.

upvoted 1 times

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

Selected Answer: A

What's wrong with C is: "Copy the snapshots and enable encryption"

upvoted 3 times

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

Selected Answer: A

key: snapshots
upvoted 1 times

 **AntonioMinolfi** 5 months, 2 weeks ago

Selected Answer: A

I was undecided if to choose A or C.
But since you can't restore a snapshot to an existing instance C is out. You can only create a new one.
[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html#:~:text>You%20can%27t%20restore%20from%20a%20DB%20snapshot%20to%20an%20existing%20DB%20instance%3B%20a%20new%20DB%20instance%20is%20created%20when%20you%20rest](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html#:~:text>You%20can%27t%20restore%20from%20a%20DB%20snapshot%20to%20an%20existing%20DB%20instance%3B%20a%20new%20DB%20instance%20is%20created%20when%20you%20restore.)ore.

upvoted 1 times

 **TMabs** 5 months, 3 weeks ago

A makes sence
upvoted 1 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: C

A. Replacing the existing DB instance with an encrypted snapshot can result in downtime and potential data loss during migration.

B. Creating a new encrypted EBS volume for snapshots does not address the encryption of the DB instance itself.

D. Copying snapshots to an encrypted S3 bucket only encrypts the snapshots, but does not address the encryption of the DB instance.

Option C is the most suitable as it involves copying and encrypting the snapshots using AWS KMS, ensuring encryption for both the database and snapshots.

upvoted 2 times

 **BartoszGolebiowski24** 5 months ago

From the question:

"...What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?"

I think the question is about encrypting current and future snapshots instead of the old snapshots.

upvoted 1 times

 **Abrar2022** 10 months ago

If daily snapshots are taken from the daily DB instance. Why create another copy? You just need to encrypt the latest daily DB snapshot and the restore from the existing encrypted snapshot.

upvoted 3 times

 **[Removed]** 11 months ago

If there is anyone who is willing to share his/her contributor access, then please write to vinyachethi99@gmail.com

upvoted 1 times

 **kruasan** 11 months ago

Selected Answer: A

You can't restore from a DB snapshot to an existing DB instance; a new DB instance is created when you restore.

upvoted 4 times

 **C_M_M** 11 months, 2 weeks ago

A and C are almost similar except that A is latest snapshot, while C is snapshots (all the snapshots).

I don't see any other difference btw those two options.

Option A is clearly the correct on as all you need is the latest snapshot.

upvoted 2 times

 **JoeGuan** 7 months, 2 weeks ago

I agree, in the wizard you would select ONE SNAPSHOT (singular in A), not all of the SNAPSHOTS (Plural in C)

upvoted 1 times

 **rushlav** 11 months, 2 weeks ago

A

You can only encrypt an Amazon RDS DB instance when you create it, not after the DB instance is created.

However, because you can encrypt a copy of an unencrypted snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

upvoted 1 times

 **Abhineet9148232** 1 year ago

Selected Answer: C

Encryption is enabled during the Copy process itself.

<https://repost.aws/knowledge-center/encrypt-rds-snapshots>

upvoted 1 times

 **Bang3R** 1 year ago

Selected Answer: C

C is the more complete answer as you need KMS to encrypt the snapshot copy prior to restoring it to the Database instance.
upvoted 1 times

✉ **jdr75** 11 months, 3 weeks ago

BUT you can't restore encrypted snapshot to an existing DB instance. Only no NEW DB (not an existing one). The procedure described in this way:
"(...) you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance."

refers to create a NEW DB instance (this encrypted), never restoring in a existing one.

The RDB engine understands that restoring from a encrypted snapshot is form create an encrypted NEW database.

upvoted 2 times

✉ **TungPham** 1 year ago

Selected Answer: C

A not resolve data create in future.
You can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created.
C will make this, see image below
Architecture
Source architecture

Unencrypted RDS DB instance

Target architecture

Encrypted RDS DB instance

The destination RDS DB instance is created by restoring the DB snapshot copy of the source RDS DB instance.

An AWS KMS key is used for encryption while restoring the snapshot.

An AWS DMS replication task is used to migrate the data.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>

upvoted 1 times

✉ **jaswantn** 1 year ago

Option A seems correct.

With option (A) we already have DB snapshots. Just encrypt the latest available copy of snapshot, why to copy the snapshot once again (as told in option C).

upvoted 1 times

✉ **jkmaws** 1 year, 1 month ago

A

You can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created. However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance. If your project allows for downtime (at least for write transactions) during this activity, this is all you need to do. When the new, encrypted copy of the DB instance becomes available, you can point your applications to the new database.

upvoted 1 times

Question #122

Topic 1

A company wants to build a scalable key management infrastructure to support developers who need to encrypt data in their applications. What should a solutions architect do to reduce the operational burden?

- A. Use multi-factor authentication (MFA) to protect the encryption keys.
- B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys.
- C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys.
- D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys.

Correct Answer: B

Community vote distribution

 B (100%)

 **123jhl0**  1 year, 5 months ago

Selected Answer: B

If you are a developer who needs to digitally sign or verify data using asymmetric keys, you should use the service to create and manage the private keys you'll need. If you're looking for a scalable key management infrastructure to support your developers and their growing number of applications, you should use it to reduce your licensing costs and operational burden...
<https://aws.amazon.com/kms/faqs/#:~:text=If%20you%20are%20a%20developer%20who%20needs%20to%20digitally,a%20broad%20set%20of%20industry%20and%20regional%20compliance%20regimes.>

upvoted 21 times

 **ocbn3wby** 1 year, 3 months ago

Most documented answers. Thank you, 123jhl0.

upvoted 3 times

 **Buruguduystunstugudunstuy**  1 year, 2 months ago

Selected Answer: B

The correct answer is Option B. To reduce the operational burden, the solutions architect should use AWS Key Management Service (AWS KMS) to protect the encryption keys.

AWS KMS is a fully managed service that makes it easy to create and manage encryption keys. It allows developers to easily encrypt and decrypt data in their applications, and it automatically handles the underlying key management tasks, such as key generation, key rotation, and key deletion. This can help to reduce the operational burden associated with key management.

upvoted 6 times

 **Ruffyit**  4 months, 3 weeks ago

AWS KMS handles the encryption key management, rotation, and auditing. This removes the undifferentiated heavy lifting for developers.

KMS integrates natively with many AWS services like S3, EBS, RDS for encryption. This makes it easy to encrypt data.

KMS scales automatically as key usage increases. Developers don't have to worry about provisioning key infrastructure.

Fine-grained access controls are available via IAM policies and grants. KMS is secure by default.

Features like envelope encryption make compliance easier for regulated workloads.

AWS handles the hardware security modules (HSMs) for cryptographic key storage

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

The main reasons are:

AWS KMS handles the encryption key management, rotation, and auditing. This removes the undifferentiated heavy lifting for developers.

KMS integrates natively with many AWS services like S3, EBS, RDS for encryption. This makes it easy to encrypt data.

KMS scales automatically as key usage increases. Developers don't have to worry about provisioning key infrastructure.

Fine-grained access controls are available via IAM policies and grants. KMS is secure by default.

Features like envelope encryption make compliance easier for regulated workloads.

AWS handles the hardware security modules (HSMs) for cryptographic key storage

upvoted 2 times

 **cookieMr** 9 months, 1 week ago

Selected Answer: B

By utilizing AWS KMS, the company can offload the operational responsibilities of key management, including key generation, rotation, and protection. AWS KMS provides a scalable and secure infrastructure for managing encryption keys, allowing developers to easily integrate encryption into their applications without the need to manage the underlying key infrastructure.

Option A (MFA), option C (ACM), and option D (IAM policy) are not directly related to reducing the operational burden of key management. While these options may provide additional security measures or access controls, they do not specifically address the scalability and management aspects of a key management infrastructure. AWS KMS is designed to simplify the key management process and is the most suitable option for reducing the operational burden in this scenario.

upvoted 2 times

 **cheese929** 11 months ago

Selected Answer: B

B is correct.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **Jtic** 1 year, 4 months ago

Selected Answer: B

If you are responsible for securing your data across AWS services, you should use it to centrally manage the encryption keys that control access to your data. If you are a developer who needs to encrypt data in your applications, you should use the AWS Encryption SDK with AWS KMS to easily generate, use and protect symmetric encryption keys in your code.

upvoted 2 times

Question #123

Topic 1

A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application's performance?

- A. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.
- B. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.
- C. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.
- D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

Correct Answer: D

Community vote distribution



✉️ **123jh10** 1 year, 5 months ago

Selected Answer: D

This issue is solved by SSL offloading, i.e. by moving the SSL termination task to the ALB.
<https://aws.amazon.com/blogs/aws/elastic-load-balancer-support-for-ssl-termination/>
 upvoted 19 times

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

Selected Answer: D

The correct answer is D. To increase the application's performance, the solutions architect should import the SSL certificate into AWS Certificate Manager (ACM) and create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

An Application Load Balancer (ALB) can offload the SSL termination process from the EC2 instances, which can help to increase the compute capacity available for the web application. By creating an ALB with an HTTPS listener and using the SSL certificate from ACM, the ALB can handle the SSL termination process, leaving the EC2 instances free to focus on running the web application.

upvoted 11 times

✉️ **Ruffyt** 4 months, 3 weeks ago

This issue is solved by SSL offloading, i.e. by moving the SSL termination task to the ALB.
<https://aws.amazon.com/blogs/aws/elastic-load-balancer-support-for-ssl-termination/>
 upvoted 2 times

✉️ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

The key reasons are:

Using an Application Load Balancer with an HTTPS listener allows SSL termination to happen at the load balancer layer. The EC2 instances behind the load balancer receive only unencrypted traffic, reducing load on them. Importing the custom SSL certificate into ACM allows the ALB to use it for HTTPS listeners. This removes the need to install and manage SSL certificates on each EC2 instance. ALB handles the SSL overhead and scales automatically. The EC2 fleet focuses on app logic. Options A, B, C don't offload SSL overhead from the EC2 instances themselves.

upvoted 2 times

✉️ **cookieMr** 9 months, 1 week ago

Selected Answer: D

By using ACM to manage the SSL certificate and configuring an ALB with HTTPS listener, the SSL termination will be handled by the load balancer instead of the web servers. This offloading of SSL processing to the ALB reduces the compute capacity burden on the web servers and improves their performance by allowing them to focus on serving the dynamic web application.

Option A suggests creating a new SSL certificate using ACM, but it does not address the SSL termination offloading and load balancing capabilities provided by an ALB.

Option B suggests migrating the SSL certificate to an S3 bucket, but this approach does not provide the necessary SSL termination and load balancing functionalities.

Option C suggests creating another EC2 instance as a proxy server, but this adds unnecessary complexity and management overhead without

leveraging the benefits of ALB's built-in load balancing and SSL termination capabilities.

Therefore, option D is the most suitable choice to increase the application's performance in this scenario.

upvoted 2 times

 **dejung** 1 year, 1 month ago

Selected Answer: A

Why is A wrong?

upvoted 2 times

 **Yadav_Sanjay** 10 months, 3 weeks ago

Company uses its own SSL certificate. Option A says.. Create a SSL certificate in ACM

upvoted 2 times

 **xdkonorek2** 4 months, 3 weeks ago

ec2 instances still would be responsible for decrypting traffic and it wouldn't solve load issue

upvoted 1 times

 **remand** 1 year, 2 months ago

Selected Answer: D

SSL termination is the process of ending an SSL/TLS connection. This is typically done by a device, such as a load balancer or a reverse proxy, that is positioned in front of one or more web servers. The device decrypts incoming SSL/TLS traffic and then forwards the unencrypted request to the web server. This allows the web server to process the request without the overhead of decrypting and encrypting the traffic. The device then re-encrypts the response from the web server and sends it back to the client. This allows the device to offload the SSL/TLS processing from the web servers and also allows for features such as SSL offloading, SSL bridging, and SSL acceleration.

upvoted 4 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D to offload the SSL encryption workload

upvoted 1 times

 **Aamee** 1 year, 3 months ago

Selected Answer: D

Due to this statement particularly: "The company has its own SSL certificate" as it's not created from AWS ACM itself.

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

D is correct

upvoted 1 times

 **Six_Fingered_Jose** 1 year, 5 months ago

Selected Answer: D

agree with D

upvoted 1 times

Question #124

Topic 1

A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.

What should the solutions architect recommend?

- A. Implement EC2 Spot Instances.
- B. Purchase EC2 Reserved Instances.
- C. Implement EC2 On-Demand Instances.
- D. Implement the processing on AWS Lambda.

Correct Answer: A

Community vote distribution

A (100%)

✉  **Kapello10**  1 year, 3 months ago

Selected Answer: A

Cant be implemented on Lambda because the timeout for Lambda is 15mins and the Job takes 60minutes to complete

Answer >> A

upvoted 20 times

✉  **Evangelia**  1 year, 5 months ago

spot instances

upvoted 5 times

✉  **thewalker**  1 month, 3 weeks ago

Selected Answer: A

There is a chance of interrupting the jobs, but as they can be started and stopped at any given time, the MOST COST effective is going for Spot.

upvoted 2 times

✉  **Ruffyit** 4 months, 3 weeks ago

Spot Instances provide significant cost savings for flexible start and stop batch jobs.

Purchasing Reserved Instances (B) is better for stable workloads, not dynamic ones.

On-Demand Instances (C) are costly and lack potential cost savings like Spot Instances.

AWS Lambda (D) is not suitable for long-running batch jobs.

upvoted 2 times

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

Selected Answer: A

key: can be started and stopped at any given time with no negative impact

upvoted 2 times

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

Selected Answer: A

Spot can do that

upvoted 1 times

✉  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

The key reasons are:

Spot can provide significant cost savings (up to 90%) compared to On-Demand.

Since the job is stateless and can be stopped/restarted anytime, the intermittent availability of Spot is not an issue.

Spot supports the same instance types as On-Demand, so optimal instance types can be chosen.

For a 60+ minute batch job, the chance of Spot interruption is low. But if it happens, the job can just be restarted.

Reserved Instances don't offer any advantage for a highly dynamic job like this.

Lambda is not a good fit given the long runtime requirement.

upvoted 3 times

✉  **cookieMr** 9 months ago

Selected Answer: A

Spot Instances provide significant cost savings for flexible start and stop batch jobs.

Purchasing Reserved Instances (B) is better for stable workloads, not dynamic ones.

On-Demand Instances (C) are costly and lack potential cost savings like Spot Instances.

AWS Lambda (D) is not suitable for long-running batch jobs.

upvoted 1 times

 **beginnercloud** 9 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **alexiscloud** 12 months ago

Answer A:

typically takes upwards of 60 minutes total to complete.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: A

The correct answer is Option A. To design a scalable and cost-effective solution for the batch processing job, the solutions architect should recommend implementing EC2 Spot Instances.

EC2 Spot Instances allow users to bid on spare Amazon EC2 computing capacity and can be a cost-effective solution for stateless, interruptible workloads that can be started and stopped at any time. Since the batch processing job is stateless, can be started and stopped at any time, and typically takes upwards of 60 minutes to complete, EC2 Spot Instances would be a good fit for this workload.

upvoted 2 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: A

Spot Instances should be good enough and cost effective because the job can be started and stopped at any given time with no negative impact.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

Option A

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 1 times

 **SimonPark** 1 year, 4 months ago

Selected Answer: A

A is the answer

upvoted 1 times

Question #125

Topic 1

A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.

Which combination of configuration options will meet these requirements? (Choose two.)

- A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
- B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
- C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
- D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.
- E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Correct Answer: CE

Community vote distribution



✉️ **mabotega** 1 year, 4 months ago

Selected Answer: AD

Answer A for: The EC2 instances and the RDS DB instance should not be exposed to the public internet. Answer D for: The EC2 instances require internet access to complete payment processing of orders through a third-party web service. Answer A for: The application must be highly available.

upvoted 26 times

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

D allows public internet access which is not desired. The answer is not d.

The most accurate answers are AB

upvoted 2 times

✉️ **pentium75** 3 months ago

B is wrong because you can't deploy NAT GW in a private subnet. Correct answer is E (mislabelled as a second D). Stem says that the EC2 instances (!) must not be exposed to the Internet, the Load Balancer can be exposed.

upvoted 1 times

✉️ **AbhiJo** 1 year, 4 months ago

We will require 2 private subnets, D does mention 1 subnet

upvoted 4 times

✉️ **pentium75** 3 months ago

There's two D options ;) second is correct

upvoted 2 times

✉️ **smd_** 10 months, 4 weeks ago

why not option B.The EC2 instances can be launched in private subnets across two Availability Zones, and the Application Load Balancer can be deployed in the private subnets. NAT gateways can be configured in each private subnet to provide internet access for the EC2 instances to communicate with the third-party web service.

upvoted 1 times

✉️ **ruqui** 10 months, 1 week ago

B option wrong! NAT gateways must be created in public subnets!!

upvoted 8 times

✉️ **x33** 6 months, 3 weeks ago

I think you are wrong on this. In fact, NAT gateways are typically created in private subnets.

upvoted 1 times

✉️ **RNess** 5 months, 1 week ago

NAT Gateway can't be used by EC2 instance in the same subnet (only from other subnets)

upvoted 4 times

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

A and E!

Application has to be highly available while the instance and database should not be exposed to the public internet, but the instances still require access to the internet. NAT gateway has to be deployed in public subnets in this case while instances and database remain in private subnets in the VPC, therefore answer is (A) and (E).

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

If the instances did not require access to the internet, then the answer could have been

(B) to use a private NAT gateway and keep it in the private subnets to communicate only to the VPCs.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

upvoted 19 times

✉  **darn** 11 months, 1 week ago

your link is right but your voting is wrong, should be AD, although that still doesn't explain why 2 NAT gateways

upvoted 3 times

✉  **cheroh_tots** 2 weeks, 4 days ago

Because NAT gateways are availability zone specific, if you need HA you will need a NAT gateway in each availability zone.

upvoted 1 times

✉  **ale_brd_** 3 months, 2 weeks ago

cus application has to be HA, if one NAT gateway fails the other could take the traffic

upvoted 4 times

✉  **SaurabhTiwari1**  3 months ago

Selected Answer: AD

AD is right , last one D

upvoted 1 times

✉  **rlamberti** 5 months, 1 week ago

Selected Answer: AD

AE

Two public subnets = two addresses for ALB = high availability

two private subnets with NAT gateway to allow egress traffic to internet - application tier will be able to complete payment

upvoted 5 times

✉  **RNess** 5 months, 1 week ago

Selected Answer: AD

AE

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

upvoted 3 times

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

Selected Answer: AD

AE. There are two Ds, the last option should be E.

upvoted 2 times

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

Selected Answer: AB

AB. should not be exposed to the public internet => private subnet

upvoted 1 times

✉  **pentium75** 3 months ago

EC2 instances should not be exposed to the public Internet, LB should

upvoted 1 times

✉  **ayrus1992** 8 months, 1 week ago

Selected Answer: C

CE

Highly Available and Secure

upvoted 1 times

✉  **bahaa_shaker** 7 months ago

read the question again, it asks to make the ec2 and rds in private subnet

do not mislead others if you are not sure of your answer

C is wrong answer but 1000000%

its A and D

upvoted 1 times

✉  **omerap12** 9 months ago

Selected Answer: AD

Answer A for: The EC2 instances and the RDS DB instance should not be exposed to the public internet. Answer D for: The EC2 instances require internet access to complete payment processing of orders through a third-party web service. Answer A for: The application must be highly available.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: AD

Option D configures a VPC with a public subnet for the web tier, allowing customers to access the website. The private subnet provides a secure environment for the EC2 instances and the RDS DB instance. NAT gateways are used to provide internet access to the EC2 instances in the private subnet for payment processing.

Option A uses an Auto Scaling group to launch the EC2 instances in private subnets, ensuring they are not directly accessible from the public internet. The RDS Multi-AZ DB instance is also placed in private subnets, maintaining security.

upvoted 1 times

 **beginnercloud** 9 months, 2 weeks ago

Selected Answer: AD

Second D so like E.

upvoted 2 times

 **fishy_resolver** 9 months, 3 weeks ago

Selected Answer: CD

I had it as AD, but for me the question asked for high availability, and A doesn't specify across availability zones. So, A is more secure but not highly available. C is less secure but highly available

upvoted 1 times

 **antropaws** 9 months, 4 weeks ago

Selected Answer: AD

AD because 2 NAT gateways in 2 public subnets in 2 AZs.

upvoted 2 times

 **bgsanata** 10 months, 1 week ago

Selected Answer: CD

C - provide required HA

E - Best answer to the access requirements. The NAT gateway is required for the EC2 instances to access the third-party web service. This do not expose them for inbound connections from Internet.

upvoted 1 times

 **studynoplay** 10 months, 3 weeks ago

Selected Answer: AD

A & the 2nd D. You have to put each NAT gateway in each public subnet

upvoted 2 times

 **cheese929** 11 months ago

Selected Answer: AD

A and the second D are the correct choices. ALB in the public subnet for access from the internet. NAT gateways and the EC2s in the private subnet over 2 AZs to meet the requirements.

A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.

D. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

upvoted 1 times

 **kruasan** 11 months ago

Selected Answer: AD

AE

Option B is not a valid solution as it only includes private subnets, and both the NAT gateway and Application Load Balancer require public subnets.

upvoted 2 times

Question #126

Topic 1

A solutions architect needs to implement a solution to reduce a company's storage costs. All the company's data is in the Amazon S3 Standard storage class. The company must keep all data for at least 25 years. Data from the most recent 2 years must be highly available and immediately retrievable.

Which solution will meet these requirements?

- A. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.
- B. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years.
- C. Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.
- D. Set up an S3 Lifecycle policy to transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately and to S3 Glacier Deep Archive after 2 years.

Correct Answer: B*Community vote distribution*

rjam 1 year, 4 months ago

Selected Answer: B

Why Not C? Because Intelligent Tier the objects are automatically moved to different tiers.

The question says "the data from most recent 2 yrs should be highly available and immediately retrievable", which means in intelligent tier , if you activate archiving option(as Option C specifies) , the objects will be moved to Archive tiers(instant to access to deep archive access tiers) in 90 to 730 days. Remember these archive tiers performance will be similar to S3 glacier flexible and s3 deep archive which means files cannot be retrieved immediately within 2 yrs .

We have a hard requirement in question which says it should be retrievable immediately for the 2 yrs. which cannot be achieved in Intelligent tier. So B is the correct option imho.

Because of the above reason Its possible only in S3 standard and then configure lifecycle configuration to move to S3 Glacier Deep Archive after 2 yrs.

upvoted 13 times

MutiverseAgent 8 months, 2 weeks ago

Mmm.. You can enable Intelligent-Tiering and take advantage of the infrequent Access tier and thus reducing costs. To avoid moving objects to the deep archive tier before the two years it would be enough to enable ONLY the check "Deep Archive Access tier" and set days to 720 (two years, which is curiously the maximum value), and keep disabled the check "Archive Access tier" to avoid the Intelligent-Tiering move objects to the non-instant retrieval tier. That will work, offcourse this specific configuration is not mentioned in the question which leaves some doubts about which option is the correct.

upvoted 1 times

MutiverseAgent 8 months, 2 weeks ago

Just to clarify, my previous comment is about how answer B) might be correct and the MOST cheapest option under the correct configuration.

upvoted 1 times

MutiverseAgent 8 months, 2 weeks ago

Sorry, I meant answer C) might be correct

upvoted 1 times

Abdou1604 7 months, 1 week ago

but your S3 intelligent-tiering will move the object to S3 infrequent access tier which is a single AZ tier , and then the HA requirement will not be respected

upvoted 1 times

TelaO 1 year, 4 months ago

Selected Answer: B

B is the only right answer. C does not indicate archiving after 2 years. If it did specify 2 years, then C would also be an option.

upvoted 8 times

LoXoL 2 months, 2 weeks ago

Selected Answer: B

A. We can't move to Glacier immediately as data from last 2 yrs need to be immediately retrievable

B. It's the perfect fit: getting HA and instant access (with current solution = S3 std), then moving to Deep Archive after 2 yrs (very cheap)

C: Highly expensive because of Intelligent Tiering

D: it lacks HA with One Zone

upvoted 1 times

✉️ **SaurabhTiwari1** 3 months ago

Selected Answer: B

Data remain in S3 standard storage for 2 years then it will be move to s3 glacier deep archive after 2 year.

upvoted 2 times

✉️ **Ruffyit** 4 months, 3 weeks ago

but your S3 intelligent-tiering will move the object to S3 infrequent access tier which is a single AZ tier , and then the HA requirement will not be respected

upvoted 1 times

✉️ **David_Ang** 5 months, 1 week ago

Selected Answer: B

i understand why "B" is more correct than "C" and is because "C" is bad formulated, if in the answer would say "life cycle after 2 years of using intelligent tiring" then it would be the correct answer. so "B" is correct

upvoted 1 times

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

Selected Answer: B

I would not opt for C simply because S3IT was specifically designed for scenarios where the access patterns are unknown. This scenario has clearly known access patterns making option B the best.

upvoted 2 times

✉️ **cookieMr** 9 months ago

Selected Answer: B

Option A is incorrect because immediately transitioning objects to S3 Glacier Deep Archive would not fulfill the requirement of keeping the most recent 2 years of data highly available and immediately retrievable.

Option C is also incorrect because using S3 Intelligent-Tiering with archiving option would not meet the requirement of immediately retrievable data for the most recent 2 years.

Option D is not the best choice because transitioning objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) and then to S3 Glacier Deep Archive would not satisfy the requirement of immediately retrievable data for the most recent 2 years.

Option B is the correct solution. By setting up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years, the company can keep all data for at least 25 years while ensuring that data from the most recent 2 years remains highly available and immediately retrievable in the Amazon S3 Standard storage class. This solution optimizes storage costs by leveraging the Glacier Deep Archive for long-term storage.

upvoted 2 times

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

this makes sense the question is a bit tricky. I now understand that all the data is already kept in S3 Standard meaning immediate retrieval of the most recent data is remains highly available.

upvoted 1 times

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

Why not D

upvoted 2 times

✉️ **RNess** 5 months, 1 week ago

"Data from the most recent 2 years must be highly available and immediately retrievable."

upvoted 1 times

✉️ **RNess** 5 months, 1 week ago

Additionally,
S3 Standard Availability = 99.99%
S3 One Zone-IA Availability = 99.5%
upvoted 1 times

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

Selected Answer: B

B is the only one possible.

upvoted 1 times

✉️ **rushlav** 11 months, 2 weeks ago

C would not work as the names of these S3 archives are called Archive Access Tier and Deep Archive access tiers, so since they mention glacier in option C , I think its B which is the correct.

upvoted 1 times

✉️ **CaoMengde09** 1 year, 1 month ago

It's pretty straight forward.

S3 Standard answers for High Availability/Immediate retrieval for 2 years. S3 Intelligent Ttiering would just incur additional cost of analysis while the company insures that it requires immediate retrieval in any moment and without risk to Availability. So a capital B

upvoted 2 times

✉️ **G3** 1 year, 1 month ago

C appears to be appropriate - good case for intelligent tiering
upvoted 1 times

 **Sdraju** 1 year ago

Intelligent tiering appears to be best suited for unknown usage pattern.. but with a known usage pattern Life cycle policy may be optimal.
upvoted 1 times

 **Robrobtutu** 11 months, 1 week ago

The option just says Intelligent Tiering, it doesn't specify when it would transition the date to Deep Archive, so how do we know it would do it at the correct time? It has to be A.
upvoted 1 times

 **DaveNL** 1 year, 2 months ago

Selected Answer: C

C. Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.

S3 Intelligent Tiering supports changing the default archival time to 730 days (2 years) from the default 90 or 180 days. Other levels of tiering are instant access tiers.

upvoted 2 times

 **Zerotn3** 1 year, 2 months ago

Selected Answer: D

Option D is the correct solution for this scenario.

S3 Lifecycle policies allow you to automatically transition objects to different storage classes based on the age of the object or other specific criteria. In this case, the company needs to keep all data for at least 25 years, and the data from the most recent 2 years must be highly available and immediately retrievable.

upvoted 4 times

 **Ifrad** 1 year, 2 months ago

If the option for D was Infrequent Access it would be good, but here it is One Zone-IA which is not highly available. Then it must be B
upvoted 5 times

 **Zerotn3** 1 year, 2 months ago

Option A is not a good solution because it would transition all objects to S3 Glacier Deep Archive immediately, making the data from the most recent 2 years not immediately retrievable. Option B is not a good solution because it would not make the data from the most recent 2 years immediately retrievable.

Option C is not a good solution because S3 Intelligent-Tiering is designed to automatically move objects between two storage classes (Standard and Infrequent Access) based on object access patterns. It does not provide a way to transition objects to S3 Glacier Deep Archive, which is required for long-term storage.

Option D is the correct solution because it would transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately, making the data from the most recent 2 years immediately retrievable. After 2 years, the objects would be transitioned to S3 Glacier Deep Archive for long-term storage. This solution meets the requirements of the company to keep all data for at least 25 years and make the data from the most recent 2 years immediately retrievable.

upvoted 2 times

 **Ello2023** 1 year, 2 months ago

B is immediately retrievable, has high availability and using the lifecycle you can transition to deep archive after the 2 years time period.
upvoted 1 times

 **hahahumble** 1 year, 2 months ago

S3 One Zone-IA is not highly available compared with S3 standard

https://aws.amazon.com/about-aws/whats-new/2018/04/announcing-s3-one-zone-infrequent-access-a-new-amazon-s3-storage-class/?nc1=h_ls

upvoted 2 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: B

B looks correct
upvoted 2 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B
upvoted 1 times

Question #127

Topic 1

A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.

Which set of services should a solutions architect recommend to meet these requirements?

- A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
- B. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage
- C. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage
- D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Correct Answer: A

Community vote distribution



✉️ **Sauran** Highly Voted 1 year, 5 months ago

Selected Answer: D

Max instance store possible at this time is 30TB for NVMe which has the higher I/O compared to EBS.

is4gen.8xlarge 4 x 7,500 GB (30 TB) NVMe SSD

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#instance-store-volumes>

upvoted 29 times

✉️ **ishitamodi4** 1 year, 3 months ago

instance store volume for the root volume, the size of this volume varies by AMI, but the maximum size is 10 GB

upvoted 1 times

✉️ **JayBee65** 1 year, 3 months ago

This link shows a max capacity of 30TB, so what is the problem?

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#instance-store-volumes>

upvoted 1 times

✉️ **JayBee65** 1 year, 3 months ago

Only the following instance types support an instance store volume as the root device: C3, D2, G2, I2, M3, and R3, and we're using an I3, so an instance store volume is irrelevant.

upvoted 2 times

✉️ **antropaws** 9 months, 4 weeks ago

THE CORRECT ANSWER IS A.

The biggest Instance Store Storage Optimized option (is4gen.8xlarge) has a capacity of only 3TB.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-store-volumes.html#instance-store-vol-so>

upvoted 2 times

✉️ **michellemeloc** 10 months, 4 weeks ago

Update: i3en.metal and i3en.24xlarge = 8 x 7500 GB (60TB)

upvoted 2 times

✉️ **MiniYang** Highly Voted 3 months, 2 weeks ago

Selected Answer: A

The correct Answer is A :

Amazon EC2 instance store (Instance Store) is usually not the best choice because the storage it provides is temporary and tied to the life cycle of the instance. When an instance is stopped or terminated, data on the instance store is lost.

In this scenario, the company's requirements were to have the maximum possible I/O performance and required durable data storage. Therefore, using Amazon EC2 Instance Store does not meet these requirements because it lacks durability.

In contrast, Amazon EBS (Elastic Block Store) provides persistent regional block storage and can meet the needs of high-performance I/O. Therefore, the answer should include Amazon EBS, not Amazon EC2 instance storage.

upvoted 7 times

✉️ **pentium75** 3 months ago

"The company's requirements were to have the maximum possible I/O performance and required durable data storage." Yeah, but not for the same data.

10 TB "maximum possible I/O performance" for processing (= temporary)

300 TB "very durable" (= S3)

900 TB "for archival" (= Glacier)

upvoted 3 times

✉ **LoXoL** 2 months, 2 weeks ago

pentium75 is right.

upvoted 1 times

✉ **henna2024** **Most Recent** 1 month ago

the answer is D

From a maximum I/O perspective, Amazon EBS is significantly better than Amazon EC2 instance store for two main reasons:

1. Underlying Storage Technology:

Amazon EBS: Utilizes Solid State Drives (SSDs) and NVMe storage options, offering high-performance IOPS (Input/Output Operations Per Second) and throughput.

Amazon EC2 Instance Store: Relies on the local hard disk drives (HDDs) attached to the EC2 instance, which have significantly lower IOPS and throughput compared to SSDs.

upvoted 1 times

✉ **vip2** 1 month, 1 week ago

Selected Answer: D

Instance store is more than 10T

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Selected Answer: D

A sounds good but D is better as the store is physically attached to the instance!

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

upvoted 1 times

✉ **foha2012** 2 months, 1 week ago

D - I chose A. But its a trick question. Upon reading Pentium75's Comment, I agree it should be D. However, I would feel more confident if it mentioned "temporary 10Gb" in the question...

upvoted 2 times

✉ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: A

"D" is dependant on instance type of hpc6id.32xlarge is 16TB for accelerated computing with NVMe SSD. I will go for "A" because it does not depend on EC2 instance as a requirement.

upvoted 1 times

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

Selected Answer: A

A looks right.

upvoted 1 times

✉ **SaurabhTiwari1** 3 months ago

Selected Answer: A

A is right

upvoted 2 times

✉ **Marco_St** 4 months ago

Selected Answer: D

vote for D since the demand is asking for maximum I/O while did not specify how durable the performance should be. So D. otherwise more realistic and durable option is A with high I/O performance as well

upvoted 1 times

✉ **Chiznitz** 4 months, 2 weeks ago

Selected Answer: D

The keyword here is "maximum possible I/O performance".

EBS and Ec2 instance store are good options, but EC2 is higher than EBS in terms of I/O performance. Maximum possible is clearly Ec2 instance storage.

There are some concerns about the 10TB needed, however, storage optimized Ec2 instance stores can take up to 24 x 13980 GB (ie 312 TB)
So option D is the winner here.

upvoted 2 times

✉ **Azure55** 4 months, 3 weeks ago

Selected Answer: A

well! read option D again, it says EC2 Instance, not EC2 Instances!
so the answer is obviously A.

upvoted 1 times

 **pentium75** 3 months ago

Huh? "Instance store" is the name of the service, and it's what provides "maximum I/O performance possible", WAY above what EBS can.
upvoted 2 times

 **tom_cruise** 4 months, 3 weeks ago

Selected Answer: D

"An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content. It can also be used to store temporary data that you replicate across a fleet of instances, such as a load-balanced pool of web servers."

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

upvoted 1 times

 **Ruffyt** 4 months, 3 weeks ago

We are talkimng about storage here and EC2 instance store in not a viable solution for for a storage.

upvoted 1 times

 **pentium75** 3 months ago

Why would a "store" not be "a viable solution for storage"? Nothing says the 10 TB must be durable. We need maximum I/O, which only instance store provides.

upvoted 2 times

 **foha2012** 2 months, 1 week ago

I agree with you. However, I would have felt more comfortabe if the question had "Temporary 10GB" in the question. I chose A first but Now I agree with you and I think it should be D.

upvoted 1 times

 **aptx4869** 4 months, 4 weeks ago

Selected Answer: A

We are talkimng about storage here and EC2 instance store in not a viable solution for for a storage.

upvoted 1 times

 **pentium75** 3 months ago

Why would a "store" not be "a viable solution for storage"? Nothing says the 10 TB must be durable. We need maximum I/O, which only instance store provides.

upvoted 1 times

 **David_Ang** 5 months, 1 week ago

Selected Answer: A

dude literally EC2 instances storage systems are based on EBS volumes, who it would be more efficient to use an instance, than use a service that is meant for that job. "C" and "D" are simply not cost-efficient.

upvoted 1 times

 **pentium75** 3 months ago

"Instance store" is a service which uses local disks on the hypervisors, instance store is NOT "based on EBS volumes"!

upvoted 2 times

 **BrijMohan08** 6 months, 1 week ago

Selected Answer: D

10tb, good enough for EC2

10 TB required only for processing -> Temp memory

For durable storage s3 is a perfect fit in this scenario.

upvoted 1 times

Question #128

Topic 1

A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead. What should a solutions architect do to meet these requirements?

- A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.
- B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.
- C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.
- D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

Correct Answer: A

Community vote distribution

B (72%)

A (27%)

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

Selected Answer: A

Requirement is "minimizes cost and operational overhead"

A is better option than B as EKS add additional cost and operational overhead.

upvoted 15 times

✉  **Lalo** 9 months, 3 weeks ago

USING SPOT INSTANCES WITH EKS

https://ec2spotworkshops.com/using_ec2_spot_instances_with_eks.html

upvoted 4 times

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

In my opinion option A) seems to be a reasonable at first because setting up AWS EKS might be seem as an operation overhead comparing to the option of running the containers inside the EC2 using docker just as you we do on your own machines. However, consider installing docker on multiple EC2 instances and manually manage docker instances and images will end up in chaos, so, as a conclusion, the operational cost of setting up AWS EKS will worth the effort.

upvoted 5 times

✉  **ruqui** 10 months, 1 week ago

option A is the worst option in terms of operational overhead ... you have to install your own kubernetes cluster!!! B is a more suitable option

upvoted 4 times

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

you do not necessary need to install K8S, in terms of plain containers you can run them using docker just as you do on your own machine.
upvoted 1 times

✉  **GalileoEC2**  1 year ago

Answer is A:

Amazon ECS: ECS itself is free, you pay only for Amazon EC2 resources you use.

Amazon EKS: The EKS management layer incurs an additional cost of \$144 per month per cluster.

Advantages of Amazon ECS include: Spot instances: Because containers are immutable, you can run many workloads using Amazon EC2 Spot Instances (which can be shut down with no advance notice) and save 90% on on-demand instance costs.

upvoted 8 times

✉  **vip2**  1 month, 1 week ago

Selected Answer: A

Does A implicitly means run spot Instance on ECS?

upvoted 1 times

✉  **awsgeek75** 2 months, 3 weeks ago

Selected Answer: B

Spot instances for disruption friendly containers which are also cheaper.

EKS allows using spot instances from a managed node group that takes away the EC2 operational overhead.

Link: <https://aws.amazon.com/blogs/containers/amazon-eks-now-supports-provisioning-and-managing-ec2-spot-instances-in-managed-node-groups/>

"Previously, customers had to run Spot Instances as self-managed worker nodes in their EKS clusters. This meant doing some heavy lifting such as building and maintaining configuration for Spot Instances in EC2 Auto Scaling groups, deploying a tool for handling Spot interruptions gracefully, deploying AMI updates, and updating the kubelet version running on their worker nodes. Now, all you need to do is supply a single parameter to indicate that a managed node group should launch Spot Instances, and provide multiple instance types that would be used by the underlying EC2 Auto Scaling group."

upvoted 1 times

 **pipici** 4 months, 1 week ago

Selected Answer: A

A has less operational overhead
upvoted 2 times

 **xdkonorek2** 4 months, 3 weeks ago

Selected Answer: B

running containers without container service like EKS introduce huge operational effort
upvoted 4 times

 **David_Ang** 5 months, 1 week ago

Selected Answer: B

dude always if you have a service that is meant to be used for a job there is the correct answer, is logic.
upvoted 6 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: B

It is a lot of work to manage docker environment on ec2 instance by yourself.
upvoted 3 times

 **poponpo** 5 months, 3 weeks ago

Selected Answer: A

k8s is not easy solution. there are too many to study about it. You have to know about ingress, storageclass, cni, namesapce, etc... they make burdened to operate.
upvoted 1 times

 **Modulopi** 5 months, 4 weeks ago

Selected Answer: A

reponse A
upvoted 1 times

 **TariqKipkemei** 6 months, 3 weeks ago

Selected Answer: B

Minimize costs = Spot instances
Minimize operational overhead = Amazon EKS is a managed Kubernetes service that makes it easy for you to run Kubernetes on AWS and on-premises.

https://aws.amazon.com/pm/eks/?trk=c69c708c-c423-4c07-9fc8-513781540cc7&sc_channel=ps&ef_id=Cj0KCQjw9MCnBhCYARIsAB1WQVWD7pSyGgjzsk6QHMNAIZrHvuAzZd4cy9b4QAaCcB5QTn6MR_czhWkaAm6UEALw_wcB:G:s&s_kwcid=AL!4422!3!669047416746!e!!g!!eks!20433874212!155230227787#:~:text=is%20Amazon%20EKS%3F-,Amazon%20EKS,-is%20a%20managed

I would not try to overthink this.
upvoted 4 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

The key reasons are:

Using Spot Instances reduces EC2 costs significantly compared to On-Demand.
EKS managed node groups simplify running and scaling containerized applications vs self-managed Kubernetes.
Since the applications are stateless and fault-tolerant, intermittent Spot interruptions are acceptable.
The combination of Spot + EKS provides the most cost-efficient infrastructure with minimal operational overhead.
Options A, C and D either use On-Demand instances or self-managed infrastructure, which increases costs and overhead.
upvoted 3 times

 **aadityaravi8** 8 months, 3 weeks ago

to run application with minimum cost, use spot instances and to reduce operational overhead, run it on EKS.
Hence B should be right answer.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: B

Option B is the recommended solution. Using Spot Instances within an Amazon EKS managed node group allows you to run containers in a managed Kubernetes environment while taking advantage of the cost savings offered by Spot Instances. Spot Instances provide access to spare EC2 capacity at significantly lower prices than On-Demand Instances. By utilizing Spot Instances in an EKS managed node group, you can reduce costs while maintaining high availability for your stateless applications.

Option A suggests using Spot Instances in an EC2 Auto Scaling group, which is a valid approach. However, utilizing Amazon EKS provides a more streamlined and managed environment for running containers.

Options C and D suggest using On-Demand Instances, which would provide stable capacity but may not be the most cost-effective solution for minimizing costs, as On-Demand Instances typically have higher prices compared to Spot Instances.

upvoted 4 times

 **Abrar2022** 10 months ago

There are no additional costs to use Amazon EKS managed node groups. You only pay for the AWS resources that you provision.
upvoted 3 times

 **TheAbsoluteTruth** 11 months, 4 weeks ago

Selected Answer: B

La opción B es la mejor para cumplir con los requisitos de minimización de costos y gastos generales operativos mientras se ejecutan contenedores en la nube de AWS. Amazon EKS es un servicio de orquestación de contenedores altamente escalable y de alta disponibilidad que se encarga de administrar y escalar automáticamente los nodos de contenedor subyacentes. El uso de instancias de spot en un grupo de nodos administrados de Amazon EKS ayudará a reducir los costos en comparación con las instancias bajo demanda, ya que las instancias de spot son instancias de EC2 disponibles a precios significativamente más bajos, pero pueden ser interrumpidas con poco aviso. Al aprovechar la capacidad no utilizada de EC2 a un precio reducido, la empresa puede ahorrar dinero en costos de infraestructura sin comprometer la tolerancia a fallos o la escalabilidad de sus aplicaciones en contenedores.

upvoted 3 times

 **alexiscloud** 12 months ago

B: Sport instance save cost
upvoted 1 times

Question #129

Topic 1

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure. Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

- A. Migrate the PostgreSQL database to Amazon Aurora.
- B. Migrate the web application to be hosted on Amazon EC2 instances.
- C. Set up an Amazon CloudFront distribution for the web application content.
- D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
- E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Correct Answer: AE*Community vote distribution*

ArielSchivo Highly Voted 1 year, 4 months ago

Selected Answer: AE

I would say A and E since Aurora and Fargate are serverless (less operational overhead).
upvoted 10 times

baba365 6 months, 2 weeks ago

There's a difference between Amazon Aurora and Amazon Aurora Serverless
upvoted 1 times

pentium75 3 months ago

"Aurora serverless" is still a flavor of Aurora, it's not a different product.
upvoted 1 times

JTruong Most Recent 2 months, 3 weeks ago

Selected Answer: AE

PostgreSQL is compatible w/ Aurora
Fargate & ECS are also paired with containers
A&E
upvoted 1 times

Ruffyit 4 months, 3 weeks ago

I would say A and E since Aurora and Fargate are serverless (less operational overhead)
upvoted 1 times

TariqKipkemei 6 months, 3 weeks ago

Selected Answer: AE

Requirement is to reduce operational overhead,
Amazon Aurora provides built-in security, continuous backups, serverless compute, up to 15 read replicas, automated multi-Region replication.
AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without managing servers.
upvoted 3 times

Guru4Cloud 7 months, 1 week ago

Selected Answer: AE

The reasons are:

Migrating the database to Amazon Aurora provides a high performance, scalable PostgreSQL-compatible database with minimal overhead.
Migrating the containerized web app to Fargate removes the need to provision and manage EC2 instances. Fargate auto-scales.
Together, Aurora and Fargate reduce operational overhead and complexity for the data and application tiers.
upvoted 1 times

cookieMr 9 months ago

Selected Answer: AE

A is the correct answer because migrating the database to Amazon Aurora reduces operational overhead and offers scalability and automated backups.

E is the correct answer because migrating the web application to AWS Fargate with Amazon ECS eliminates the need for infrastructure management, simplifies deployment, and improves resource utilization.

- B. Migrating the web application to Amazon EC2 instances would not directly address the operational overhead and capacity planning concerns mentioned in the scenario.
- C. Setting up an Amazon CloudFront distribution improves content delivery but does not directly address the operational overhead or capacity planning limitations.
- D. Configuring Amazon ElastiCache improves performance but does not directly address the operational overhead or capacity planning challenges mentioned.

Therefore, the correct answers are A and E as they address the requirements, while the incorrect answers (B, C, D) do not provide the desired solutions.

upvoted 1 times

 **studynoplay** 10 months, 3 weeks ago

Selected Answer: AE

Improve the application's infrastructure = Modernize Infrastructure = Least Operational Overhead = Serverless

upvoted 1 times

 **Robrobtutu** 11 months, 1 week ago

Selected Answer: AE

A and E are the best options.

upvoted 1 times

 **bgsanata** 1 year ago

Selected Answer: AE

A and E

upvoted 1 times

 **rapatajones** 1 year, 2 months ago

Selected Answer: AE

a e.....

upvoted 1 times

 **goodmail** 1 year, 2 months ago

One should that Aurora is not serverless. Aurora serverless and Aurora are 2 Amazon services. I prefer C, however the question does not mention any frontend requirements.

upvoted 1 times

 **aba2s** 1 year, 2 months ago

Selected Answer: AE

Yes, go for A and E since thes two ressources are serverless.

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: AE

The correct answers are A and E. To improve the application's infrastructure, the solutions architect should migrate the PostgreSQL database to Amazon Aurora and migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Amazon Aurora is a fully managed, scalable, and highly available relational database service that is compatible with PostgreSQL. Migrating the database to Amazon Aurora would reduce the operational overhead of maintaining the database infrastructure and allow the company to focus on building and scaling the application.

AWS Fargate is a fully managed container orchestration service that enables users to run containers without the need to manage the underlying EC2 instances. By using AWS Fargate with Amazon Elastic Container Service (Amazon ECS), the solutions architect can improve the scalability and efficiency of the web application and reduce the operational overhead of maintaining the underlying infrastructure.

upvoted 1 times

 **techhb** 1 year, 3 months ago

A and E are obvious choices.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: AE

Option A and E

upvoted 1 times

 **SilentMilli** 1 year, 3 months ago

Selected Answer: AE

A and E

upvoted 1 times

 **333666999** 1 year, 3 months ago

Selected Answer: CE

C not A. and E

upvoted 1 times

 **pentium75** 3 months ago

So you'd move the database from on-premises to AWS Aurora, but leave the application containers on premises, and place Cloud Front in front of them?

upvoted 1 times

Question #130

Topic 1

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
- B. Use a target tracking policy to dynamically scale the Auto Scaling group.
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

The correct answer is B. To maintain the desired performance across all instances in the Amazon EC2 Auto Scaling group, the solutions architect should use a target tracking policy to dynamically scale the Auto Scaling group.

A target tracking policy allows the Auto Scaling group to automatically adjust the number of EC2 instances in the group based on a target value for a metric. In this case, the target value for the CPU utilization metric could be set to 40% to maintain the desired performance of the application. The Auto Scaling group would then automatically scale the number of instances up or down as needed to maintain the target value for the metric.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>
upvoted 15 times

 **awsgEEK75** Most Recent 2 months, 1 week ago

Selected Answer: B

40% CPU for best performance is a "target tracking" policy for scaling so B is correct.
A: Wrong policy
CD: Won't achieve 40% CPU
upvoted 2 times

 **Ruffyit** 4 months, 3 weeks ago

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>
upvoted 2 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: B

target tracking policy = maintain
upvoted 4 times

 **youdelin** 5 months, 2 weeks ago

Selected Answer: B

I really don't get what kind of software running like a car with the most economical fuel speed range, but well, the answer is B
upvoted 2 times

 **TariqKipkemei** 6 months, 3 weeks ago

Selected Answer: B

The application performs best when the CPU utilization of the EC2 instances is at or near 40%. Target tracking will maintain CPU utilization at 40%. When CloudWatch detects that the average CPU utilization is beyond 40%, it will trigger the target tracking policy to scale out the auto scaling group to meet this target utilization. Once everything is settled and the average CPU utilization has gone below 40%, another scale in action will kick in and reduce the number of auto scaling instances in the auto scaling group.
upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

The key reasons are:

A target tracking policy allows defining a specific target metric value to maintain, in this case 40% CPU utilization.
Auto Scaling will automatically add or remove instances to keep utilization at the target level, without manual intervention.
This will dynamically scale the group to maintain performance as load changes.
A simple scaling policy only responds to breaching thresholds, not maintaining a target.
Scheduled actions and Lambda would require manual calculation and updates to track utilization.
Target tracking policies are the native Auto Scaling feature designed to maintain a metric at a target value.

upvoted 3 times

 **cookieMr** 9 months ago

Selected Answer: B

Target tracking policy is the most appropriate choice. This policy allows ASG to automatically adjust the desired capacity based on a target metric, such as CPU utilization. By setting the target metric to 40%, ASG will scale the number of instances up or down as needed to maintain the desired CPU utilization level. This ensures that the application's performance remains optimal.

A suggests using a simple scaling policy, which allows for scaling based on a fixed metric or threshold. However, it may not be as effective as a target tracking policy in dynamically adjusting the capacity to maintain a specific CPU utilization level.

C suggests using an Lambda to update the desired capacity. While this can be done programmatically, it would require custom scripting and may not provide the same level of automation and responsiveness as a target tracking policy.

D suggests using scheduled scaling actions to scale up and down ASG at predefined times. This approach is not suitable for maintaining the desired performance in real-time based on actual CPU utilization.

upvoted 2 times

 **Robrobtutu** 11 months, 1 week ago

Selected Answer: B

B of course.

upvoted 1 times

 **aba2s** 1 year, 2 months ago

Selected Answer: B

B seem to the correct response.

With a target tracking scaling policy, you can increase or decrease the current capacity of the group based on a target value for a specific metric. This policy will help resolve the over-provisioning of your resources. The scaling policy adds or removes capacity as required to keep the metric at or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern.

upvoted 3 times

 **orionizzie** 1 year, 3 months ago

Selected Answer: B

target tracking - CPU at 40%

upvoted 2 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **ArielSchivo** 1 year, 4 months ago

Selected Answer: B

Option B. Target tracking policy.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

upvoted 4 times

 **Nigma** 1 year, 4 months ago

B

CPU utilization = target tracking

upvoted 2 times

 **SimonPark** 1 year, 4 months ago

Selected Answer: B

B is the answer

upvoted 1 times

Question #131

Topic 1

A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL. What should a solutions architect do to meet these requirements?

- A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
- B. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.
- C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
- D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

Correct Answer: D

Community vote distribution

D (100%)

✉️  **123jh10**  1 year, 5 months ago

Selected Answer: D

I want to restrict access to my Amazon Simple Storage Service (Amazon S3) bucket so that objects can be accessed only through my Amazon CloudFront distribution. How can I do that?

Create a CloudFront origin access identity (OAI)

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/>

upvoted 33 times

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

Thanks it convinces me

upvoted 1 times

✉️  **Guru4Cloud**  7 months, 1 week ago

Selected Answer: D

The key reasons are:

An OAI provides secure access between CloudFront and S3 without exposing the S3 bucket publicly.

The OAI is associated with the CloudFront distribution.

The S3 bucket policy limits access only to that OAI.

This ensures only CloudFront can access the objects, not direct S3 access.

Option A is complex to manage individual bucket policies.

Option B exposes credentials that aren't needed.

Option C works but OAI is the preferred method.

So using an origin access identity provides the most secure way to serve private S3 content through CloudFront. The OAI prevents direct public access to the S3 bucket.

upvoted 7 times

✉️  **xdkonorek2**  4 months, 3 weeks ago

Selected Answer: D

C would also work but missing important details in the answer

D is legacy and architect should not recommend it

upvoted 4 times

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

Selected Answer: D

"If your users try to access objects using Amazon S3 URLs, they're denied access. The origin access identity has permission to access objects in your Amazon S3 bucket, but users don't."

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

upvoted 1 times

✉️  **cookieMr** 9 months ago

Selected Answer: D

To meet the requirements of serving files through CloudFront while restricting direct access to the S3 bucket URL, the recommended approach is to use an origin access identity (OAI). By creating an OAI and assigning it to the CloudFront distribution, you can control access to the S3 bucket.

This setup ensures that the files stored in the S3 bucket are only accessible through CloudFront and not directly through the S3 bucket URL.

Requests made directly to the S3 URL will be blocked.

Option A suggests writing individual policies for each S3 bucket, which can be cumbersome and difficult to manage, especially if there are multiple

buckets involved.

Option B suggests creating an IAM user and assigning it to CloudFront, but this does not address restricting direct access to the S3 bucket URL.

Option C suggests writing an S3 bucket policy with CloudFront distribution ID as the Principal, but this alone does not provide the necessary restrictions to prevent direct access to the S3 bucket URL.

upvoted 3 times

✉ **antropaws** 9 months, 4 weeks ago

DECEMBER 2022 UPDATE:

Restricting access to an Amazon S3 origin:

CloudFront provides two ways to send authenticated requests to an Amazon S3 origin: origin access control (OAC) and origin access identity (OAI). We recommend using OAC because it supports:

All Amazon S3 buckets in all AWS Regions, including opt-in Regions launched after December 2022
Amazon S3 server-side encryption with AWS KMS (SSE-KMS)
Dynamic requests (PUT and DELETE) to Amazon S3

OAI doesn't work for the scenarios in the preceding list, or it requires extra workarounds in those scenarios.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

upvoted 1 times

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

Selected Answer: D

The correct answer is D. To meet the requirements, the solutions architect should create an origin access identity (OAI) and assign it to the CloudFront distribution. The S3 bucket permissions should be configured so that only the OAI has read permission.

An OAI is a special CloudFront user that is associated with a CloudFront distribution and is used to give CloudFront access to the files in an S3 bucket. By using an OAI, the company can serve the files through the CloudFront distribution while preventing direct access to the S3 bucket.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

upvoted 4 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: D

D is the right answer

upvoted 1 times

✉ **gloritown** 1 year, 3 months ago

Selected Answer: D

D is correct but instead of OAI using OAC would be better since OAI is legacy

upvoted 3 times

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

Thanks, I didn't know about OAC.

upvoted 1 times

✉ **Wpcorgan** 1 year, 4 months ago

D is correct

upvoted 1 times

Question #132

Topic 1

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

Which combination should a solutions architect recommend to meet these requirements?

- A. Amazon CloudFront and Amazon S3
- B. AWS Lambda and Amazon DynamoDB
- C. Application Load Balancer with Amazon EC2 Auto Scaling
- D. Amazon Route 53 with internal Application Load Balancers

Correct Answer: A*Community vote distribution*


3%

 **G3**  1 year, 1 month ago

Selected Answer: A

Historical reports = Static content = S3
upvoted 17 times

 **dokaedu**  1 year, 4 months ago

A is the correct answer
The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.
upvoted 10 times

 **MrPCarrot**  2 months, 1 week ago

Bringing content closer to users, Answer is A
upvoted 2 times

 **TariqKipkemei** 6 months, 3 weeks ago

Selected Answer: A

Global, cost-effective, serverless, low latency = CloudFront with S3
Static content = S3
upvoted 5 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A
Historical reports = Static content = S3
upvoted 2 times

 **cookieMr** 9 months ago

By using CloudFront, the website can leverage the global network of edge locations to cache and deliver the performance reports to users from the nearest edge location, reducing latency and providing fast response times. Amazon S3 serves as the origin for the files, where the reports are stored.

Option B is incorrect because AWS Lambda and Amazon DynamoDB are not the most suitable services for serving downloadable files and meeting the website demands globally.

Option C is incorrect because using an Application Load Balancer with Amazon EC2 Auto Scaling may require more infrastructure provisioning and management compared to the CloudFront and S3 combination. Additionally, it may not provide the same level of global scalability and fast response times as CloudFront.

Option D is incorrect because while Amazon Route 53 is a global DNS service, it alone does not provide the caching and content delivery capabilities required for serving the downloadable reports. Internal Application Load Balancers do not address the global scalability and caching requirements specified in the scenario.

upvoted 4 times

 **Bmarodi** 8 months, 2 weeks ago

Very good explanations!
upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: A

The correct answer is Option A. To meet the requirements, the solutions architect should recommend using Amazon CloudFront and Amazon S3.

By combining Amazon CloudFront and Amazon S3, the solutions architect can provide a scalable and cost-effective solution that limits the provisioning of infrastructure resources and provides the fastest possible response time.

<https://aws.amazon.com/cloudfront/>

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

upvoted 3 times

✉ **techhb** 1 year, 3 months ago

A is correct

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: A

A is the best and most cost effective option if only download of the static pre-created report(no data processing before downloading) is a requirement.

upvoted 1 times

✉ **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 1 times

✉ **sdasdawa** 1 year, 4 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/27935-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

✉ **Nirmal3331** 1 year, 4 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/27935-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

✉ **sAMPLUNK** 1 year, 4 months ago

Selected Answer: A

See this discussion:

<https://www.examtopics.com/discussions/amazon/view/27935-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

✉ **manu427** 1 year, 4 months ago

Selected Answer: C

load balancing + scalability + cost effective

upvoted 1 times

✉ **pentium75** 3 months ago

Why use EC2 instances to serve historical report files? Those belong in S3. No need to run in VM to let users download static content.

upvoted 3 times

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

Selected Answer: B

I think the answer is B

upvoted 1 times

✉ **pentium75** 3 months ago

No ;) Both cannot store the reports nor provide them for download.

upvoted 3 times

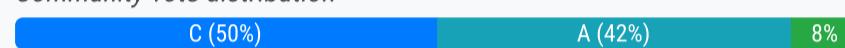
Question #133

Topic 1

A company runs an Oracle database on premises. As part of the company's migration to AWS, the company wants to upgrade the database to the most recent available version. The company also wants to set up disaster recovery (DR) for the database. The company needs to minimize the operational overhead for normal operations and DR setup. The company also needs to maintain access to the database's underlying operating system.

Which solution will meet these requirements?

- A. Migrate the Oracle database to an Amazon EC2 instance. Set up database replication to a different AWS Region.
- B. Migrate the Oracle database to Amazon RDS for Oracle. Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.
- C. Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the database in another AWS Region.
- D. Migrate the Oracle database to Amazon RDS for Oracle. Create a standby database in another Availability Zone.

Correct Answer: D*Community vote distribution*

ArielSchivo Highly Voted 1 year, 4 months ago

Option C since RDS Custom has access to the underlying OS and it provides less operational overhead. Also, a read replica in another Region can be used for DR activities.

<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>
upvoted 33 times

KalarAzar 9 months, 2 weeks ago

You can't create cross-Region replicas in RDS Custom for Oracle: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/custom-rr.html#custom-rr.limitations>

upvoted 17 times

brushek Highly Voted 1 year, 5 months ago

Selected Answer: C

It should be C:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-custom.html>
and
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/working-with-custom-oracle.html>
upvoted 19 times

bhgt 5 months, 3 weeks ago

how it is C when the read replica is not meant for DR
upvoted 2 times

wsdasdasdqwdaw 5 months ago

If the source DB instance fails, you can promote your Read Replica to a standalone source server.
upvoted 7 times

Uzbekistan Most Recent 3 days, 3 hours ago

Selected Answer: D

Option C and B Do Not provide disaster recovery which is part of question.

Overall, option D provides a managed solution with minimal operational overhead, automated backups, disaster recovery capabilities, and high availability while meeting the requirement of maintaining access to the underlying operating system.
Create a standby database in another Availability Zone.
upvoted 1 times

Kenneth99 2 weeks ago

Vote C

<https://aws.amazon.com/blogs/database/part-2-implement-multi-master-replication-with-rds-custom-for-oracle-high-availability-disaster-recovery/>

The second node can be used as read replica and serve for DR
upvoted 1 times

wizcloudifa 3 weeks, 4 days ago

Selected Answer: D

Its straight forward guys, only D provides the DR solution and no other options do, so D is the right answer

upvoted 1 times

 **chickenmf** 2 weeks, 6 days ago

RDS Custom is the only DB that provides access to the underlying OS

upvoted 2 times

 **Saiyh** 1 month, 1 week ago

RDS Custom makes it possible for you as a database administrator to access and customize your database environment and operating system. With RDS Custom, you can customize to meet the requirements of legacy, custom, and packaged applications.

Amazon RDS Custom for Oracle supports read replicas that are built on Data Guard technology, and you can use these replicas to offload reads from the primary and for disaster recovery

upvoted 1 times

 **thewalker** 1 month, 3 weeks ago

Selected Answer: C

Only A and C will provide the access to the underlying infrastructure. C is the best option as it is the managed service from AWS.

upvoted 1 times

 **rt_7777** 2 months ago

Not sure why answer is D where another availability is only HA setup not DR

upvoted 1 times

 **Mitansh** 2 months, 1 week ago

Selected Answer: C

it is true guys, it should be C

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

This is my second pass of the question and after doing a lot of research I think both A and C are right as there is no tie-breaker in the question. A will work as well as D. the solution is not required to be least costly, least administrative, etc. when it comes to "underlying access to the OS". Custom RDS gives you root access to the underlying instance and AWS takes care of instance upgrade and placement. This makes it slightly better than A but A also gives you the underlying access but in much better way. So what is the priority here? I would still stick with C just because it promotes an AWS product.

upvoted 1 times

 **bujuman** 2 months, 2 weeks ago

Selected Answer: A

Simple as voting option A in order to maintain access to underlying OS

upvoted 3 times

 **Wang87** 2 months, 3 weeks ago

Selected Answer: A

Underlying access is only available on EC2 and RDS Custom
RDS custom Limitations

- 1) You can't create RDS custom for Oracle in Read- only mode,
- 2) You can't create cross-region RDS custom for oracle replicas.

Answer is : A

upvoted 5 times

 **awsgeek75** 2 months, 3 weeks ago

Selected Answer: C

Choice is between A and C as only these options allow access to underlying OS (required part of the question).

Between EC2 and RDS Custom, the RDS custom is better as it utilizes more of AWS offerings. Read replicas have to be made manually in different regions for DR in both options A and C but A uses at least one extra AWS managed service to reduce the overhead so it looks more beneficial for the user.

upvoted 1 times

 **JTruong** 2 months, 3 weeks ago

Selected Answer: C

<https://aws.amazon.com/rds/custom/>

Scroll down to the Benefits of Amazon RDS Custom - Priv. access to underlying OS & DB environment

So...C is the correct answer

upvoted 3 times

 **Sadiya_Javid_Abbasi** 2 months, 4 weeks ago

Build high availability for Amazon RDS Custom for Oracle using read replicas

<https://aws.amazon.com/blogs/database/build-high-availability-for-amazon-rds-custom-for-oracle-using-read-replicas/>

You can achieve high availability (HA) and disaster recovery (DR) for Oracle databases using a physical standby database by creating and maintaining a physical copy of the primary database. The standby instance can be hosted in a location different and far enough from the primary instance, such as a different Region or Availability Zone, to maintain the availability of the database when the primary instance is impacted by unplanned incidents

upvoted 1 times

✉️  **djgodzilla** 3 months ago

you can always create an external replicas in another EC2 instance on a different region
upvoted 1 times

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

Selected Answer: D

You are all wrong. The answer is (D)
Because option (C) read-only replicas are restricted to the same region as the original database, option (B) snapshots cannot be written (to maintain the underlying operating system)
The only way is (D)

upvoted 1 times

✉️  **pentium75** 3 months ago

But D doesn't provide "access to the underlying operating system". Requirement is DR, it does not say anything about different region (DR could be in another AZ).

upvoted 1 times

Question #134

Topic 1

A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing and new data by using SL. The company stores the data in an Amazon S3 bucket. The data requires encryption and must be replicated to a different AWS Region. Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon Athena to query the data.
- B. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon RDS to query the data.
- C. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.
- D. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon RDS to query the data.

Correct Answer: A

Community vote distribution

C (51%)

A (49%)

✉  **123jh10**  1 year, 5 months ago

Selected Answer: C

SSE-KMS vs SSE-S3 - The last seems to have less overhead (as the keys are automatically generated by S3 and applied on data at upload, and don't require further actions. KMS provides more flexibility, but in turn involves a different service, which finally is more "complex" than just managing one (S3). So A and B are excluded. If you are in doubt, you are having 2 buckets in A and B, while just keeping one in C and D.

<https://s3browser.com/server-side-encryption-types.aspx>

Decide between C and D is deciding on Athena or RDS. RDS is a relational db, and we have documents on S3, which is the use case for Athena.

Athena is also serverless, which eliminates the need of controlling the underlying infrastructure and capacity. So C is the answer.

<https://aws.amazon.com/athena/>

upvoted 52 times

✉  **markw92** 9 months, 1 week ago

See comment from Nicknameinvalid below. You get your answer.

upvoted 1 times

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

It's since replication works for new objects but not for the existing ones, unless you use batch replication which is not the case.

upvoted 1 times

✉  **Chiznitz** 4 months, 2 weeks ago

Answer A has you move the data before you enable replication, therefore there is no difference between A and C when it comes to the point in time you enable replication. I agree A would be a better choice if the order of operations said, create a bucket->Enable encryption->move files...but it doesn't. It has you create the bucket and move the files.

upvoted 2 times

✉  **dokaedu**  1 year, 4 months ago

Answer is A:

Amazon S3 Bucket Keys reduce the cost of Amazon S3 server-side encryption using AWS Key Management Service (SSE-KMS). This new bucket-level key for SSE can reduce AWS KMS request costs by up to 99 percent by decreasing the request traffic from Amazon S3 to AWS KMS. With a few clicks in the AWS Management Console, and without any changes to your client applications, you can configure your bucket to use an S3 Bucket Key for AWS KMS-based encryption on new objects.

The Existing S3 bucket might have unencrypted data - encryption will apply new data received after the applying of encryption on the new bucket.

upvoted 24 times

✉  **s50600822** 10 months, 2 weeks ago

Don't know what "kays" are, could they be a trap?

upvoted 1 times

✉  **Bmarodi** 9 months, 3 weeks ago

Kays = keys, mistype i think.

upvoted 1 times

✉  **AKBM7829** 7 months ago

But in server side encryption Multi Region Keys is not possible which leaves to Option C

upvoted 2 times

✉  **RBSK** 1 year, 3 months ago

Cost reduction is in comparison bet Bucket level KMS key and object level KMS key. Not between SSE-KMS and SSE-S3. Hence its a wrong comparison
upvoted 2 times

 **RODROSKAR** 1 year, 4 months ago

Reducing cost was never the target, it's LEAST operational. In that regard SSE-S3 AWS fully managed.
upvoted 3 times

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

The answer is A because SSE-S3 does not support cross-region replication of encrypted data. If you perform cross-region replication, you will have to re-encrypt the data.
upvoted 1 times

 **suryansb** 1 month ago

Selected Answer: A

awai it is correct
upvoted 1 times

 **thewalker** 1 month, 3 weeks ago

Selected Answer: C

As per Amazon Q:

The easiest way to encrypt existing objects in S3 is to use server-side encryption with S3-managed keys (SSE-S3). Here are the basic steps:
 1. Enable SSE-S3 on the target S3 bucket if it is not already enabled. This will ensure all new or copied objects are encrypted automatically.
 2. Create an S3 inventory report for the source bucket containing the objects. This will generate a CSV file with metadata of all objects.
 3. Use S3 Select or AWS Athena to query the inventory report and filter for only unencrypted objects.
 4. Create an S3 Batch Operations job to copy the filtered unencrypted objects to the target bucket. The copy operation will automatically encrypt the objects using the bucket's SSE-S3 configuration.

upvoted 1 times

 **thewalker** 1 month, 3 weeks ago

5. Monitor the job completion to ensure all objects were encrypted. You can optionally delete the original unencrypted versions after verifying successful encryption.
This approach minimizes disruption and performs the encryption without having to rewrite existing data or code.

Also Refer:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-copy-example-bucket-key.html>

upvoted 1 times

 **pentium75** 3 months ago

Selected Answer: C

Data in S3 is queried with Athena, not RDS, thus B and D are out.

A requires a new bucket and loading data into that - Why, since data is already in S3? It says to enable CRR only after loading the data, so existing data won't be replicated anyway.

C uses existing data (less operational overhead compared to loading data into a new bucket) and SSE-E3 (less operational overhead than SSE-KMS).

upvoted 6 times

 **LoXoL** 2 months, 2 weeks ago

Most clear explanation. Thanks!
upvoted 1 times

 **DHADD003** 3 months ago

Selected Answer: A

I selected A because SSE-S3 keys are not multi-regional keys. You must use SSE-KMS for the multi-regional keys and then for serverless its Aurora.
upvoted 1 times

 **pentium75** 3 months ago

It says "data requires encryption", not that it must use same key in both regions.
upvoted 1 times

 **djgodzilla** 3 months ago

Selected Answer: A

The most suitable solution with the least operational overhead for the company's requirements is:

Option A:

Create a new S3 bucket.

Load the data into the new S3 bucket.

Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region.

Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS).

Use Amazon Athena to query the data.

This option aligns with the specified requirements of encrypting the data, replicating it to a different AWS Region, and utilizing serverless querying with Amazon Athena. It also minimizes operational overhead by leveraging AWS managed services.

upvoted 2 times

 **SaurabhTiwari1** 3 months ago

Selected Answer: A

A is correct - SSE-KMS is multi region keys and Athena is serverless for analyze

C is incorrect - SSE-S3 is region specific for encryption

upvoted 1 times

 **kmargaronis** 3 months, 1 week ago

Selected Answer: C

C. is correct after January 2023 because "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."

upvoted 2 times

 **chasingsummer** 3 months, 1 week ago

Selected Answer: C

SSE-S3 is the easiest to use and offers strong encryption, while SSE-C provides more control over your encryption keys (and much more admin overhead)

upvoted 1 times

 **ale_brd_** 3 months, 2 weeks ago

Selected Answer: C

Therefore, the most appropriate solution to meet the requirements of the serverless application is to load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.

This solution effectively leverages the existing S3 bucket, S3 Cross-Region Replication for data replication, SSE-S3 for encryption, and Amazon Athena for efficient data querying, enabling the company to analyze existing and new data with minimal management effort and a serverless architecture.

upvoted 1 times

 **ale_brd_** 3 months, 2 weeks ago

Selected Answer: A

the most appropriate solution to meet the requirements of the serverless application is to load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.

This solution effectively leverages the existing S3 bucket, S3 Cross-Region Replication for data replication, SSE-S3 for encryption, and Amazon Athena for efficient data querying, enabling the company to analyze existing and new data with minimal management effort and a serverless architecture.

upvoted 1 times

 **BhavyaMPatel** 3 months, 3 weeks ago

Selected Answer: C

right answer should be c as we need less overhead and if we are using sse-s3

then encrypted object and object encrypted with sse-s3 replicate by default for object encrypted with sse-kms. Specify which KMS Key to encrypt the objects within the target bucket we need to adapt the KMS Key Policy for the target key, An IAM Role with kms:Decrypt for the source KMS Key and kms:Encrypt for the target KMS Key, we might get KMS throttling errors, in which case you can ask for a Service Quotas increase so less operation is in c option so right answer should be c

upvoted 1 times

 **sofodofo** 4 months, 4 weeks ago

Selected Answer: C

Seems like C - refer to <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html#replication-default-encryption>

<How default bucket encryption affects replication>

When you enable default encryption for a replication destination bucket, the following encryption behavior applies:

- If objects in the source bucket are not encrypted, the replica objects in the destination bucket are encrypted by using the default encryption settings of the destination bucket. As a result, the entity tags (ETags) of the source objects differ from the ETags of the replica objects. If you have applications that use ETags, you must update those applications to account for this difference.

upvoted 1 times

 **RNess** 5 months, 1 week ago

Selected Answer: A

<https://aws.amazon.com/blogs/storage/encrypting-existing-amazon-s3-objects-with-the-aws-cli/#:~:text=To%20encrypt%20an%20existing%20object,data%20using%20server%2Dside%20encryption.>

upvoted 1 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: A

"To encrypt an existing object using SSE, you replace the object. To encrypt existing objects in place, you can use the Copy Object or Copy Part API. This copies the objects with the same name and encrypts the object data using server-side encryption."

<https://aws.amazon.com/blogs/storage/encrypting-existing-amazon-s3-objects-with-the-aws-cli/#:~:text=To%20encrypt%20an%20existing%20object,data%20using%20server%2Dside%20encryption.>

upvoted 2 times

Question #135

Topic 1

A company runs workloads on AWS. The company needs to connect to a service from an external provider. The service is hosted in the provider's VPC. According to the company's security team, the connectivity must be private and must be restricted to the target service. The connection must be initiated only from the company's VPC.

Which solution will meet these requirements?

- A. Create a VPC peering connection between the company's VPC and the provider's VPC. Update the route table to connect to the target service.
- B. Ask the provider to create a virtual private gateway in its VPC. Use AWS PrivateLink to connect to the target service.
- C. Create a NAT gateway in a public subnet of the company's VPC. Update the route table to connect to the target service.
- D. Ask the provider to create a VPC endpoint for the target service. Use AWS PrivateLink to connect to the target service.

Correct Answer: D

Community vote distribution

D (100%)

 **123jh10**  1 year, 5 months ago

Selected Answer: D

AWS PrivateLink provides private connectivity between VPCs, AWS services, and your on-premises networks, without exposing your traffic to the public internet. AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify your network architecture.

Interface **VPC endpoints**, powered by AWS PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace.

<https://aws.amazon.com/privatelink/>

upvoted 32 times

 **remand**  1 year, 2 months ago

Selected Answer: D

The solution that meets these requirements best is option D.

By asking the provider to create a VPC endpoint for the target service, the company can use AWS PrivateLink to connect to the target service. This enables the company to access the service privately and securely over an Amazon VPC endpoint, without requiring a NAT gateway, VPN, or AWS Direct Connect. Additionally, this will restrict the connectivity only to the target service, as required by the company's security team.

Option A VPC peering connection may not meet security requirement as it can allow communication between all resources in both VPCs.

Option B, asking the provider to create a virtual private gateway in its VPC and use AWS PrivateLink to connect to the target service is not the optimal solution because it may require the provider to make changes and also you may face security issues.

Option C, creating a NAT gateway in a public subnet of the company's VPC can expose the target service to the internet, which would not meet the security requirements.

upvoted 8 times

 **RNess**  5 months, 1 week ago

Selected Answer: D

AWS PrivateLink / VPC Endpoint Services:

- Connect services privately from your service VPC to customers VPC
- Doesn't need VPC Peering, public Internet, NAT Gateway, Route Tables
- Must be used with Network Load Balancer & ENI

upvoted 1 times

 **TariqKipkemei** 6 months, 3 weeks ago

Selected Answer: D

option D is correct

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

The best solution to meet the requirements is option D:

Ask the provider to create a VPC endpoint for the target service

Use AWS PrivateLink to connect to the target service

The reasons are:

PrivateLink provides private connectivity between VPCs without using public internet.

The provider creates a VPC endpoint in their VPC for the target service.

The company uses PrivateLink to securely access the endpoint from their VPC.

Connectivity is restricted only to the target service.

The connection is initiated only from the company's VPC.
Options A, B, C would expose the connection to the public internet or require infrastructure changes in the provider's VPC.

PrivateLink enables private, restricted connectivity to the target service without VPC peering or public exposure.
upvoted 2 times

 **cookieMr** 9 months ago

Selected Answer: D

Option C meets the requirements of establishing a private and restricted connection to the service hosted in the provider's VPC. By asking the provider to create a VPC endpoint for the target service, you can establish a direct and private connection from your company's VPC to the target service. AWS PrivateLink ensures that the connectivity remains within the AWS network and does not require internet access. This ensures both privacy and restriction to the target service, as the connection can only be initiated from your company's VPC.

- A. VPC peering does not restrict access only to the target service.
- B. PrivateLink is typically used for accessing AWS services, not external services in a provider's VPC.
- C. NAT gateway does not provide a private and restricted connection to the target service.

Option D is the correct choice as it uses AWS PrivateLink and VPC endpoint to establish a private and restricted connection from the company's VPC to the target service in the provider's VPC.

upvoted 3 times

 **Abrar2022** 9 months, 4 weeks ago

VPC Endpoint (Target Service) - for specific services (not accessing whole vpc)
VPC Peering - (accessing whole VPC)
upvoted 3 times

 **Abrar2022** 10 months ago

VPC Peering Connection:
All resources in a VPC, such as ECSs and load balancers, can be accessed.

VPC Endpoint:

Allows access to a specific service or application. Only the ECSs and load balancers in the VPC for which VPC endpoint services are created can be accessed.

upvoted 1 times

 **eugene_stalker** 10 months ago

Selected Answer: D

Option D, but seems that it is vice versa. Customer needs to create PrivateLink and VPC endpoint to connect to PrivateLink
upvoted 1 times

 **studynoplay** 10 months, 3 weeks ago

AWS PrivateLink / VPC Endpoint Services:

- Connect services privately from your service VPC to customers VPC
- Doesn't need VPC Peering, public Internet, NAT Gateway, Route Tables
- Must be used with Network Load Balancer & ENI

upvoted 2 times

 **Help2023** 1 year, 1 month ago

Selected Answer: D

D. Here you are the one initiating the connection

upvoted 1 times

 **devonwho** 1 year, 1 month ago

Selected Answer: D

PrivateLink is a more generalized technology for linking VPCs to other services. This can include multiple potential endpoints: AWS services, such as Lambda or EC2; Services hosted in other VPCs; Application endpoints hosted on-premises.

<https://www.tinystacks.com/blog-post/aws-vpc-peering-vs-privatelink-which-to-use-and-when/>

upvoted 1 times

 **devonwho** 1 year, 1 month ago

Selected Answer: D

While VPC peering enables you to privately connect VPCs, AWS PrivateLink enables you to configure applications or services in VPCs as endpoints that your VPC peering connections can connect to.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: D

The solution that meets these requirements is Option D:

- * Ask the provider to create a VPC endpoint for the target service.
- * Use AWS PrivateLink to connect to the target service.

Option D involves asking the provider to create a VPC endpoint for the target service, which is a private connection to the service that is hosted in the provider's VPC. This ensures that the connection is private and restricted to the target service, as required by the company's security team. The company can then use AWS PrivateLink to connect to the target service over the VPC endpoint. AWS PrivateLink is a fully managed service that

enables you to privately access services hosted on AWS, on-premises, or in other VPCs. It provides secure and private connectivity to services by using private IP addresses, which ensures that traffic stays within the Amazon network and does not traverse the public internet.

Therefore, Option D is the solution that meets the requirements.

upvoted 2 times

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

AWS PrivateLink documentation: <https://docs.aws.amazon.com/privatelink/latest/userguide/what-is-privatelink.html>

upvoted 1 times

✉ **techhb** 1 year, 3 months ago

D is right, if requirement was to be ok with public internet then option C was ok.

upvoted 1 times

✉ **k1kavi1** 1 year, 3 months ago

Selected Answer: D

D (VPC endpoint) looks correct. Below are the differences between VPC Peering & VPC endpoints.

https://support.huaweicloud.com/intl/en-us/vpcep_faq/vpcep_04_0004.html#:~:text>You%20can%20create%20a%20VPC%20endpoint%20to%20connect%20your%20local,connection%20over%20an%20internal%20network.&text=VPC%20Peering%20supports%20only%20communications%20between%20two%20VPCs%20in%20the%20same%20region.&text=You%20can%20use%20Cloud%20Connect,between%20VPCs%20in%20different%20regions.

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: D

D is the right answer

upvoted 1 times

Question #136

Topic 1

A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The on-premises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on-premises database.

Which combination of actions must a solutions architect take to meet these requirements? (Choose two.)

- A. Create an ongoing replication task.
- B. Create a database backup of the on-premises database.
- C. Create an AWS Database Migration Service (AWS DMS) replication server.
- D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization.

Correct Answer: CD*Community vote distribution*

123jh10 1 year, 5 months ago

Selected Answer: AC

AWS Database Migration Service (AWS DMS) helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database.

... With AWS Database Migration Service, you can also continuously replicate data with low latency from any supported source to any supported target.

<https://aws.amazon.com/dms/>

upvoted 26 times

pentium75 3 months ago

PostgreSQL -> Aurora PostgreSQL requires schema conversion per <https://aws.amazon.com/dms/schema-conversion-tool/>

upvoted 2 times

LoXoL 2 months, 2 weeks ago

SCT is compatible with PostgreSQL as source and Aurora PostgreSQL as destination, but not required.

upvoted 1 times

gustavtd 1 year, 2 months ago

Selected Answer: AC

AC, here it is clearly shown https://docs.aws.amazon.com/zh_cn/dms/latest/sbs/chap-manageddatabases.postgresql-rds-postgresql.html

upvoted 8 times

LuckyAro 1 year, 2 months ago

You nailed it !

upvoted 1 times

Alphateccc 2 weeks, 1 day ago

answer is CD : postgresql and aurora postgresql have different schemes, you need sct for conversion and dms for the migration (replication)

upvoted 1 times

vip2 1 month, 1 week ago

Selected Answer: AC

AC

perform ongoing replication using AWS DMS to keep the source and target databases in sync

upvoted 1 times

farnamjam 2 months, 4 weeks ago

Selected Answer: AC

DMS has Continuous Data Replication using CDC

upvoted 2 times

Michael_Li 3 months, 2 weeks ago

CD

A is out because it does not specify what is the service to perform the replication task, clearly what needed here is DMS

B is out because backup is solution to keep 2 DB in sync, backup and restore takes long time

C is correct as DMS takes care both full load and ongoing replication, see this youtube video <https://www.youtube.com/watch?v=VhXDa9SPDLw>

D is right as from to PostgreSQL to Amazon Aurora PostgreSQL you need AWS Schema Conversion Tool, see <https://aws.amazon.com/dms/schema-conversion-tool/>

E is out monitor itself doen't perform the replication work, if we have to choose 3 options then we can have E selected

upvoted 2 times

 **pentium75** 3 months ago

https://docs.aws.amazon.com/zh_cn/dms/latest/sbs/chap-manageddatabases.postgresql-rds-postgresql-ongoing-replication.html literally says that you must "configure the ongoing replication task"

upvoted 2 times

 **Mikado211** 3 months, 3 weeks ago

Well technically when you operate such task, you must create a database on the cloud, then operate a migration using DMS and none of the propositions give you those two tasks separately. Sometimes those questions can be really frustrating.

upvoted 1 times

 **Amitabha09** 5 months, 3 weeks ago

- C. Create an AWS Database Migration Service (AWS DMS) replication server.
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization.

AWS DMS can replicate data from on-premises databases to Aurora PostgreSQL in real time, so the on-premises database will remain online and accessible during the migration. AWS DMS can also automatically convert the database schema, so there is no need to use AWS SCT.

An Amazon EventBridge rule can be used to monitor the database synchronization and send notifications if any errors occur. This is important because it allows the solutions architect to quickly identify and resolve any issues that may arise during the migration.

A database backup of the on-premises database is not necessary because AWS DMS will replicate the data in real time. Creating an ongoing replication task is not necessary because AWS DMS will automatically create an ongoing replication task when the replication server is created.

upvoted 2 times

 **David_Ang** 5 months, 1 week ago

Mate you can monitor everything you want but it is not going to make sure the synchronization is working, an alert is not going to help.

upvoted 3 times

 **TariqKipkemei** 6 months, 3 weeks ago

Selected Answer: AC

Create an AWS Database Migration Service (AWS DMS) replication server then create an ongoing replication task

upvoted 3 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: AC

A) Create an ongoing replication task

C) Create an AWS Database Migration Service (AWS DMS) replication server

The key reasons are:

An ongoing DMS replication task keeps the source and target databases synchronized during the migration.

The DMS replication server manages and executes the replication tasks.

Together, these will continuously replicate changes from on-prem to Aurora to keep them in sync.

A database backup alone wouldn't maintain synchronization.

upvoted 1 times

 **MutiverseAgent** 8 months, 1 week ago

Selected Answer: AC

<https://docs.aws.amazon.com/dms/latest/sbs/chap-manageddatabases.postgresql-rds-postgresql.html>

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_GettingStarted.Replication.html

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: AC

These two actions (AC) will help meet the requirements of migrating the on-premises PostgreSQL database to Amazon Aurora PostgreSQL while keeping the on-premises database accessible and synchronized with the Aurora database. The ongoing replication task will ensure continuous data replication between the on-premises database and Aurora. The AWS DMS replication server will facilitate the migration process and handle the data replication.

B. Creating a database backup does not ensure ongoing synchronization.

D. Converting the database schema does not address the requirement of synchronization.

E. Creating an EventBridge rule only monitors synchronization, but doesn't handle migration.

The correct combination is A and C.

upvoted 3 times

 **Nandha707** 9 months, 2 weeks ago

Answer is CD. Postgresql to Aurora Postgresql needed SCT.

<https://aws.amazon.com/ko/dms/schema-conversion-tool/>

upvoted 1 times

 **Bmarodi** 9 months, 3 weeks ago

Selected Answer: AC

Option A & C are the right answer.

upvoted 1 times

✉ **kruasan** 11 months ago

Selected Answer: AC

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-postgresql-database-to-aurora-postgresql.html>
upvoted 1 times

✉ **osmk** 1 year ago

A-><https://docs.aws.amazon.com/dms/latest/sbs/chap-manageddatabases.oracle2rds.replication.html>
C-><https://docs.aws.amazon.com/dms/latest/userguide/Welcome.html>

upvoted 2 times

✉ **Erbug** 1 year ago

Selected Answer: AC

This question is giving us two conditions to solve it. One of them is on-premise database must remain online and accessible during the migration and the second one is Aurora database must remain synchronized with the on-premises database. So to meet them all A and C will be the correct options for us.

PS: if the question was just asking us something related to the DB migration process alone, all options would be correct.

upvoted 2 times

Question #137

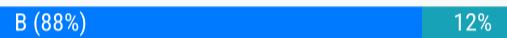
Topic 1

A company uses AWS Organizations to create dedicated AWS accounts for each business unit to manage each business unit's account independently upon request. The root email recipient missed a notification that was sent to the root user email address of one account. The company wants to ensure that all future notifications are not missed. Future notifications must be limited to account administrators. Which solution will meet these requirements?

- A. Configure the company's email server to forward notification email messages that are sent to the AWS account root user email address to all users in the organization.
- B. Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.
- C. Configure all AWS account root user email messages to be sent to one administrator who is responsible for monitoring alerts and forwarding those alerts to the appropriate groups.
- D. Configure all existing AWS accounts and all newly created accounts to use the same root user email address. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

Correct Answer: D

Community vote distribution



✉️ **123jh10** 1 year, 5 months ago

Selected Answer: B

Use a group email address for the management account's root user
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_email-address
 upvoted 24 times

✉️ **cookieMr** 9 months ago

Selected Answer: B

Option B ensures that all future notifications are not missed by configuring the AWS account root user email addresses as distribution lists that are monitored by a few administrators. By setting up alternate contacts in the AWS Organizations console or programmatically, the notifications can be sent to the appropriate administrators responsible for monitoring and responding to alerts. This solution allows for centralized management of notifications and ensures they are limited to account administrators.

- A. Floods all users with notifications, lacks granularity.
 - C. Manual forwarding introduces delays, centralizes responsibility.
 - D. No flexibility for specific account administrators, limits customization.
- upvoted 7 times

✉️ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: B

No idea why "D" would be correct answer unless there is some missing context in the question or the answer. "B" is best practice as pointed out in other links.
 upvoted 1 times

✉️ **David_Ang** 5 months, 1 week ago

Selected Answer: B

the only answer with sense is "B", because "A" is not exclusive, "C" is exactly the case the want to avoid, and "D" just don't make sense
 upvoted 1 times

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

Selected Answer: B

distribution list is the way to go
 upvoted 2 times

✉️ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

The reasons are:

- Alternate contacts allow defining other users to receive root emails.
 - Distribution lists ensure multiple admins get notified.
 - Limits notifications to account admins rather than all users.
 - Using the same root email address for all accounts (Option D) is not recommended.
 - Relying on one admin or external forwarding (Options A, C) introduces delays or single points of failure.
- upvoted 1 times

 **Itsume** 9 months, 1 week ago

all admins need access or else some wont get the right mails and cant do their job,
sending it only to a few would disrupt the workflows so it is D

upvoted 1 times

 **fishy_resolver** 9 months, 3 weeks ago

Selected Answer: D

From the links provided below there are no mention of having a distribution list capability within AWS:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_email-address

As per link for best practices:

Use a group email address for the management account's root user!

upvoted 1 times

 **Abrar2022** 9 months, 4 weeks ago

The clue is in the pudding!!

Question: account "administrators"

Answer: Configure all AWS account root user email addresses as distribution lists that go to a few "administrators"

upvoted 1 times

 **Rainchild** 11 months ago

Selected Answer: B

Option A: wrong - sends email to everybody

Option B: correct (but sub-optimal because distribution lists aren't all that secure)

Option C: wrong - single point of failure on the new administrator

Option D: wrong - each root email address must be unique, you can't change them all to the same one

upvoted 2 times

 **jdr75** 11 months, 3 weeks ago

Selected Answer: B

The more aligned answer to this article:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_email-address

is B.

D would be best if it'd said that the email you configure as "root user email address" will be a distribution list.

The phrase "all future notifications are not missed" points to D, cos' it said:

".. and all newly created accounts to use the same root user email address"

so the future account that will be created will be covered with the business policy.

It's not 100% clear, but I'll choose B.

upvoted 2 times

 **TheAbsoluteTruth** 11 months, 4 weeks ago

Una pregunta si la gente va votando las preguntas por que los administradores no cambian la respuesta correcta. Es a interpretación y ya?

upvoted 1 times

 **jdr75** 11 months, 3 weeks ago

El administrador de "examtopics" pasa olímpicamente de marcar la respuesta correcta y es evidente que muchas respuestas que indica como "correctas" no lo son. Dice muy poco del servicio que dan.

upvoted 1 times

 **jaswantn** 1 year ago

Using the method of crossing out the option that does not fit....

Option A: address to all users of organization (wrong)

Option B: go to a few administration who can respond to alerts (question says to send notification to administrators not a selected few)

Option C: send to one administrator and giving him responsibility (wrong)

Option D: correct (as this is the one option left after checking all others).

upvoted 1 times

 **Zerotn3** 1 year, 2 months ago

Selected Answer: D

Option B does not meet the requirements because it would require configuring all AWS account root user email addresses as distribution lists, which is not necessary to meet the requirements.

upvoted 2 times

 **mp165** 1 year, 2 months ago

Unless I am reading this wrong from AWS, it seems D is proper as it says to use a single account and then set to forward to other emails.

Use an email address that forwards received messages directly to a list of senior business managers. In the event that AWS needs to contact the owner of the account, for example, to confirm access, the email is distributed to multiple parties. This approach helps to reduce the risk of delays in responding, even if individuals are on vacation, out sick, or leave the business.

upvoted 2 times

 **Burugduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: D

To meet the requirements of ensuring that all future notifications are not missed and are limited to account administrators, the company should take the following action:

Option D. Configure all existing AWS accounts and all newly created accounts to use the same root user email address. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

By configuring all AWS accounts to use the same root user email address and setting up AWS account alternate contacts, the company can ensure that all notifications are sent to a single email address that is monitored by one or more administrators. This will allow the company to ensure that all notifications are received and responded to promptly, without the risk of notifications being missed.

upvoted 3 times

 **bullrem** 1 year, 2 months ago

Option D would not meet the requirement of limiting the notifications to account administrators. Instead, it is better to use option B, which is to configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. This way, the company can ensure that the notifications are received by the appropriate people and that they are not missed. Additionally, AWS account alternate contacts can be configured in the AWS Organizations console or programmatically, which allows the company to have more granular control over who receives the notifications.

upvoted 5 times

 **techhb** 1 year, 3 months ago

B makes more sense

upvoted 1 times

Question #138

Topic 1

A company runs its ecommerce application on AWS. Every new order is published as a message in a RabbitMQ queue that runs on an Amazon EC2 instance in a single Availability Zone. These messages are processed by a different application that runs on a separate EC2 instance. This application stores the details in a PostgreSQL database on another EC2 instance. All the EC2 instances are in the same Availability Zone. The company needs to redesign its architecture to provide the highest availability with the least operational overhead. What should a solutions architect do to meet these requirements?

- A. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Create another Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.
- B. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
- C. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
- D. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Create a third Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database

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

 **123jh10**  1 year, 5 months ago

Selected Answer: B

Migrating to Amazon MQ reduces the overhead on the queue management. C and D are dismissed. Deciding between A and B means deciding to go for an AutoScaling group for EC2 or an RDS for Postgress (both multi- AZ). The RDS option has less operational impact, as provide as a service the tools and software required. Consider for instance, the effort to add an additional node like a read replica, to the DB.
<https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/active-standby-broker-deployment.html>
<https://aws.amazon.com/rds/postgresql/>
 upvoted 26 times

 **EKA_CloudGod** 1 year, 3 months ago

This also helps anyone in doubt; <https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/active-standby-broker-deployment.html>
 upvoted 1 times

 **UWSFish** 1 year, 5 months ago

Yes but active/standby is fault tolerance, not HA. I would concede after thinking about it that B is probably the answer that will be marked correct but its not a great question.
 upvoted 3 times

 **Buruguduystunstugudunstuy**  1 year, 2 months ago

Selected Answer: B

To meet the requirements of providing the highest availability with the least operational overhead, the solutions architect should take the following actions:

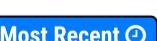
* By migrating the queue to Amazon MQ, the architect can take advantage of the built-in high availability and failover capabilities of the service, which will help ensure that messages are delivered reliably and without interruption.

* By creating a Multi-AZ Auto Scaling group for the EC2 instances that host the application, the architect can ensure that the application is highly available and able to handle increased traffic without the need for manual intervention.

* By migrating the database to a Multi-AZ deployment of Amazon RDS for PostgreSQL, the architect can take advantage of the built-in high availability and failover capabilities of the service, which will help ensure that the database is always available and able to handle increased traffic.

Therefore, the correct answer is Option B.

upvoted 5 times

 **awsgeek75**  2 months, 1 week ago

Selected Answer: B

CD, you cannot have EC2 scaling work with RabbitMQ as only one instance can be active

A: Is good but B is better

B: Correct due to usage of RDS for PG so less overhead

upvoted 1 times

 **chandu7024** 6 months ago

Agree with B
upvoted 1 times

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

Selected Answer: B

B offers high availability and low operational overheads.
upvoted 1 times

✉️ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

Option B is the best solution to meet the high availability and low overhead requirements:

Migrate the queue to redundant Amazon MQ
Use Auto Scaling groups across AZs for the application
Migrate the database to Multi-AZ RDS PostgreSQL
The reasons are:

Amazon MQ provides a managed, highly available RabbitMQ cluster
Multi-AZ Auto Scaling distributes the application across AZs

RDS PostgreSQL is managed, multi-AZ capable database
Together this architecture removes single points of failure
RDS and MQ reduce operational overhead over self-managed

upvoted 4 times

✉️ **MNotABot** 8 months, 2 weeks ago

B
least operational overhead (Amazon RDS for PostgreSQL --> hence AD out / C says EC2 so out --> Hence B)
upvoted 1 times

✉️ **cookieMr** 9 months ago

Selected Answer: B

Option B provides the highest availability with the least operational overhead. By migrating the queue to a redundant pair of RabbitMQ instances on Amazon MQ, the messaging system becomes highly available. Creating a Multi-AZ Auto Scaling group for EC2 instances hosting the application ensures that it can automatically scale and maintain availability across multiple Availability Zones. Migrating the database to a Multi-AZ deployment of Amazon RDS for PostgreSQL provides automatic failover and data replication across multiple Availability Zones, enhancing availability and reducing operational overhead.

- A. Incorrect because it does not address the high availability requirement for the RabbitMQ queue and the PostgreSQL database.
 - C. Incorrect because it does not provide redundancy for the RabbitMQ queue and does not address the high availability requirement for the PostgreSQL database.
 - D. Incorrect because it does not address the high availability requirement for the RabbitMQ queue and does not provide redundancy for the application instances.
- upvoted 2 times

✉️ **Gary_Phillips_2007** 1 year ago

Selected Answer: B

B for me.
upvoted 1 times

✉️ **techhb** 1 year, 3 months ago

Selected Answer: B

B is right all explanations below are correct
upvoted 1 times

✉️ **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B is right answer
upvoted 1 times

✉️ **Wpcorgan** 1 year, 4 months ago

B for me
upvoted 1 times

Question #139

Topic 1

A reporting team receives files each day in an Amazon S3 bucket. The reporting team manually reviews and copies the files from this initial S3 bucket to an analysis S3 bucket each day at the same time to use with Amazon QuickSight. Additional teams are starting to send more files in larger sizes to the initial S3 bucket.

The reporting team wants to move the files automatically to an analysis S3 bucket as the files enter the initial S3 bucket. The reporting team also wants to use AWS Lambda functions to run pattern-matching code on the copied data. In addition, the reporting team wants to send the data files to a pipeline in Amazon SageMaker Pipelines.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

- A. Create a Lambda function to copy the files to the analysis S3 bucket. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.
- B. Create a Lambda function to copy the files to the analysis S3 bucket. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.
- C. Configure S3 replication between the S3 buckets. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.
- D. Configure S3 replication between the S3 buckets. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.

Correct Answer: A*Community vote distribution*

Six_Fingered_Jose Highly Voted 1 year, 5 months ago

Selected Answer: D

i go for D here
A and B says you are copying the file to another bucket using lambda,
C and D just uses S3 replication to copy the files,

They are doing exactly the same thing while C and D do not require setting up of lambda, which should be more efficient

The question says the team is manually copying the files, automatically replicating the files should be the most efficient method vs manually copying or copying with lambda.

upvoted 25 times

vipyodha 9 months, 1 week ago

yes d because of least operational overhead and also s3 event notification can only send to sns.sqs.and lambda , not to sagemaker.eventbridge can send to sagemaker

upvoted 11 times

Abdou1604 5 months, 3 weeks ago

but the reporting team also wants to use AWS Lambda functions to run pattern-matching code on the copied , S3 replication cons is copying everything

upvoted 2 times

pentium75 3 months ago

The Lambda functions should run "on the copied data", so first copy, THEN run Lambda function, which is achieved by D.

upvoted 2 times

123jh10 Highly Voted 1 year, 5 months ago

Selected Answer: B

C and D aren't answers as replicating the S3 bucket isn't efficient, as other teams are starting to use it to store larger docs not related to the reporting, making replication not useful.

As Amazon SageMaker Pipelines, ... is now supported as a target for routing events in Amazon EventBridge, means the answer is B
<https://aws.amazon.com/about-aws/whats-new/2021/04/new-options-trigger-amazon-sagemaker-pipeline-executions/>

upvoted 18 times

JayBee65 1 year, 3 months ago

I think you are mis-interpreting the question. I think you need to use all files, including the ones provided by other teams, otherwise how can you tell what files to copy? I think the point of this statement is to show that more files are in use, and being copied at different times, rather than suggesting you need to differentiate between the two sources of files.

upvoted 7 times

 **KADSM** 1 year, 4 months ago

Not sure how far lambda will cope up with larger files with the timelimit in place.
upvoted 4 times

 **byteb** 3 months, 1 week ago

"The reporting team wants to move the files automatically to analysis S3 bucket as the files enter the initial S3 bucket." Replication is asynchronous, with lambda the data will be available faster. So I think A is the answer.
upvoted 1 times

 **vipyodha** 9 months, 1 week ago

but B is not least operational overhead , D is least operational overhead
upvoted 2 times

 **jdr75** 11 months, 3 weeks ago

You misinterpret it ... the reporting team is overload, cos' more teams request their services uploading more data to the bucket. That's the reason reporting team need to automate the process. So ALL the bucket objects need to be copied to other bucket, and the replication is better than use Lambda. So the answer is D.
upvoted 3 times

 **andyngkh86** Most Recent 2 months ago

I go for C, because option C no need to configure event notifications, but D need to extra work to configure the event notification, for the least operation, option C is best choice
upvoted 1 times

 **Marco_St** 4 months ago

Selected Answer: D

B is the first option I denied. Since it makes the event happens inside the analysis bucket to trigger the lambda function. so if the lambda function is running code to copy files from initial bucket to analysis bucket. Then this lambda function should be triggered by the event in initial bucket like once the data reaches in the initial bucket then lambda is triggered. D is the answer.
upvoted 1 times

 **AntonioMinolfi** 5 months, 2 weeks ago

Selected Answer: D

Utilizing a lambda function would introduce additional operational overhead, eliminating options A and B. S3 replication offers a simpler setup and efficiently accomplishes the task. S3 notifications cannot use SageMaker as a destination; the permissible destinations include SQS, SNS, Lambda, and Eventbridge, so C is out.
upvoted 8 times

 **vijaykamal** 6 months ago

Selected Answer: D

Create lambda for replication is overhead. This dismisses A and B
S3 event notification cannot be directed to Sagemaker directly. This dismisses C
Correct Answer: D
upvoted 1 times

 **TariqKipkemei** 6 months, 3 weeks ago

Selected Answer: D

D provide the least operational overhead
upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

Option D is the solution with the least operational overhead:

Use S3 replication between buckets
Send S3 events to EventBridge
Add Lambda and SageMaker as EventBridge rule targets
The reasons this has the least overhead:
upvoted 3 times

 **MutiverseAgent** 8 months, 1 week ago

Selected Answer: D

Correct: D
B & D the only possible as Sagemaker is not supported as target for S3 events. Using bucket replication as D mention is more efficient than using a lambda as B mention.
upvoted 2 times

 **cookieMr** 9 months ago

Selected Answer: D

Option D is correct because it combines S3 replication, event notifications, and Amazon EventBridge to automate the copying of files from the initial S3 bucket to the analysis S3 bucket. It also allows for the execution of Lambda functions and integration with SageMaker Pipelines.

Option A is incorrect because it suggests manually copying the files using a Lambda function and event notifications, but it does not utilize S3 replication or EventBridge for automation.

Option B is incorrect because it suggests using S3 event notifications directly with EventBridge, but it does not involve S3 replication or utilize Lambda for copying the files.

Option C is incorrect because it only involves S3 replication and event notifications without utilizing EventBridge or Lambda functions for further processing.

upvoted 2 times

 **studynoplay** 10 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html#supported-notification-destinations>

S3 can NOT send event notification to SageMaker. This rules out C. you have to send to • Amazon EventBridge 1st then to SageMaker
upvoted 6 times

 **eendee** 11 months, 2 weeks ago

Selected Answer: D

Why I believe it is not C? The key here is in the s3:ObjectCreated:"Put". The replication will not fire the s3:ObjectCreated:Put. event. See link here:
<https://aws.amazon.com/blogs/aws/s3-event-notification/>

upvoted 5 times

 **kraken21** 12 months ago

Selected Answer: D

D takes care of automated moving and lambda for pattern matching are covered efficiently in D.

upvoted 1 times

 **SuketuKohli** 1 year ago

only one destination type can be specified for each event notification in S3 event notifications

upvoted 1 times

 **gmehra** 1 year ago

Selected Answer: A

Answer is A

The statement says move the file. Replication won't move the file it will just create a copy. so Obviously C and D are out. When you Event notification and Lambda why we need Event bridge as more service. So answer is A

upvoted 2 times

 **Kaireny54** 11 months, 4 weeks ago

A and B says : create a lambda function to COPY also. Then, following your idea, A and B are out too... ;)
obviously move argument isn't accurate in this question

upvoted 1 times

 **markw92** 9 months, 1 week ago

I searched S3 documentation and couldn't find where s3 event notification can trigger sagemaker pipelines. It can SNS,SQS and lambda. I am not sure A is the right choice.

upvoted 1 times

 **Steve_4542636** 1 year ago

Selected Answer: B

Using lambda is one of the requirements. Sns, sqs, lambda, and event bridge are the only s3 notification destinations
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html>.

upvoted 1 times

 **bullrem** 1 year, 2 months ago

both A and D options can meet the requirements with the least operational overhead as they both use automatic event-driven mechanisms (S3 event notifications and EventBridge rules) to trigger the Lambda function and copy the files to the analysis S3 bucket. The Lambda function can then run the pattern-matching code, and the files can be sent to the SageMaker pipeline.

Option A, directly copying the files to the analysis S3 bucket using a Lambda function, is more straight forward, option D using S3 replication and EventBridge rules is more flexible and can be more powerful as it allows you to use more complex event-driven flows.

upvoted 2 times

Question #140

Topic 1

A solutions architect needs to help a company optimize the cost of running an application on AWS. The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture.

The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year.

Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two.)

- A. Use Spot Instances for the data ingestion layer
- B. Use On-Demand Instances for the data ingestion layer
- C. Purchase a 1-year Compute Savings Plan for the front end and API layer.
- D. Purchase 1-year All Upfront Reserved instances for the data ingestion layer.
- E. Purchase a 1-year EC2 instance Savings Plan for the front end and API layer.

Correct Answer: AC

Community vote distribution

AC (100%)

SimonPark Highly Voted 1 year, 4 months ago

Selected Answer: AC

EC2 instance Savings Plan saves 72% while Compute Savings Plans saves 66%. But according to link, it says "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 and Lambda usage." EC2 instance Savings Plans are not applied to Fargate or Lambda upvoted 18 times

aba2s Highly Voted 1 year, 2 months ago

Selected Answer: AC

Compute Savings Plans can be used for EC2 instances and Fargate. Whereas EC2 Savings Plans support EC2 only.
upvoted 8 times

TariqKipkemei Most Recent 6 months, 3 weeks ago

Selected Answer: AC

Compute Savings Plans can also apply to Fargate and Lambda Usage.
upvoted 2 times

AKBM7829 7 months ago

BC is the answer
data ingestion = Spot Instance but
Keyword "Usage Unpredictable" : On-Demand

and for API its Compute Savings Plan

upvoted 1 times

awashenko 5 months, 2 weeks ago

Spot instances can auto scale so Spot instance is correct.

upvoted 1 times

Guru4Cloud 7 months, 1 week ago

Selected Answer: AC

The two most cost-effective purchasing options for this architecture are:

- A) Use Spot Instances for the data ingestion layer
- C) Purchase a 1-year Compute Savings Plan for the front end and API layer

The reasons are:

Spot Instances provide the greatest savings for flexible, interruptible EC2 workloads like data ingestion.
Savings Plans offer significant discounts for predictable usage like the front end and API layer.

All Upfront and partial/no Upfront RI's don't align well with the sporadic EC2 usage.

On-Demand is more expensive than Spot for flexible EC2 workloads.

By matching purchasing options to the workload patterns, Spot for unpredictable EC2 and Savings Plans for steady-state usage, the solutions architect optimizes cost efficiency.

upvoted 2 times

 **cookieMr** 9 months ago

Selected Answer: AC

Using Spot Instances for the data ingestion layer will provide the most cost-effective option for sporadic and unpredictable workloads, as Spot Instances offer significant cost savings compared to On-Demand Instances (Option A).

Purchasing a 1-year Compute Savings Plan for the front end and API layer will provide cost savings for predictable utilization over the course of a year (Option C).

Option B is less cost-effective as it suggests using On-Demand Instances for the data ingestion layer, which does not take advantage of cost-saving opportunities.

Option D suggests purchasing 1-year All Upfront Reserved instances for the data ingestion layer, which may not be optimal for sporadic and unpredictable workloads.

Option E suggests purchasing a 1-year EC2 instance Savings Plan for the front end and API layer, but Compute Savings Plans are typically more suitable for predictable workloads.

upvoted 3 times

 **Abrar2022** 9 months, 4 weeks ago

Spot instances for data injection because the task can be terminated at anytime and tolerate disruption. Compute Saving Plan is cheaper than EC2 instance Savings plan.

upvoted 1 times

 **Abrar2022** 10 months ago

EC2 instance Savings Plans are not applied to Fargate or Lambda

upvoted 1 times

 **Noviiice** 1 year ago

Why not B?

upvoted 1 times

 **SkyZeroZx** 11 months, 4 weeks ago

because onDemand is more expensive than spot additionally that the workload has no problem with being interrupted at any time

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: AC

To optimize the cost of running this application on AWS, you should consider the following options:

- A. Use Spot Instances for the data ingestion layer
- C. Purchase a 1-year Compute Savings Plan for the front-end and API layer

Therefore, the most cost-effective solution for hosting this application would be to use Spot Instances for the data ingestion layer and to purchase either a 1-year Compute Savings Plan or a 1-year EC2 instance Savings Plan for the front-end and API layer.

upvoted 2 times

 **AKBM7829** 7 months ago

Yes, but in the question it also states that it is 'Unpredictable' So, On-Demand is suitable over Spot Instance right which makes BC as the answer

upvoted 1 times

 **awashenko** 5 months, 2 weeks ago

Spot instances can auto scale so Spot is still correct.

upvoted 1 times

 **techhb** 1 year, 3 months ago

Selected Answer: AC

Too obvious answer.

upvoted 1 times

 **berks** 1 year, 3 months ago

Selected Answer: AC

AC

can be interrupted at any time => spot

upvoted 2 times

 **TECHNOWARRIOR** 1 year, 3 months ago

A,E::

Savings Plan — EC2

Savings Plan offers almost the same savings from a cost as RIs and adds additional Automation around how the savings are being applied. One way to understand is to say that EC2 Savings Plan are Standard Reserved Instances with automatic switching depending on Instance types being used within the same instance family and additionally applied to ECS Fargate and Lambda.

Savings Plan — Compute

Savings Plan offers almost the same savings from a cost as RIs and adds additional Automation around how the savings are being applied. For example, they provide flexibility around instance types and regions so that you don't have to monitor new instance types that are being launched.

It is also applied to Lambda and ECS Fargate workloads. One way to understand is to say that Compute Savings Plan are Convertible Reserved Instances with automatic switching depending on Instance types being used.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: AC

A and C

upvoted 1 times

 **rjam** 1 year, 4 months ago

its A and C . <https://www.densify.com/finops/aws-savings-plan>

upvoted 1 times

 **bunnychip** 1 year, 5 months ago

Selected Answer: AC

api is not EC2.need to use compute savings plan

upvoted 4 times

 **Chunsl1** 1 year, 5 months ago

E makes more sense than C. See <https://aws.amazon.com/savingsplans/faq/>, EC2 instance Savings Plan (up to 72% saving) costs less than Compute Savings Plan (up to 66% saving)

upvoted 4 times

 **capepenguin** 1 year, 5 months ago

Isn't the EC2 Instance Savings Plan not applicable to Fargate and Lambda?

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 6 times

 **Yadav_Sanjay** 10 months, 3 weeks ago

I Agree

upvoted 1 times

Question #141

Topic 1

A company runs a web-based portal that provides users with global breaking news, local alerts, and weather updates. The portal delivers each user a personalized view by using mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible.

How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

- A. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.
- B. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.
- C. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve the static content. Serve the dynamic content directly from the ALB.
- D. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.

Correct Answer: B*Community vote distribution*

A (70%)

B (27%)

 **huiy**  1 year, 5 months ago

Selected Answer: A

Answer is A.

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content

<https://www.examtopics.com/discussions/amazon/view/81081-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 28 times

 **MutiverseAgent** 8 months, 1 week ago

Also, option B does not use CloudFront which means all the traffic will go through the internet; So, despite deploying resources in two regions and using the lowest latency point, that public internet connection might probably be slower than a connection through a private aws network as Cloudfront can use.

upvoted 2 times

 **Six_Fingered_Jose**  1 year, 5 months ago

Selected Answer: B

Answer should be B,

CloudFront reduces latency if its only static content, which is not the case here.

For Dynamic content, CF cant cache the content so it sends the traffic through the AWS Network which does reduces latency, but it still has to travel through another region.

For the case with 2 region and Route 53 latency routing, Route 53 detects the nearest resource (with lowest latency) and routes the traffic there. Because the traffic does not have to travel to resources far away, it should have the least latency in this case here.

upvoted 12 times

 **Aamee** 1 year, 3 months ago

Can you pls. provide a ref. link from where this info. got extracted?

upvoted 1 times

 **manueleng2007** 8 months ago

this is link <https://aws.amazon.com/es/blogs/aws-spanish/cloudfront-para-la-distribucion-de-contenido-estatico-y-dinamico/>
upvoted 2 times

 **Abdou1604** 5 months, 3 weeks ago

What about across the world :)

upvoted 4 times

 **Onimole** 1 year, 4 months ago

Cf works for both static and dynamic content

upvoted 9 times

 **awsgeek75** 2 months, 1 week ago

two regions won't cover the whole world.

upvoted 1 times

 Uzbekistan Most Recent 2 days, 9 hours ago

Selected Answer: C

CloudFront for Static Content: By leveraging Amazon CloudFront, static content such as images, stylesheets, and scripts can be cached and distributed globally across a network of edge locations. This ensures that users receive static content from the nearest edge location, reducing latency and improving performance.

Serve Dynamic Content from ALB: Since dynamic content requires real-time processing and cannot be effectively cached at edge locations, serving dynamic content directly from the Application Load Balancer (ALB) is appropriate. The ALB can handle dynamic requests efficiently within the AWS Region where the application is deployed.

upvoted 1 times

 Parul25 1 month, 3 weeks ago

CloudFront improves the performance, availability, and security of your dynamic content but not the latency as compared to Route 53 Latency Routing policy. Hence option B

<https://aws.amazon.com/cloudfront/dynamic-content/>

upvoted 1 times

 Parul25 1 month, 3 weeks ago

I choose option B.

While CloudFront can accelerate content delivery by caching static content at edge locations, it may not be the most effective solution in this scenario. Since the portal delivers a mixture of static and dynamic content, leveraging Route 53 latency routing for dynamic content delivery ensures that users are directed to the nearest AWS Region hosting the dynamic content.

upvoted 1 times

 pentium75 3 months ago

Selected Answer: A

"Least amount of latency for all users" "across the world" = CloudFront, thus B and D are out. Also, deploying the stack in "two regions" would benefit those two regions, but not users "across the world".

CloudFront can also cache dynamic content, thus A.

upvoted 6 times

 Bennysieg 3 months, 3 weeks ago

Selected Answer: A

Answer is option A:

Earth Networks uses a CDN so that they can provide dynamic and personalized web based content quickly to their users with very low latency and high performing response times. Specifically, they need to be able to provide local information to the end user, in near real time, and need a CDN that allows them to adjust things like time to live, query strings, and cookie information so that they can pass all that information back to the origin to pull just what the user needs.

upvoted 1 times

 AZ_Master 4 months, 1 week ago

Selected Answer: B

Those are personalized content - where CloudFront could not help much.

upvoted 2 times

 David_Ang 5 months, 1 week ago

Selected Answer: A

"A" because cloud front is more efficient

upvoted 1 times

 Wayne23Fang 5 months, 2 weeks ago

Selected Answer: B

A or B very close. But the (B) camp arguments earlier made me lean to B: Cloudfront doesn't help much for dynamic content, which is probably the bottleneck; On average, two dynamic server could cut response half.

upvoted 2 times

 BrijMohan08 6 months, 1 week ago

Selected Answer: D

Option D is the most suitable choice for minimizing latency for all users. It leverages the use of multiple AWS regions, geolocation routing, and the ALB to ensure that users are directed to the closest region, reducing latency for both static and dynamic content. This approach provides a high level of availability and performance for global users.

upvoted 2 times

 TariqKipkemei 6 months, 2 weeks ago

Selected Answer: A

CloudFront to the rescue....whoosh

upvoted 2 times

 Guru4Cloud 7 months, 1 week ago

Selected Answer: A

The solution that will ensure the LEAST amount of latency for all users is:

A. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.

Here's why:

Option A (Single AWS Region, Amazon CloudFront for both static and dynamic content):

Deploying the application stack in a single AWS Region helps reduce complexity and potential data synchronization issues that might arise from using multiple regions

upvoted 2 times

 **MM_Korvinus** 7 months, 3 weeks ago

Selected Answer: B

I think CloudFront does not improve latency in this case, because CF works as kind of cache of data. Cache works fine in case of static data, but here each user can have its own dynamically created data, this every user will need to go to origin. So in this case CF can make the latency worse. On the other hand route53 with latency routing to ALB in different regions may actually increase the average user latency.

upvoted 1 times

 **MutiverseAgent** 8 months, 1 week ago

Selected Answer: A

It's A, according this page (<https://aws.amazon.com/cloudfront/dynamic-content/>) CloudFront is commonly used for "News, sports, local, weather" as this is content mostly bounded to a region.

upvoted 4 times

 **MutiverseAgent** 8 months, 1 week ago

Also, option B does not use CloudFront which means all the traffic will go through the internet; So, despite deploying resources in two regions and using the lowest latency point, that public internet connection might probably be slower than a connection through a private aws network as Cloudfront can use.

upvoted 1 times

 **ayeah** 9 months ago

Selected Answer: A

CloudFront is a CDN that is well adapted for dynamic content.

News, sports, local, weather

Web applications of this type often have a geographic focus with customized content for end users. Content can be cached at edge locations for varying lengths of time depending on type of content. For example, hourly updates can be cached for up to an hour, while urgent alerts may only be cached for a few seconds so end users always have the most up to date information available to them. A content delivery network is a great platform for serving common types of experiences for news and weather such as articles, dynamic map tiles, overlays, forecasts, breaking news or alert tickers, and video.

<https://aws.amazon.com/cloudfront/dynamic-content/>

upvoted 1 times

 **smartegnine** 9 months, 4 weeks ago

I would definitely go to C

If you are serving dynamic content such as web applications or APIs directly from an Amazon Elastic Load Balancer (ELB) or Amazon EC2 instances to end users on the internet, you can improve the performance, availability, and security of your content by using Amazon CloudFront as your content delivery network.

<https://aws.amazon.com/cloudfront/dynamic-content/>

upvoted 1 times

Question #142

Topic 1

A gaming company is designing a highly available architecture. The application runs on a modified Linux kernel and supports only UDP-based traffic. The company needs the front-end tier to provide the best possible user experience. That tier must have low latency, route traffic to the nearest edge location, and provide static IP addresses for entry into the application endpoints.

What should a solutions architect do to meet these requirements?

- A. Configure Amazon Route 53 to forward requests to an Application Load Balancer. Use AWS Lambda for the application in AWS Application Auto Scaling.
- B. Configure Amazon CloudFront to forward requests to a Network Load Balancer. Use AWS Lambda for the application in an AWS Application Auto Scaling group.
- C. Configure AWS Global Accelerator to forward requests to a Network Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.
- D. Configure Amazon API Gateway to forward requests to an Application Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

Correct Answer: C

Community vote distribution

C (100%)

✉️  **dokaedu**  1 year, 4 months ago

Correct Answer: C

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 70 times

✉️  **praveenas400** 1 year, 2 months ago

Explained very well. ty

upvoted 2 times

✉️  **iCcma** 1 year, 4 months ago

Thank you, your explanation helped me to better understand even the answer of question 29

upvoted 4 times

✉️  **stepman** 1 year, 3 months ago

On top of this, lambda would not be able to run application that is running on a modified Linux kernel. The answer is C .

upvoted 6 times

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

Selected Answer: C

The correct answer is Option C. To meet the requirements;

* AWS Global Accelerator is a service that routes traffic to the nearest edge location, providing low latency and static IP addresses for the front-end tier. It supports UDP-based traffic, which is required by the application.

* A Network Load Balancer is a layer 4 load balancer that can handle UDP traffic and provide static IP addresses for the application endpoints.

* An EC2 Auto Scaling group ensures that the required number of Amazon EC2 instances is available to meet the demand of the application. This will help the front-end tier to provide the best possible user experience.

Option A is not a valid solution because Amazon Route 53 does not support UDP traffic.

Option B is not a valid solution because Amazon CloudFront does not support UDP traffic.

Option D is not a valid solution because Amazon API Gateway does not support UDP traffic.

upvoted 6 times

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

My mistake, correction on Option A, it is the Application Load Balancers do not support UDP traffic. They are designed to load balance HTTP and HTTPS traffic, and they do not support other protocols such as UDP.

upvoted 4 times

✉️  **sidharthwader**  3 weeks, 1 day ago

If the situation demands for UDP or some protocols that are not at application level then it would be better to use Global Accelerator and here they need top notch performance hence using it with NLB would be the best answer. Cloud Front does not support UDP nor does it support use of NLB upvoted 1 times

Murtadhaceit 3 months, 3 weeks ago

Selected Answer: C

UDP: NLB.
Static IP: Global Accelerator.
upvoted 1 times

TariqKipkemei 6 months, 2 weeks ago

Selected Answer: C

UDP, static IP = Global Accelerator and Network Load Balancer
upvoted 1 times

Guru4Cloud 7 months, 1 week ago

Selected Answer: C

AWS Global Accelerator provides static IP addresses that serve as a fixed entry point to application endpoints. This allows optimal routing to the nearest edge location.

Using a Network Load Balancer (NLB) allows support for UDP traffic, as NLBs can handle TCP and UDP protocols. The application runs on a modified Linux kernel, so using Amazon EC2 instances directly will provide the needed customization and low latency. The EC2 instances can be auto scaled based on demand to provide high availability. API Gateway and Application Load Balancer are more suited for HTTP/HTTPS and REST API type workloads. For a UDP gaming workload, Global Accelerator + NLB + EC2 is a better architectural fit.

upvoted 1 times

cookieMr 9 months ago

Selected Answer: C

AWS Global Accelerator is designed to improve the availability and performance of applications by routing traffic through the AWS global network to the nearest edge locations, reducing latency. By configuring AWS Global Accelerator to forward requests to a Network Load Balancer, UDP-based traffic can be efficiently distributed across multiple EC2 instances in an Auto Scaling group. Using Amazon EC2 instances for the application allows for customization of the Linux kernel and support for UDP-based traffic. This solution provides static IP addresses for entry into the application endpoints, ensuring consistent access for users.

Option A suggests using AWS Lambda for the application, but Lambda is not suitable for long-running UDP-based applications and may not provide the required low latency.

Option B suggests using CloudFront, which is primarily designed for HTTP/HTTPS traffic and does not have native support for UDP-based traffic. Option D suggests using API Gateway, which is primarily used for RESTful APIs and does not support UDP-based traffic.

upvoted 2 times

Abrar2022 9 months, 4 weeks ago

aws global accelerator provides static IP addresses.
upvoted 1 times

Bmarodi 10 months, 1 week ago

Selected Answer: C

My choice is option C, due to the followings: Amazon Global Accelerator routes traffic to nearest edge locations, it supports UDP-based traffic, and it provides static IP addresses as well, hence C is right answer.

upvoted 1 times

bakamon 11 months, 4 weeks ago

Answer : C
CloudFront : Doesn't support static IP addresses
ALB : Doesn't support UDP
upvoted 1 times

Devsin2000 1 year ago

C - <https://aws.amazon.com/global-accelerator/>
upvoted 1 times

SilentMilli 1 year, 2 months ago

Selected Answer: C

To meet the requirements of providing low latency, routing traffic to the nearest edge location, and providing static IP addresses for entry into the application endpoints, the best solution would be to use AWS Global Accelerator. This service routes traffic to the nearest edge location and provides static IP addresses for the application endpoints. The front-end tier should be configured with a Network Load Balancer, which can handle UDP-based traffic and provide high availability. Option C, "Configure AWS Global Accelerator to forward requests to a Network Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group," is the correct answer.

upvoted 1 times

techhb 1 year, 3 months ago

Selected Answer: C

C is obvious choice here.
upvoted 1 times

career360guru 1 year, 3 months ago

Selected Answer: C

C as Global Accelerator is the best choice for UDP based traffic needing static IP address.
upvoted 1 times

 **Certified101** 1 year, 3 months ago

Selected Answer: C

c correct
upvoted 1 times

 **Qjb8m9h** 1 year, 3 months ago

CloudFront is designed to handle HTTP protocol meanwhile Global Accelerator is best used for both HTTP and non-HTTP protocols such as TCP and UDP. HENCE C is the ANSWER!

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

C is correct
upvoted 1 times

Question #143

Topic 1

A company wants to migrate its existing on-premises monolithic application to AWS. The company wants to keep as much of the front-end code and the backend code as possible. However, the company wants to break the application into smaller applications. A different team will manage each application. The company needs a highly scalable solution that minimizes operational overhead.

Which solution will meet these requirements?

- A. Host the application on AWS Lambda. Integrate the application with Amazon API Gateway.
- B. Host the application with AWS Amplify. Connect the application to an Amazon API Gateway API that is integrated with AWS Lambda.
- C. Host the application on Amazon EC2 instances. Set up an Application Load Balancer with EC2 instances in an Auto Scaling group as targets.
- D. Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target.

Correct Answer: D

Community vote distribution



Ken701 Highly Voted 1 year, 4 months ago

I think the answer here is "D" because usually when you see terms like "monolithic" the answer will likely refer to microservices.
upvoted 34 times

Bevemo Highly Voted 1 year, 4 months ago

Selected Answer: D

D is organic pattern, lift and shift, decompose to containers, first making most use of existing code, whilst new features can be added over time with lambda+api gw later.
A is leapfrog pattern. requiring refactoring all code up front.
upvoted 17 times

jbkrishna Most Recent 1 week ago

Different teams working means " microservices based architecture" so basically decoupling the application ..u can achieve this only by containerizing the app so answer is D
upvoted 1 times

NayeraB 1 month, 1 week ago

Selected Answer: B

B allows for a serverless architecture using AWS Lambda functions, which are highly scalable and require minimal operational overhead. AWS Amplify can help in managing the front-end code, while Amazon API Gateway integrated with AWS Lambda can handle the backend services.

D imo is not the best option in this scenario. While ECS can be a good choice for containerized workloads, it might introduce more operational overhead compared to a serverless solution like AWS Lambda and AWS Amplify.
upvoted 3 times

awsgeek75 2 months, 1 week ago

Selected Answer: D

I have a problem with this question.
"The company wants to keep as much of the front-end code and the backend code as possible"
So containerization is the solution here (D)? ABC don't make much sense so I will go with D but using containers for FE/BE code and configuring ALB for ECS (hopefully for frontend containers) is a pain in practice. Maybe this is worded in a bad way.
upvoted 3 times

vip2 2 months, 1 week ago

Selected Answer: B

Original state: monolithic with FE and BE code
Wanted state: separate to multiple components for diff. teams as Microservices

B is correct to decouple monolithic to microservices.

D still keep monolithic application in ECS.

upvoted 3 times

06042022 2 months, 3 weeks ago

IT is B. AWS amplify.
AWS Amplify will help separate FE and BE. I agree with MM_Korvinus answer.
upvoted 2 times

 **JTruong** 2 months, 3 weeks ago

Selected Answer: D

<https://aws.amazon.com/tutorials/break-monolith-app-microservices-ecs-docker-ec2/module-three/>

This page explained clearly why D is the correct answer

upvoted 1 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: D

'Non-monolithic', 'smaller applications', 'minimized operational overhead' all screaming 'microservices'.

upvoted 4 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

The reasons are:

ECS allows running Docker containers, so the existing monolithic app can be containerized and run on ECS with minimal code changes.

The app can be broken into smaller microservices by containerizing different components and managing them separately.

ECS provides auto scaling capabilities to scale each microservice independently.

Using an Application Load Balancer with ECS enables distributing traffic across containers and auto scaling.

ECS has minimal operational overhead compared to managing EC2 instances directly.

Serverless options like Lambda and API Gateway would require significant code refactoring which is not ideal for migrating an existing app.

upvoted 5 times

 **MM_Korvinus** 7 months, 3 weeks ago

Selected Answer: B

Honestly, from my experience, the minimal operational overhead is with Amplify and API Gateway with lambdas. Both services have neat release features, you do not need to fiddle around ECS configurations as everything is server-less, which is also highly scalable. Eventhough it is much harder to refactor monolithic app to this set-up it is definitely easier to operate. Not talking about complexities around ALB.

upvoted 8 times

 **Fielies23** 7 months, 2 weeks ago

I actually agree with this, they have a monolithic application that contains the Front-end and Back-end. They clearly state they want different teams managing different applications. This is telling me they want a team to manage the front-end and a team to manage the back-end. A,C and D suggest simply running copies of the monolith application (containing front and back end). So how will different teams manage different applications?? B is the only one that actually splits front and back end

upvoted 1 times

 **pentium75** 3 months ago

How do you want to run a "monolithic application" in Lambda?

upvoted 2 times

 **cookieMr** 9 months ago

Selected Answer: D

ECS provides a highly scalable and managed environment for running containerized applications, reducing operational overhead. By setting up an ALB with ECS as the target, traffic can be distributed across multiple instances of the application for scalability and availability. This solution enables different teams to manage each application independently, promoting team autonomy and efficient development.

A is more suitable for event-driven and serverless workloads. It may not be the ideal choice for migrating a monolithic application and maintaining the existing codebase.

B integrates with Lambda and API Gateway, it may not provide the required flexibility for breaking the application into smaller applications and managing them independently.

C would involve managing the infrastructure and scaling manually. It may result in higher operational overhead compared to using a container service like ECS.

upvoted 2 times

 **antropaws** 9 months, 4 weeks ago

Selected Answer: D

I was confused about this, but actually Amazon ECS service can be configured to use Elastic Load Balancing to distribute traffic evenly across the tasks in your service.

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/create-application-load-balancer.html>

upvoted 1 times

 **studynoplay** 10 months, 2 weeks ago

Selected Answer: D

monolithic = microservices = ECS

upvoted 4 times

 **C_M_M** 11 months, 1 week ago

I thought ALB is about distributing load. How do we want to use it to connect decoupled applications that needs to call themselves. I am kind of confused why most people are going with D.

I think I will go with A.

upvoted 2 times

✉️  **Devsin2000** 1 year ago

I think the answer is A
B is wrong because the requirement is not for the backend. C and D are not suitable because the ALB is not best suited for middle tier applications.
upvoted 2 times

✉️  **pentium75** 3 months ago

"Monolithic application" does not sound like Lambda.
upvoted 1 times

✉️  **aws4myself** 1 year, 2 months ago

I will go with A because - less operational and High availability (Lambda has these)

If it is ECS, operational overhead and can only be scaled up to an EC2 assigned under it.

upvoted 2 times

✉️  **pentium75** 3 months ago

ECS with Fargate. I don't think a "monolithic application" can run on Lambda.
upvoted 1 times

Question #144

Topic 1

A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPUUtilization metrics are spiking when monthly reports run.

What is the MOST cost-effective solution?

- A. Migrate the monthly reporting to Amazon Redshift.
- B. Migrate the monthly reporting to an Aurora Replica.
- C. Migrate the Aurora database to a larger instance class.
- D. Increase the Provisioned IOPS on the Aurora instance.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

Option B: Migrating the monthly reporting to an Aurora Replica may be the most cost-effective solution because it involves creating a read-only copy of the database that can be used specifically for running large reports without impacting the performance of the primary database. This solution allows the company to scale the read capacity of the database without incurring additional hardware or I/O costs.

upvoted 12 times

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

The incorrect solutions are:

Option A: Migrating the monthly reporting to Amazon Redshift may not be cost-effective because it involves creating a new data store and potentially significant data migration and ETL costs.

Option C: Migrating the Aurora database to a larger instance class may not be cost-effective because it involves changing the underlying hardware of the database and potentially incurring additional costs for the larger instance.

Option D: Increasing the Provisioned IOPS on the Aurora instance may not be cost-effective because it involves paying for additional I/O capacity that may not be necessary for other workloads on the database.

upvoted 10 times

✉  **Mikado211** Highly Voted 3 months, 2 weeks ago

Selected Answer: B

Report = Aurora replica

upvoted 7 times

✉  **TariqKipkemei** Most Recent 6 months, 2 weeks ago

Selected Answer: B

Migrate the monthly reporting to an Aurora Replica

upvoted 3 times

✉  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

Aurora Replicas utilize the same storage as the primary instance so there is no additional storage cost.

Replicas can be created and destroyed easily to match reporting needs.

The primary Aurora instance size does not need to be changed, avoiding additional cost.

Workload is offloaded from the primary instance, improving its performance.

No major software/configuration changes needed compared to options like Redshift.

upvoted 3 times

✉  **cd93** 7 months, 1 week ago

I don't understand why doubling everything (instances, network cost, maintenance effort, and especially storage) can be considered "cost-saving" for a simple monthly report...

An instance upgrade can very well be much cheaper. This question is very vague and does not provide enough information.

upvoted 2 times

✉  **cd93** 7 months, 1 week ago

Silly me, I thought upgrading instance type includes storage upgrade (increase read iops) lol. The question pointed out that hard drive is also a limiting factor, so correct answer is B.

upvoted 3 times

(cookieMr) 9 months ago

Selected Answer: B

B is correct because migrating the monthly reporting to an Aurora Replica can offload the reporting workload from the primary Aurora instance, reducing the impact on its performance during large reports. Using an Aurora Replica provides scalability and allows the replica to handle the read-intensive reporting queries, improving the overall performance of the ecommerce application.

A is wrong because migrating to Amazon Redshift introduces additional costs and complexity, and it may not be necessary to switch to a separate data warehousing service for this specific issue.

C is wrong because simply increasing the instance class of the Aurora database may not be the most cost-effective solution if the performance issue can be resolved by offloading the reporting workload to an Aurora Replica.

D is wrong because increasing the Provisioned IOPS alone may not address the issue of spikes in CPUUtilization during large reports, as it primarily focuses on storage performance rather than overall database performance.

upvoted 4 times

(Abrar2022) 10 months ago

By using an Aurora Replica for running large reports, the primary database will be relieved of the additional read load, improving performance for the ecommerce application.

upvoted 1 times

(Bmarodi) 10 months, 1 week ago

Selected Answer: B

Option B is right answer.

upvoted 1 times

(studynoplay) 10 months, 2 weeks ago

Finally a question where there are no controversies

upvoted 3 times

(SilentMilli) 1 year, 2 months ago

Selected Answer: B

The most cost-effective solution for addressing high ReadIOPS and CPU utilization when running large reports would be to migrate the monthly reporting to an Aurora Replica. An Aurora Replica is a read-only copy of an Aurora database that is updated in real-time with the primary database. By using an Aurora Replica for running large reports, the primary database will be relieved of the additional read load, improving performance for the ecommerce application. Option B, "Migrate the monthly reporting to an Aurora Replica," is the correct answer.

upvoted 1 times

(career360guru) 1 year, 3 months ago

Selected Answer: B

B is the best option

upvoted 2 times

(sanket1990) 1 year, 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

(Wpcorgan) 1 year, 4 months ago

B is correct

upvoted 1 times

(backbencher2022) 1 year, 4 months ago

Selected Answer: B

ReadIOPS issue inclining towards Read Replica as the most cost effective solution here

upvoted 4 times

(rjam) 1 year, 4 months ago

Answer B

upvoted 2 times

Question #145

Topic 1

A company hosts a website analytics application on a single Amazon EC2 On-Demand Instance. The analytics software is written in PHP and uses a MySQL database. The analytics software, the web server that provides PHP, and the database server are all hosted on the EC2 instance. The application is showing signs of performance degradation during busy times and is presenting 5xx errors. The company needs to make the application scale seamlessly.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use an Application Load Balancer to distribute the load to each EC2 instance.
- B. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.
- C. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AWS Lambda function to stop the EC2 instance and change the instance type. Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization surpasses 75%.
- D. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AMI of the web application. Apply the AMI to a launch template. Create an Auto Scaling group with the launch template. Configure the launch template to use a Spot Fleet. Attach an Application Load Balancer to the Auto Scaling group.

Correct Answer: D

Community vote distribution



✉️ **Konb** Highly Voted 10 months, 3 weeks ago

Selected Answer: D

I was tempted to pick A but then I realized there are two key requirements:

- scale seamlessly
- cost-effectively

None of A-C give seamless scalability. A and B are about adding second instance (which I assume does not match to "scale seamlessly"). C is about changing instance type.

Therefore D is only workable solution to the scalability requirement

upvoted 14 times

✉️ **pbpally** 10 months, 3 weeks ago

Yup. Got me too. I picked A, saw D, and then reread the "scale seamlessly" part. D is correct.

upvoted 5 times

✉️ **NayeraB** 1 month, 1 week ago

But wouldn't RDS scale as well? Also Spot instances seems like a bit of a risky decision

upvoted 2 times

✉️ **genny** Highly Voted 11 months, 3 weeks ago

Selected Answer: A

I wouldn't run my website on spot instances. Spot instances might be terminated at any time, and since I need to run analytics application it's not an option for me. And using route 53 for load balancing of 2 instances is an overkill. I go with A.

upvoted 10 times

✉️ **AZ_Master** 4 months, 1 week ago

It is spot fleet - not spot instances. They can include On-Demand instances and can also maintain the target capacity automatically.

A Spot Fleet is a set of Spot Instances and optionally On-Demand Instances that is launched based on criteria that you specify. The Spot Fleet selects the Spot capacity pools that meet your needs and launches Spot Instances to meet the target capacity for the fleet. By default, Spot Fleets are set to maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated.

Ref: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-fleet.html>

upvoted 11 times

✉️ **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: D

I'll pick D because it sounds fun :)

upvoted 1 times

✉️ **pentium75** 3 months ago

Selected Answer: D

"Scale seamlessly", none of A-C include scaling at all.
upvoted 1 times

 **xdkonorek2** 4 months, 2 weeks ago

Selected Answer: D

spot instance receives 2 minutes interruption notice, it should be enough for requests to finish, it's quite unusual for app to run longer requests
only option D allow for seamless scaling with autoscaling group
upvoted 1 times

 **BrijMohan08** 6 months, 1 week ago

Selected Answer: B

Option B is a cost-effective choice that combines the benefits of database migration to RDS, horizontal scaling with EC2 instances, and control over traffic distribution with Route 53 weighted routing, making it the best solution for the given requirements.
upvoted 2 times

 **pentium75** 3 months ago

But there's no scaling at all in B.
upvoted 3 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: D

Scale seamlessly = Autoscaling group, Amazon Aurora MySQL DB instance
Cost effective = Spot Fleet
upvoted 4 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

The key reasons are:

Migrating the database to Amazon Aurora MySQL provides a scalable, high performance database to support the application.
Creating an AMI of the web application and using it in an Auto Scaling group with Spot instances allows cheap and efficient scaling of the web tier.
The Application Load Balancer distributes traffic across the Auto Scaling group.
Spot instances in an Auto Scaling group allow cost-optimized automatic scaling based on demand.
This approach provides high availability and seamless scaling without manual intervention.
upvoted 4 times

 **cookieMr** 9 months ago

D is correct because migrating the database to Amazon Aurora provides better scalability and performance compared to Amazon RDS for MySQL.
Creating an AMI of the web application allows for easy replication of the application on multiple instances. Using a launch template and Auto Scaling group with Spot Fleet provides cost optimization by leveraging spot instances. Adding an Application Load Balancer ensures the load is distributed across the instances for seamless scaling.

A is incorrect because using an Application Load Balancer with multiple EC2 instances is a better approach for scalability compared to relying on a single instance.

B is incorrect because weighted routing in Amazon Route 53 distributes traffic based on fixed weights, which may not dynamically adjust to the changing load.

C is incorrect because using AWS Lambda to stop and change the instance type based on CPU utilization is not an efficient way to handle scaling for a web application. Auto Scaling is a better approach for dynamic scaling.

upvoted 2 times

 **jdr75** 11 months, 3 weeks ago

Selected Answer: D

the options that said "launch a second EC2", have no sense ... why 2?, why not 3 or 4 or 5?
so options A and B drop.

C is no sense (Lambda doing this like a Scaling Group?, absurd)

Has to be D. Little strange cos' Aurora is a very good solution, but NOT CHEAP (remember: cost-effectively).

To be honest, the most cost-effectively is B je je

upvoted 2 times

 **SuketuKohli** 1 year ago

A Spot Fleet is a set of Spot Instances and optionally On-Demand Instances that is launched based on criteria that you specify. The Spot Fleet selects the Spot capacity pools that meet your needs and launches Spot Instances to meet the target capacity for the fleet. By default, Spot Fleets are set to maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated. You can submit a Spot Fleet as a one-time request, which does not persist after the instances have been terminated. You can include On-Demand Instance requests in a Spot Fleet request.

upvoted 2 times

 **KZM** 1 year, 1 month ago

Ans: D

Both Amazon RDS for MySQL and Amazon Aurora MySQL are designed to provide customers with fully managed relational database services, but Amazon Aurora MySQL is designed to provide better performance, scalability, and reliability, making it a better option for customers who need high-performance database services.

upvoted 1 times

✉  **bullrem** 1 year, 2 months ago

Selected Answer: D

Using an Auto Scaling group with a launch template and a Spot Fleet allows the company to scale the application seamlessly and cost-effectively, by automatically adding or removing instances based on the demand, and using Spot instances which are spare compute capacity available in the AWS region at a lower price than On-Demand instances. And also by migrating the database to Amazon Aurora MySQL DB instance, it provides higher scalability, availability, and performance than traditional MySQL databases.

upvoted 2 times

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

Selected Answer: D

The answer is D:

Migrate the database to Amazon Aurora MySQL - this will let the DB scale on its own; it'll scale automatically without needing adjustment. Create AMI of the web app and using a launch template - this will make the creating of any future instances of the app seamless. They can then be added to the auto scaling group which will save them money as it will scale up and down based on demand. Using a spot fleet to launch instances- This solves the "MOST cost-effective" portion of the question as spot instances come at a huge discount at the cost of being terminated at any time Amazon deems fit. I think this is why there's a bit of disagreement on this. While it's the most cost effective, it would be a terrible choice if amazon were to terminate that spot instance during a busy period.

upvoted 1 times

✉  **gustavtd** 1 year, 2 months ago

But I have a question,

For Spot instance, is it possible that at some time there is no spot resources available at all? because it is not guaranteed, right?

upvoted 4 times

✉  **Rupak10** 1 year, 1 month ago

Spot fleet not spot instance mentioned over there. Spot fleet = Spot instance + on-demand instance. If we cannot manage the spot instance then we can use an on-demand instance.

upvoted 6 times

✉  **RupeC** 8 months, 1 week ago

Super bit of info. Thanks

upvoted 1 times

✉  **Zerotn3** 1 year, 2 months ago

Selected Answer: D

Option D is the most cost-effective solution that meets the requirements.

Migrating the database to Amazon Aurora MySQL will allow the database to scale automatically, so it can handle an increase in traffic without manual intervention. Creating an AMI of the web application and using a launch template will allow the company to quickly and easily launch new instances of the application, which can then be added to an Auto Scaling group. This will allow the application to automatically scale up and down based on demand, ensuring that there are enough resources to handle busy times without incurring the cost of running idle resources.

Using a Spot Fleet to launch the instances will allow the company to take advantage of Amazon's spare capacity and get a discount on their EC2 instances. Attaching an Application Load Balancer to the Auto Scaling group will allow the load to be distributed across all of the available instances, improving the performance and reliability of the application.

upvoted 3 times

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

Selected Answer: D

Option D is the most cost-effective solution because;

* it uses an Auto Scaling group with a launch template and a Spot Fleet to automatically scale the number of EC2 instances based on the workload.

* using a Spot Fleet allows the company to take advantage of the lower prices of Spot Instances while still providing the required performance and availability for the application.

* using an Aurora MySQL database instance allows the company to take advantage of the scalability and performance of Aurora.

upvoted 3 times

Question #146

Topic 1

A company runs a stateless web application in production on a group of Amazon EC2 On-Demand Instances behind an Application Load Balancer. The application experiences heavy usage during an 8-hour period each business day. Application usage is moderate and steady overnight. Application usage is low during weekends. The company wants to minimize its EC2 costs without affecting the availability of the application. Which solution will meet these requirements?

- A. Use Spot Instances for the entire workload.
- B. Use Reserved Instances for the baseline level of usage. Use Spot instances for any additional capacity that the application needs.
- C. Use On-Demand Instances for the baseline level of usage. Use Spot Instances for any additional capacity that the application needs.
- D. Use Dedicated Instances for the baseline level of usage. Use On-Demand Instances for any additional capacity that the application needs.

Correct Answer: B*Community vote distribution*

rob74 1 year, 4 months ago

Selected Answer: B

In the Question is mentioned that it has o Demand instances...so I think is more cheapest reserved and spot
upvoted 18 times

Qjb8m9h 1 year, 3 months ago

Answer is B: Reserved is cheaper than on demand the company has. And it's meet the availability (HA) requirement as to spot instance that can be disrupted at any time.

PRICING BELOW.

On-Demand: 0% There's no commitment from you. You pay the most with this option.

Reserved : 40%-60% 1-year or 3-year commitment from you. You save money from that commitment.

Spot 50%-90% Ridiculously inexpensive because there's no commitment from the AWS side.

upvoted 12 times

pentium75 3 months ago

Selected Answer: B

This is a bit unclear, but B seems the best option of the ones given.

Usage is either "heavy" (during the 8 hours), "moderate and steady" (overnight) or "low" (during weekends). So there is always SOME usage, which could be covered by a few Reserved Instances (which would be cheaper than On-Demand Instances).

A - "Spot instances for the entire workload", might 'affect the availability of the application'

B - Seems the best answer

C - More expensive than B

D - Dedicated instances aka dedicated hardware -> very expensive

upvoted 4 times

awsgeek75 2 months, 1 week ago

Agree, very little clarity between B and C but B makes more sense.

upvoted 1 times

HackPack 3 months ago

I vote for C:

Please explain me if I am wrong:

If application experiences heavy usage during an 8-hour period each business day and all other time we don't need them? it mean than on-demand price will be only 33% from total cost so saving will be near 66%, more than reserved instances all other load we can cover by spot instances.

So why it not C?

upvoted 1 times

dungtrungpham 1 month, 3 weeks ago

You got it wrong.

You need the application all the time (24/7) because it says: "moderate and steady overnight, low usage at the weekend", not 8 hours a day
upvoted 1 times

VladanO 3 months, 4 weeks ago

Selected Answer: C

On-Demand Instances are more appropriate than Reserved Instances because "The application is used heavily for a period of 8 hours every weekday" requirements.

upvoted 1 times

 **rcptryk** 3 months, 4 weeks ago

Selected Answer: C

The answer should be C. Because if reserved is chosen, you have to pay for every hour. I calculate from this pages (if I'm wrong please correct me) <https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/#:~:text=Reserved%20Instances%20provide%20you%20with,instances%20when%20you%20need%20them>.
 Example: for t4g.nano
 Reserved instances $(0.003 \times 24 \times 365) + (1.90 \times 12) = 49.08$
 On demand instance $(0.0042 \times 8 \times 365) = 12.264$
 it will be added spot instances
 upvoted 2 times

 **pentium75** 3 months ago

"The baseline level of usage" is the minimum usage that is always there (even at night and during weekends), for THAT you can use Reserved Instance.
 upvoted 2 times

 **Marco_St** 4 months ago

Selected Answer: B

B, since the application needs to be on 24/7 for business days; on weekends, it can be off at any moment. The question mentions something like 8 hour per business day but!!! this is just for heavy usage, the application is also on during overnight.
 upvoted 2 times

 **Juliez** 4 months, 3 weeks ago

Why it's not A ? the application is "stateless" so it can be interrupted at any moment and the spot option is the cheaper one.
 upvoted 2 times

 **vi24** 3 days, 11 hours ago

The statelessness of a web application does not necessarily mean that it's okay to be interrupted. Statelessness refers to how the application handles requests and manages session data, not its ability to handle interruptions.
 upvoted 1 times

 **pentium75** 3 months ago

But there might not be any Spot Instances available and the app would go offline.
 upvoted 2 times

 **StudyAllNite** 4 months, 3 weeks ago

Selected Answer: C

If we assume moderate usage of 8 hours on average every day a week, this should be on demand, since it is not a 24/7 server. There is downtime on the weekends and after the initial 8 hours.
 upvoted 2 times

 **SVDK** 2 months, 2 weeks ago

There is no downtime. The application runs all the time (even weekends). Weekends is the base workload which we cover with reserved instances, the higher workloads during the week is covered by spot instances.
 upvoted 2 times

 **ACloud_Guru15** 4 months, 4 weeks ago

Selected Answer: C

Answer is C as the Jobs won't run for 24hrs/day hence Reserved instances is not required. As the Job runs for 8hrs/day we can choose On-Demand Instances
 upvoted 2 times

 **pentium75** 3 months ago

Which jobs runs for 8 hrs/day? There are 8 hours/day of HEAVY usage, but the app runs 24/7.
 upvoted 1 times

 **rexix7368** 5 months ago

Selected Answer: C

C is most cost effective option for running not 7x24 loads
 upvoted 3 times

 **Wayne23Fang** 5 months, 2 weeks ago

Selected Answer: C

I see some internet post about On-Demand vs Reserved below. I also think the argument from the (C) camp is valid. But (B) is not wrong. Just depends on usage.
 quoted from: <https://www.pcapps.com/services/aws-reserved-vs-on-demand-instances/>
 If you know you are only going to use a particular server part-time – say, 8 hours a day, 5 days a week – we recommend purchasing On-Demand Instances for those servers. If you are unsure which instance type is most appropriate for your performance needs, our advice is to start with any On-Demand Instance for a month or two, and experiment with changing the Instance Type up or down to see it performs. The goal is to "dial into" the lowest cost instance type that meets your performance needs. We recommend that you purchase Reserved Instances only when you know you are going to use it close to 24×7 (or at least more than 75% of the time).
 upvoted 4 times

 **Modulopi** 5 months, 4 weeks ago

Selected Answer: C

For 8 hours/day on demand works best
upvoted 2 times

 **Azure55** 4 months, 3 weeks ago
and Application usage is moderate and steady overnight!
upvoted 2 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: B

Main concern here is cost and availability. Reserved Instances provide you with significant savings on your Amazon EC2 costs compared to On-Demand Instance pricing. Spot instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices. You can use Spot Instances for various stateless, fault-tolerant, or flexible applications.
upvoted 2 times

 **Valder21** 6 months, 3 weeks ago

Selected Answer: D

the application has STEADY workload in the non peak hours therefore it can not be spot instances
upvoted 2 times

 **pentium75** 3 months ago

But Dedicated Instances (D) are costly as hell, and it would be overkill to have dedicated hardware for that scenario.
upvoted 2 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

The reasons are:

On-Demand Instances provide stable, reliable baseline capacity for the normal workload.
Spot Instances can provide the additional capacity needed during peak periods at a much lower hourly rate compared to On-Demand.
The stateless nature of the application allows taking advantage of Spot without affecting availability. If Spot is interrupted, the baseline On-Demand capacity remains available.
Reserved Instances require upfront commitment and may not match the variable workload.
Dedicated Instances are more expensive than On-Demand for baseline capacity.
Using only Spot Instances risks interruption during peak times if capacity is not available.
upvoted 4 times

 **toussyn** 8 months ago

Selected Answer: C

On demand for baseline:
lets say it cost \$100 per hour, then the cost of running it for a day would be: $\$100 * 8 = 800$. Times 8 because we'll only be running for 8 hours in a day.

With Reserve instance on the other hand we are locked in for a year, but at 60% discount. That means we'll be paying \$40 per hour. Running it for a day: $\$40 * 24 = \960

upvoted 4 times

Question #147

Topic 1

A company needs to retain application log files for a critical application for 10 years. The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed. The application generates more than 10 TB of logs per month. Which storage option meets these requirements MOST cost-effectively?

- A. Store the logs in Amazon S3. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.
- B. Store the logs in Amazon S3. Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.
- C. Store the logs in Amazon CloudWatch Logs. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.
- D. Store the logs in Amazon CloudWatch Logs. Use Amazon S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.

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

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

Selected Answer: B

Why not AwsBackup? No Glacier Deep is supported by AWS Backup

<https://docs.aws.amazon.com/aws-backup/latest/devguide/s3-backups.html>

AWS Backup allows you to backup your S3 data stored in the following S3 Storage Classes:

- S3 Standard
- S3 Standard - Infrequently Access (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering (S3 INT)

upvoted 10 times

 **tdkcumberland** 1 year, 4 months ago

AWS BackUp costs something, setting up S3 LCP doesn't.

upvoted 5 times

 **TariqKipkemei** Most Recent  6 months, 2 weeks ago

Selected Answer: B

S3 Lifecycle policies to the rescue

upvoted 2 times

 **cookieMr** 9 months ago

Selected Answer: B

B is the most cost-effective solution. Storing the logs in S3 and using S3 Lifecycle policies to transition logs older than 1 month to S3 Glacier Deep Archive allows for cost optimization based on data access patterns. Since logs older than 1 month are rarely accessed, moving them to S3 Glacier Deep Archive helps minimize storage costs while still retaining the logs for the required 10-year period.

A is incorrect because using AWS Backup to move logs to S3 Glacier Deep Archive can incur additional costs and complexity compared to using S3 Lifecycle policies directly.

C adds unnecessary complexity and costs by involving CloudWatch Logs and AWS Backup when direct management through S3 is sufficient.

D is incorrect because using S3 Lifecycle policies to move logs from CloudWatch Logs to S3 Glacier Deep Archive is not a valid option. CloudWatch Logs and S3 have separate storage mechanisms, and S3 Lifecycle policies cannot be applied directly to CloudWatch Logs.

upvoted 4 times

 **Mamiololo** 1 year, 2 months ago

B is correct..

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 2 months ago

Selected Answer: B

Option B (Store the logs in Amazon S3. Use S3 Lifecycle policies to move logs more than 1-month-old to S3 Glacier Deep Archive) would meet these requirements in the most cost-effective manner.

This solution would allow the application team to quickly access the logs from the past month for troubleshooting, while also providing a cost-effective storage solution for the logs that are rarely accessed and need to be retained for 10 years.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B is most cost effective. Moving logs to Cloudwatch logs may incur additional cost.
upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **ArielSchivo** 1 year, 4 months ago

Selected Answer: B

S3 + Glacier is the most cost effective.

upvoted 3 times

 **Bevemo** 1 year, 4 months ago

Selected Answer: B

D works, archive cloudwatch logs to S3 but is an additional service to pay for over B.

upvoted 1 times

 **Aamee** 1 year, 3 months ago

CloudWatch logs can't store around 10 TB of data per month I believe so both C and D options are ruled out already.

upvoted 1 times

 **masetromain** 1 year, 4 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/80772-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Question #148

Topic 1

A company has a data ingestion workflow that includes the following components:

An Amazon Simple Notification Service (Amazon SNS) topic that receives notifications about new data deliveries

An AWS Lambda function that processes and stores the data

The ingestion workflow occasionally fails because of network connectivity issues. When failure occurs, the corresponding data is not ingested unless the company manually reruns the job.

What should a solutions architect do to ensure that all notifications are eventually processed?

- A. Configure the Lambda function for deployment across multiple Availability Zones.
- B. Modify the Lambda function's configuration to increase the CPU and memory allocations for the function.
- C. Configure the SNS topic's retry strategy to increase both the number of retries and the wait time between retries.
- D. Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure destination. Modify the Lambda function to process messages in the queue.

Correct Answer: D

Community vote distribution



✉️ **bunnychip** 1 year, 5 months ago

Selected Answer: D

ensure that all notifications are eventually processed

upvoted 12 times

✉️ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure destination. Modify the Lambda function to process messages in the queue.

upvoted 2 times

✉️ **Help2023** 1 year, 1 month ago

Selected Answer: D

This is why <https://docs.aws.amazon.com/sns/latest/dg/sns-message-delivery-retries.html>

upvoted 3 times

✉️ **CaoMengde09** 1 year, 1 month ago

C is not the right answer since after several retries SNS discard the message which doesn't align with the requirement. D is the right answer
upvoted 4 times

✉️ **CaoMengde09** 1 year, 1 month ago

Best solution to process failed SNS notifications is using sns-dead-letter-queues (SQS Queue for reprocessing)
<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>

upvoted 3 times

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

Selected Answer: D

To ensure that all notifications are eventually processed, the best solution would be to configure an Amazon Simple Queue Service (SQS) queue as the on-failure destination for the SNS topic. This will allow the notifications to be retried until they are successfully processed. The Lambda function can then be modified to process messages in the queue, ensuring that all notifications are eventually processed. Option D, "Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure destination. Modify the Lambda function to process messages in the queue," is the correct answer.

upvoted 1 times

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

Selected Answer: D

I choose Option D as the correct answer.

To ensure that all notifications are eventually processed, the solutions architect can set up an Amazon SQS queue as the on-failure destination for the Amazon SNS topic. This way, when the Lambda function fails due to network connectivity issues, the notification will be sent to the queue instead of being lost. The Lambda function can then be modified to process messages in the queue, ensuring that all notifications are eventually processed.

upvoted 3 times

✉️ **techhb** 1 year, 3 months ago

Selected Answer: D

Option D to ensure that all notifications are eventually processed you need to use SQS.
upvoted 2 times

 **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C is right option.
SNS does not have any "On Failure" delivery destination. One need to configure dead-letter queue and configure SQS to read from there. So given this option D is incorrect.
upvoted 2 times

 **JayBee65** 1 year, 3 months ago

I don't think that's right

"A dead-letter queue is an Amazon SQS queue that an Amazon SNS subscription can target for messages that can't be delivered to subscribers successfully. Messages that can't be delivered due to client errors or server errors are held in the dead-letter queue for further analysis or reprocessing" from <https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>.

This is pretty much what is being described in D.

Plus C will only retry message processing, and network problems could still prevent the message from being processed, but the question states "ensure that all notifications are eventually processed". So C does not meet the requirements but D does look to do this.

upvoted 7 times

 **Gajendr** 2 months, 4 weeks ago

+ <https://docs.aws.amazon.com/sns/latest/dg/sns-message-delivery-retries.html>

""To keep the message after the retries specified in the delivery policy are exhausted, configure your subscription to move undeliverables messages to a dead-letter queue (DLQ). For more information"" So D

upvoted 1 times

 **NikaCZ** 1 year, 3 months ago

Selected Answer: D

Is correct.

upvoted 1 times

 **NikaCZ** 1 year, 3 months ago

If you want to ensure that all notifications are eventually processed you need to use SQS.

upvoted 1 times

 **Wajif** 1 year, 3 months ago

Selected Answer: D

C isn't specific. Hence D

upvoted 1 times

 **LeGlopier** 1 year, 4 months ago

Selected Answer: C

"on-failure destination" doesn't exist, only dead letter queue exist.
that's why I am leaning for C

upvoted 1 times

 **Wajif** 1 year, 3 months ago

Dead letter queue doesn't exist in SNS. They are specifically saying a new queue will be configured for failures from SNS. Hence D

upvoted 2 times

 **Wpcorgan** 1 year, 4 months ago

D is correct

upvoted 1 times

 **ds0321** 1 year, 4 months ago

Selected Answer: D

D is the answer

upvoted 1 times

 **ArielSchivo** 1 year, 4 months ago

Selected Answer: D

Option C could work but the max retries attempts is 23 days. After that messages are deleted. And you do not want that to happen! So, Option D.
upvoted 4 times

 **SimonPark** 1 year, 4 months ago

Selected Answer: D

imho, D is the answer

upvoted 1 times

Question #149

Topic 1

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.

How should a solutions architect accomplish this?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
- C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **theochan** 2 months, 1 week ago

Selected Answer: A

Easiest question ever?

upvoted 1 times

✉️  **pentium75** 3 months ago

Selected Answer: A

"specific order" = must be FIFO queue = only mentioned in A

upvoted 3 times

✉️  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.

upvoted 1 times

✉️  **cookieMr** 9 months ago

A is the correct solution. By creating an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages and setting up an AWS Lambda function to process messages from the queue, the company can ensure that the order of the event data is maintained throughout processing. SQS FIFO queues guarantee the order of messages and are suitable for scenarios where strict message ordering is required.

B is incorrect because Amazon Simple Notification Service (Amazon SNS) topics are not designed to preserve message order. SNS is a publish-subscribe messaging service and does not guarantee the order of message delivery.

C is incorrect because using an SQS standard queue does not guarantee the order of message processing. SQS standard queues provide high throughput and scale, but they do not guarantee strict message ordering.

D is incorrect because configuring an SQS queue as a subscriber to an SNS topic does not ensure message ordering. SNS topics distribute messages to subscribers independently, and the order of message processing is not guaranteed.

upvoted 4 times

✉️  **cheese929** 11 months ago

Selected Answer: A

A is correct. Use FIFO to process in the specific order required

upvoted 2 times

✉️  **Wheretocanstart** 1 year ago

Selected Answer: A

Option A is correct...data is processed in the correct order

upvoted 1 times

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

Selected Answer: A

The correct solution is Option A. Creating an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages and setting up an AWS Lambda function to process messages from the queue will ensure that the event data is processed in the correct order and minimize operational overhead.

Option B is incorrect because using Amazon Simple Notification Service (Amazon SNS) does not guarantee the order in which messages are delivered.

Option C is incorrect because using an Amazon SQS standard queue does not guarantee the order in which messages are processed.

Option D is incorrect because using an Amazon SQS queue as a subscriber to an Amazon SNS topic does not guarantee the order in which messages are processed.

upvoted 4 times

 **techhb** 1 year, 3 months ago

Only A is right option here.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

Option A is the best option.

upvoted 2 times

 **alect096** 1 year, 3 months ago

Selected Answer: A

"The data is written in a specific order that must be maintained throughout processing" --> FIFO

upvoted 4 times

 **NikaCZ** 1 year, 3 months ago

Selected Answer: A

specific order = FIFO

upvoted 1 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: A

A is correct

upvoted 1 times

 **david76x** 1 year, 3 months ago

Selected Answer: A

Definitely A

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 1 times

 **ArielSchivo** 1 year, 4 months ago

Selected Answer: A

FIFO means order, so Option A.

upvoted 4 times

 **rjam** 1 year, 4 months ago

Order --- means FIFO option A

upvoted 3 times

Question #150

Topic 1

A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.

What should the solutions architect do to meet these requirements?

- A. Create Amazon CloudWatch composite alarms where possible.
- B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.
- C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.
- D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.

Correct Answer: A

Community vote distribution

A (100%)

 **123jh10**  1 year, 5 months ago

Selected Answer: A

Composite alarms determine their states by monitoring the states of other alarms. You can **use composite alarms to reduce alarm noise**. For example, you can create a composite alarm where the underlying metric alarms go into ALARM when they meet specific conditions. You then can set up your composite alarm to go into ALARM and send you notifications when the underlying metric alarms go into ALARM by configuring the underlying metric alarms never to take actions. Currently, composite alarms can take the following actions:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Create_Composite_Alarm.html

upvoted 25 times

 **cookieMr**  9 months ago

Selected Answer: A

By creating composite alarms in CloudWatch, the solutions architect can combine multiple metrics, such as CPU utilization and read IOPS, into a single alarm. This allows the company to take action only when both conditions are met, reducing false alarms and focusing on meaningful alerts.

B can help in monitoring the overall health and performance of the application. However, it does not directly address the specific requirement of triggering an action when CPU utilization and read IOPS exceed certain thresholds simultaneously.

C. Creating CloudWatch Synthetics canaries is useful for actively monitoring the application's behavior and availability. However, it does not directly address the specific requirement of monitoring CPU utilization and read IOPS to trigger an action.

D. Creating single CloudWatch metric alarms with multiple metric thresholds where possible can be an option, but it does not address the requirement of triggering an action only when both CPU utilization and read IOPS exceed their respective thresholds simultaneously.

upvoted 7 times

 **awsgeek75**  2 months, 1 week ago

Selected Answer: A

Composite for multiple conditions like AND/OR combinations

B: This option just made me laugh. Lol, will someone just sit and look at this dashboard?

C: CW Synthetics canaries if for API

D: Single won't monitor multiple metrics

upvoted 1 times

 **Modulopi** 5 months, 4 weeks ago

Selected Answer: A

A: Composite alarms determine their states by monitoring the states of other alarms. You can use composite alarms to reduce alarm noise. For example, you can create a composite alarm where the underlying metric alarms go into ALARM when they meet specific conditions.

upvoted 1 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: A

Composite alarms was designed to handle this scenario.

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

The key reasons are:

Composite alarms allow defining alarms with multiple metrics and conditions, like high CPU AND high read IOPS in this case.

Composite alarms can avoid false positives triggered by a single metric spike.

Dashboards help visualize but won't take automated action. Synthetics tests application availability but doesn't address the metrics. Single metric alarms with multiple thresholds can't correlate across metrics and may still trigger false positives. Composite alarms allow acting quickly when both CPU and IOPS are high, per the stated need.

upvoted 4 times

 **Abrar2022** 10 months ago

The composite alarm goes into ALARM state only if all conditions of the rule are met.

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: A

Option A, creating Amazon CloudWatch composite alarms, is correct because it allows the solutions architect to create an alarm that is triggered only when both CPU utilization is above 50% and read IOPS on the disk are high at the same time. This meets the requirement to act as soon as possible if both conditions are met, while also reducing the number of false alarms by ensuring that the alarm is triggered only when both conditions are met.

upvoted 4 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

The incorrect solutions are:

In contrast, Option B, creating Amazon CloudWatch dashboards, would not directly address the requirement to trigger an alarm when both CPU utilization is high and read IOPS on the disk are high at the same time. Dashboards can be useful for visualizing metric data and identifying trends, but they do not have the capability to trigger alarms based on multiple metric thresholds.

Option C, using Amazon CloudWatch Synthetics canaries, may not be the best choice for this scenario, as canaries are used for synthetic testing rather than for monitoring live traffic. Canaries can be useful for monitoring the availability and performance of an application, but they may not be the most effective way to monitor the specific metric thresholds and conditions described in this scenario.

upvoted 3 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option D, creating single Amazon CloudWatch metric alarms with multiple metric thresholds, would not allow the solutions architect to create an alarm that is triggered only when both CPU utilization and read IOPS on the disk are high at the same time. Instead, the alarm would be triggered whenever any of the specified metric thresholds are exceeded, which may result in a higher number of false alarms.

upvoted 5 times

 **BENICE** 1 year, 3 months ago

A is correct answer

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

Option A

upvoted 1 times

 **Qjb8m9h** 1 year, 3 months ago

The AWS::CloudWatch::CompositeAlarm type creates or updates a composite alarm. When you create a composite alarm, you specify a rule expression for the alarm that takes into account the alarm states of other alarms that you have created. The composite alarm goes into ALARM state only if all conditions of the rule are met.

The alarms specified in a composite alarm's rule expression can include metric alarms and other composite alarms. Using composite alarms can reduce alarm noise.

upvoted 3 times

 **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 1 times

Question #151

Topic 1

A company wants to migrate its on-premises data center to AWS. According to the company's compliance requirements, the company can use only the ap-northeast-3 Region. Company administrators are not permitted to connect VPCs to the internet. Which solutions will meet these requirements? (Choose two.)

- A. Use AWS Control Tower to implement data residency guardrails to deny internet access and deny access to all AWS Regions except ap-northeast-3.
- B. Use rules in AWS WAF to prevent internet access. Deny access to all AWS Regions except ap-northeast-3 in the AWS account settings.
- C. Use AWS Organizations to configure service control policies (SCPs) that prevent VPCs from gaining internet access. Deny access to all AWS Regions except ap-northeast-3.
- D. Create an outbound rule for the network ACL in each VPC to deny all traffic from 0.0.0.0/0. Create an IAM policy for each user to prevent the use of any AWS Region other than ap-northeast-3.
- E. Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3.

Correct Answer: AC*Community vote distribution*

Six_Fingered_Jose Highly Voted 1 year, 5 months ago

Selected Answer: AC

agree with A and C

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_vpc.html#example_vpc_2

upvoted 18 times

cookieMr Highly Voted 9 months ago

Selected Answer: AC

A. By using Control Tower, the company can enforce data residency guardrails and restrict internet access for VPCs and denies access to all Regions except the required ap-northeast-3 Region.

C. With Organizations, the company can configure SCPs to prevent VPCs from gaining internet access. By denying access to all Regions except ap-northeast-3, the company ensures that VPCs can only be deployed in the specified Region.

Option B is incorrect because using rules in AWS WAF alone does not address the requirement of denying access to all AWS Regions except ap-northeast-3.

Option D is incorrect because configuring outbound rules in network ACLs and IAM policies for users can help restrict traffic and access, but it does not enforce the company's requirement of denying access to all Regions except ap-northeast-3.

Option E is incorrect because using AWS Config and managed rules can help detect and alert for specific resources and configurations, but it does not directly enforce the restriction of internet access or deny access to specific Regions.

upvoted 11 times

awsgEEK75 Most Recent 2 months, 1 week ago

Selected Answer: AC

B: Irrelevant WAF

D: This is confusing so I'll ignore it.

E: Wrong product

A: Control Tower can have residency guard rails and block internet access.

C: SCP is like a duplicate of A IMHO but it stops admins from circumventing A as Org policies cannot be overridden by admins unless they are org admins.

Too many assumptions

upvoted 1 times

BrijMohan08 6 months, 1 week ago

Selected Answer: AC

A. Use AWS Control Tower to implement data residency guardrails to deny internet access and deny access to all AWS Regions except ap-northeast-3.

C. Use AWS Organizations to configure service control policies (SCPs) that prevent VPCs from gaining internet access. Deny access to all AWS Regions except ap-northeast-3.

upvoted 2 times

TariqKipkemei 6 months, 2 weeks ago

Selected Answer: AC

Use Control Tower to implement data residency guardrails and Service Control Policies (SCPS) to prevent VPCs from gaining internet access.
upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: AC

AWS Control Tower guardrails and AWS Organizations SCPs provide centralized, automated mechanisms to enforce no internet connectivity for VPCs and restrict Region access to only ap-northeast-3.
upvoted 3 times

 **Abrar2022** 9 months, 2 weeks ago

Didn't know that SCPS (Service Control Policies) could be used to deny users internet access. Good to know. Always thought it's got controlling who can and can't access AWS Services.
upvoted 4 times

 **hicham0101** 11 months ago

Agree with A and C
<https://aws.amazon.com/blogs/aws/new-for-aws-control-tower-region-deny-and-guardrails-to-help-you-meet-data-residency-requirements/>
upvoted 1 times

 **yallahool** 11 months, 2 weeks ago

I choose C and D.
For control tower, it can't be A because ap-northeast-3 doesn't support it!
Also, in the case of E, it is detection and warning, so it is difficult to prevent internet connection (although the view is a little obscure).
upvoted 1 times

 **michellemeloc** 10 months, 3 weeks ago

I just check, now it's supported!!!
upvoted 2 times

 **notacert** 11 months, 3 weeks ago

Selected Answer: AC

A and C
upvoted 1 times

 **datz** 11 months, 3 weeks ago

Selected Answer: CD

C/D

A - CANNOT BE!!! AWS Control Tower is not available in ap-northeast-3! Check your
B - for sure no
C - SCPS (Service Control Policies)- For sure
D - Deny outbound rule to be placed in prod and also IAM Policy to deny Users creating services in AP-Northeast3
E - it creates an alert, which means it happens but an alert is triggered. so I think it's not good either.
upvoted 2 times

 **darn** 11 months, 1 week ago

False, Control Tower is in Osaka NorthEast 3
<https://docs.aws.amazon.com/controlltower/latest/userguide/region-how.html>
upvoted 2 times

 **Kaireny54** 11 months, 4 weeks ago

Selected Answer: CD

Control tower isn't available in AP-northeast-3 (only available in ap-northeast-1 and 2 : <https://www.aws-services.info/controlltower.html>)
For answer E, it creates an alert, which means it happens but an alert is triggered. so I think it's not good either.
That's why I would go for C and D
upvoted 2 times

 **darn** 11 months, 1 week ago

False, Control Tower is in Osaka NorthEast 3
<https://docs.aws.amazon.com/controlltower/latest/userguide/region-how.html>
upvoted 1 times

 **darn** 11 months, 1 week ago

same page you posted:
ap-northeast-3 Asia Pacific (Osaka) 2023-04-20 <https://aws.amazon.com/controlltower>
upvoted 1 times

 **Bmarodi** 10 months, 1 week ago

It's available now on the same link you pasted earlier: ap-northeast-3 Asia Pacific (Osaka) 2023-04-20.
upvoted 1 times

 **WhericanIstart** 1 year ago

Selected Answer: CE

AWS Control tower is not available in ap-northeast-3!

<https://www.aws-services.info/controlltower.html>

upvoted 1 times

✉️ **warioverde** 1 year ago

What's wrong with B?

upvoted 2 times

✉️ **AlessandraSAA** 1 year ago

Selected Answer: CE

A - CANNOT BE!!! AWS Control Tower is not available in ap-northeast-3! Check your consolle.

upvoted 4 times

✉️ **moaaz86** 1 year, 1 month ago

From ChatGPT :)

Control Tower: Can

Yes, AWS Control Tower can implement data residency guardrails to deny internet access and restrict access to AWS Regions except for one. To restrict access to AWS regions, you can create a guardrail using AWS Organizations to deny access to all AWS regions except for the one that you want to allow. This can be done by creating an organizational policy that restricts access to specific AWS services and resources based on region.

Config: Can(not).

Yes, AWS Config can help you enforce restrictions on internet access and control access to specific AWS Regions using AWS Config Rules. It's worth noting that AWS Config is a monitoring service that provides continuous assessment of your AWS resources against desired configurations. While AWS Config can alert you when a configuration change occurs, it cannot directly restrict access to resources or enforce specific policies. For that, you may need to use other AWS services such as AWS Identity and Access Management (IAM), AWS Firewall Manager, or AWS Organizations.

upvoted 3 times

✉️ **ACloud_Guru15** 4 months, 4 weeks ago

If we say AWS won't support Control Tower & config, it will simply agree by asking few more questions. Don't trust ChatGPT blindly

upvoted 1 times

✉️ **KZM** 1 year, 1 month ago

Option A uses AWS Control Tower to implement data residency guardrails, but it does not prevent internet access by itself. It only denies access to all AWS Regions except ap-northeast-3. The requirement states that administrators are not permitted to connect VPCs to the internet, so Option A does not meet this requirement.

upvoted 2 times

✉️ **pentium75** 3 months ago

"AWS Control Tower also offers guardrails to further control data residency in underlying AWS service options, for example, blocking Amazon Simple Storage Service (Amazon S3) cross-region replication or BLOCKING THE CREATION OF INTERNET GATEWAYS."

<https://aws.amazon.com/de/blogs/aws/new-for-aws-control-tower-region-deny-and-guardrails-to-help-you-meet-data-residency-requirements/>

upvoted 1 times

Question #152

Topic 1

A company uses a three-tier web application to provide training to new employees. The application is accessed for only 12 hours every day. The company is using an Amazon RDS for MySQL DB instance to store information and wants to minimize costs. What should a solutions architect do to meet these requirements?

- A. Configure an IAM policy for AWS Systems Manager Session Manager. Create an IAM role for the policy. Update the trust relationship of the role. Set up automatic start and stop for the DB instance.
- B. Create an Amazon ElastiCache for Redis cache cluster that gives users the ability to access the data from the cache when the DB instance is stopped. Invalidate the cache after the DB instance is started.
- C. Launch an Amazon EC2 instance. Create an IAM role that grants access to Amazon RDS. Attach the role to the EC2 instance. Configure a cron job to start and stop the EC2 instance on the desired schedule.
- D. Create AWS Lambda functions to start and stop the DB instance. Create Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions. Configure the Lambda functions as event targets for the rules.

Correct Answer: D

Community vote distribution



✉️ **study_aws1** Highly Voted 1 year, 4 months ago

<https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-lambda/>

It is option D. Option A could have been applicable had it been AWS Systems Manager State Manager & not AWS Systems Manager Session Manager

upvoted 31 times

✉️ **123jh10** Highly Voted 1 year, 5 months ago

Selected Answer: A

A is true for sure. "Schedule Amazon RDS stop and start using AWS Systems Manager" Steps in the documentation:

1. Configure an AWS Identity and Access Management (IAM) policy for State Manager.
2. Create an IAM role for the new policy.
3. Update the trust relationship of the role so Systems Manager can use it.
4. Set up the automatic stop with State Manager.
5. Set up the automatic start with State Manager.

<https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-systems-manager/>

upvoted 8 times

✉️ **Kien048** 1 year, 4 months ago

And ofcause, D is working, so if A also right, the question is wrong.

upvoted 4 times

✉️ **Kien048** 1 year, 4 months ago

Look like State manager and Session manager use for difference purpose even both in same dashboard console.

upvoted 1 times

✉️ **Bevemo** 1 year, 4 months ago

Agree A, free to use state manager within limits, and don't need to code or manage lambda.

upvoted 1 times

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

Option A refers to Session Manager, not State Manager as you pointed, so it is wrong. Option D is valid.

upvoted 12 times

✉️ **LP0905** Most Recent 1 week, 6 days ago

Selected Answer: D

Although both A and D is a workable solution, the requirements is to minimum cost.

The benefits of automating the startup and shutdown of RDS DB instances using Lambda allows organizations to further reduce compute costs and simplify the administration of database environments that don't need to be running continuously.

<https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-lambda/>

For using system manager to accomplish the task works however keep in mind that although we're stopping the databases, the storage costs for the databases still apply.

<https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-systems-manager/>

Initially I also thought that A would be the correct answer however looking at the administration and cost I would go for D as a better solution instead.

upvoted 2 times

 **thewalker** 1 month, 3 weeks ago

Selected Answer: A

To automatically shutdown an RDS instance during 09:00 PM to 09:00 AM and have it available between 09:00 AM to 09:00 PM, you can use AWS Systems Manager Maintenance Windows.

Create two Maintenance Windows - one to stop the RDS instance at 09:00 PM and another to start it at 09:00 AM.

For each Maintenance Window, select the "AWS-StopRDSInstance" and "AWS-StartRDSInstance" runbooks respectively and specify the cron expression for the schedule.

Tag the RDS instance with a name so it can be identified by the runbooks.

The runbooks will then automatically stop and start the RDS instance on the specified schedule without needing any manual intervention.

upvoted 1 times

 **thewalker** 1 month, 3 weeks ago

This allows cost savings by shutting down the RDS instance during non-business hours while keeping it available during the day as per your requirements. Refer to the AWS documentation for more details on configuring Maintenance Windows and runbooks.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-stop-and-start-an-amazon-rds-db-instance-using-aws-systems-manager-maintenance-windows.html>

https://repost.aws/questions/QUcVR5js8LSbOS_LE889KdIg/automatically-stop-and-start-an-amazon-rds-db-instance-in-a-cdk-app

upvoted 1 times

 **theochan** 2 months, 1 week ago

Guys, we still have to pay for RDS instance even we stopped it, isn't it?

upvoted 2 times

 **Ruffyit** 3 months, 4 weeks ago

AWS Lambda functions can be used to start and stop RDS instances programmatically.

EventBridge scheduled rules can trigger the Lambda functions at specified times daily.

This allows fully automating the starting and stopping of RDS on a schedule to match usage patterns.

RDS billing is per hour when instance is running, so stopping when not in use significantly reduces costs.

Using Lambda and EventBridge is simpler and more robust than cron jobs on EC2.

ElastiCache and Systems Manager Session Manager are useful tools but do not directly address scheduled RDS start/stop.

upvoted 2 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: D

You can use AWS Lambda and Amazon EventBridge to schedule a Lambda function to stop and start the idle databases with specific tags to save on compute costs.

<https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-lambda/#:~:text=you%20to%20schedule%20a-,Lambda%20function,-to%20stop%20and%20start>

upvoted 2 times

 **lemur88** 7 months ago

Selected Answer: D

Here is the recommended solutions which describes choice D - <https://aws.amazon.com/blogs/database/save-costs-by-automating-the-start-and-stop-of-amazon-rds-instances-with-aws-lambda-and-amazon-eventbridge/>

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

AWS Lambda functions can be used to start and stop RDS instances programmatically.

EventBridge scheduled rules can trigger the Lambda functions at specified times daily.

This allows fully automating the starting and stopping of RDS on a schedule to match usage patterns.

RDS billing is per hour when instance is running, so stopping when not in use significantly reduces costs.

Using Lambda and EventBridge is simpler and more robust than cron jobs on EC2.

ElastiCache and Systems Manager Session Manager are useful tools but do not directly address scheduled RDS start/stop.

upvoted 3 times

 **cookieMr** 9 months ago

Selected Answer: D

By using AWS Lambda functions triggered by Amazon EventBridge scheduled rules, the company can automate the start and stop actions for the Amazon RDS for MySQL DB instance based on the 12-hour access period. This allows them to minimize costs by only running the DB instance when it is needed.

Option A is not the most suitable solution because it refers to IAM policies for AWS Systems Manager Session Manager, which is primarily used for interactive shell access to EC2 instances and does not directly address the requirement of starting and stopping the DB instance.

Option B is not the most suitable solution because it suggests using Amazon ElastiCache for Redis as a cache cluster, which may not provide the desired cost optimization for the DB instance.

Option C is not the most suitable solution because launching an EC2 instance and configuring cron jobs to start and stop it does not directly address the requirement of minimizing costs for the Amazon RDS DB instance.

upvoted 3 times

✉️ **Siva007** 10 months ago

Selected Answer: D

I got this question in real exam!

upvoted 4 times

✉️ **srijrao** 9 months ago

why we need more than one lambda function to start and stop DB instance? btw how many questions came from this site?

upvoted 2 times

✉️ **ccmc** 10 months, 3 weeks ago

State Manager, a capability of AWS Systems Manager

upvoted 1 times

✉️ **Ankit_EC_ran** 11 months ago

Selected Answer: D

Option D is correct

upvoted 2 times

✉️ **Musti35** 11 months, 1 week ago

Selected Answer: D

In a typical development environment, dev and test databases are mostly utilized for 8 hours a day and sit idle when not in use. However, the databases are billed for the compute and storage costs during this idle time. To reduce the overall cost, Amazon RDS allows instances to be stopped temporarily. While the instance is stopped, you're charged for storage and backups, but not for the DB instance hours. Please note that a stopped instance will automatically be started after 7 days.

This post presents a solution using AWS Lambda and Amazon EventBridge that allows you to schedule a Lambda function to stop and start the idle databases with specific tags to save on compute costs. The second post presents a solution that accomplishes stop and start of the idle Amazon RDS databases using AWS Systems Manager.

upvoted 3 times

✉️ **test_devops_aws** 1 year ago

Selected Answer: D

<https://docs.aws.amazon.com/systems-manager-automation-runbooks/latest/userguide/automation-ref-rds.html>

upvoted 1 times

✉️ **aba2s** 1 year, 2 months ago

Selected Answer: D

AWS Lambda and Amazon EventBridge that allows you to schedule a Lambda function to stop and start the idle databases with specific tags to save on compute costs. <https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-lambda/>

upvoted 2 times

✉️ **Zerotn3** 1 year, 2 months ago

Selected Answer: D

The correct answer is D. Creating AWS Lambda functions to start and stop the DB instance and using Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions is the most cost-effective way to meet the requirements. The Lambda functions can be configured as event targets for the scheduled rules, which will allow the DB instance to be started and stopped on the desired schedule.

upvoted 4 times

Question #153

Topic 1

A company sells ringtones created from clips of popular songs. The files containing the ringtones are stored in Amazon S3 Standard and are at least 128 KB in size. The company has millions of files, but downloads are infrequent for ringtones older than 90 days. The company needs to save money on storage while keeping the most accessed files readily available for its users.

Which action should the company take to meet these requirements MOST cost-effectively?

- A. Configure S3 Standard-Infrequent Access (S3 Standard-IA) storage for the initial storage tier of the objects.
- B. Move the files to S3 Intelligent-Tiering and configure it to move objects to a less expensive storage tier after 90 days.
- C. Configure S3 inventory to manage objects and move them to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.
- D. Implement an S3 Lifecycle policy that moves the objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.

Correct Answer: D*Community vote distribution*

rjam 1 year, 4 months ago

Selected Answer: D

Answer D

Why Optoin D ?

The Question talks about downloads are infrequent older than 90 days which means files less than 90 days are accessed frequently. Standard-Infrequent Access (S3 Standard-IA) needs a minimum 30 days if accessed before, it costs more.

So to access the files frequently you need a S3 Standard . After 90 days you can move it to Standard-Infrequent Access (S3 Standard-IA) as its going to be less frequently accessed

upvoted 37 times

MutiverseAgent 8 months, 1 week ago

I do not agree. The MOST cheaper option is B, because by choosing:

D) Files older than 90 days will live eternally in the S3 Infrequently access layer at \$0.0125/GB.

B) Using Intelligent-Tiering files older than 90 days can be moved DIRECTLY to the "Archive access tier" (Glacier instant retrieval) at \$0.004/GB, avoiding/skipping the "S3 Infrequently access layer". The question also seems to be according this assumption as says "and configure it to move objects to a less expensive storage tier after 90 days".

<https://aws.amazon.com/s3/pricing/?nc=sn&loc=4>

upvoted 2 times

MutiverseAgent 8 months, 1 week ago

I am taking back my answer, the right is D) as the "Archive access tier" check present in the "Intelligent-Tiering Archive configurations" is for "S3 Glacier flexible retrieval" which is not instant retrieval.

upvoted 6 times

zeronine75 1 year, 4 months ago

Selected Answer: B

B/D seems possible answer. But, I'll go with "B".

In the following table, S3 Intelligent-Tiering seems not so expansive than S3 Standard.

https://aws.amazon.com/s3/pricing/?nc1=h_ls

And, in the question "128KB" size is talking about S3 Intelligent-Tiering stuff.

upvoted 13 times

FNJ1111 1 year, 2 months ago

also, there are probably several ringtones which aren't popular/used. Why keep them in S3 standard? The company would save money if s3 intelligent-tiering moves the unpopular ringtones to a more cost-effective tier than s3 standard.

upvoted 1 times

Wilson_S 1 year, 4 months ago

This link also has me going with "B." Specifying 128 KB in size is not a coincidence. <https://aws.amazon.com/s3/storage-classes/intelligent-tiering/>

upvoted 5 times

javitech83 1 year, 3 months ago

because of tha link it is D.

There are no retrieval charges in S3 Intelligent-Tiering. S3 Intelligent-Tiering has no minimum eligible object size, but objects smaller than 128 KB are not eligible for auto tiering. These smaller objects may be stored, but they'll always be charged at the Frequent Access tier

upvoted 1 times

javitech83 1 year, 3 months ago

oh sorry it states objects are bigger than 128 KB. B is correct
upvoted 1 times

 **ruqui** 10 months, 1 week ago

have you tried to implement B? how do you configure Intelligent Tiering to move objects to a less expensive storage tier after 90 days? and which storage tier is this 'less expensive'? the answer is clearly wrong ... correct answer is D
upvoted 3 times

 **Wajif** 1 year, 3 months ago

S3 Intelligent tiering is used when the access frequency is not known. I think 128KB is a deflector.
upvoted 7 times

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

Selected Answer: D

Right answer is D
upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: D

D is cheapest and managed by S3 Lifecycle policy
A: Not readily available
C: Wrong product
B: No choice of '90 days' so you'll be paying for Intelligent Tiering unnecessarily for files to drop out of frequent access after the first 90 days.
upvoted 1 times

 **Firdous586** 2 months, 2 weeks ago

B is the correct answer Kindly follow the below link for more information as proof
<https://aws.amazon.com/s3/storage-classes/>
upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

So D is the correct answer as IA is cheaper than Intelligent tier.
upvoted 1 times

 **Ruffyit** 3 months, 4 weeks ago

The key reasons:

S3 Lifecycle policies can automatically transition objects from S3 Standard to S3 Standard-IA after 90 days.
S3 Standard provides high performance for frequently accessed newer files.
S3 Standard-IA costs 20-30% less than S3 Standard for infrequently accessed files.
This matches access patterns - high performance for new files, cost savings for older files.
S3 Intelligent Tiering has higher request costs and complexity for this simple access pattern.
S3 Inventory lists objects and their properties but does not directly transition objects.
Lifecycle policies provide automated transitions without manual intervention.

upvoted 1 times

 **wearrexdzw3123** 4 months, 2 weeks ago

Selected Answer: D

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) has a minimum billable object size, which currently is 128KB. This means that even if the stored object is smaller than 128KB, Amazon S3 will charge for a minimum of 128KB of data.
upvoted 1 times

 **Wayne23Fang** 5 months, 2 weeks ago

Selected Answer: B

Very tricky case. Besides all the arguments for both camps. I lean to (B). There is an article about the adoption of Intelligent-Tiering in the recent years to save money. Had the following text is "all files ready", I would picked (D): keeping the most accessed files readily available . for its users. I hope AWS gives "partial credit" for both (B) and (D) regardless which is the MOST cost-effective.

upvoted 1 times

 **pentium75** 3 months ago

How do you 'configure Intelligent Tiering to move objects to a less expensive storage tier after 90 days'? It's called "intelligent" because it moves files intelligently, not after a schedule you specify.
upvoted 2 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: D

Implement an S3 Lifecycle policy that moves the objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.

I would not try to overthink this.

upvoted 1 times

 **Valder21** 6 months, 3 weeks ago

Selected Answer: D

Not B because Intelligent-tiering = unkown patterns

upvoted 1 times

✉ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

The key reasons:

S3 Lifecycle policies can automatically transition objects from S3 Standard to S3 Standard-IA after 90 days.
 S3 Standard provides high performance for frequently accessed newer files.
 S3 Standard-IA costs 20-30% less than S3 Standard for infrequently accessed files.
 This matches access patterns - high performance for new files, cost savings for older files.
 S3 Intelligent Tiering has higher request costs and complexity for this simple access pattern.
 S3 Inventory lists objects and their properties but does not directly transition objects.
 Lifecycle policies provide automated transitions without manual intervention.

upvoted 2 times

✉ **Smart** 8 months ago

Selected Answer: D

As per AWS Best Practices, S3 Intelligent Tier is designed for [unknown & changing] access patterns. Alternatively, if you do know the access pattern, use lifecycle policies.

upvoted 3 times

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

Selected Answer: B

The MOST cheaper option is B, because by choosing:

D) Files older than 90 days will live eternally in the S3 Infrequently access layer at \$0.0125/GB.
 B) Using Intelligent-Tiering files older than 90 days can be moved DIRECTLY to the "Archive access tier" (Glacier instant retrieval) at \$0.004/GB, avoiding/skipping the "S3 Infrequently access layer". The question also seems to be according this assumption as says "and configure it to move objects to a less expensive storage tier after 90 days".

<https://aws.amazon.com/s3/pricing/?nc=sn&loc=4>

upvoted 2 times

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

I am taking back my answer, the right is D) as the "Archive access tier" check present in the "Intelligent-Tiering Archive configurations" is for "S3 Glacier flexible retrieval" which is not instant retrieval.

upvoted 2 times

✉ **pentium75** 3 months ago

How do you 'configure Intelligent Tiering to move objects to a less expensive storage tier after 90 days'? It's called "intelligent" because it moves files intelligently, not after a schedule you specify.

upvoted 2 times

✉ **vini15** 8 months, 2 weeks ago

should be D

upvoted 1 times

✉ **cookieMr** 9 months ago

Selected Answer: B

By using S3 IT, the company can take advantage of automatic cost optimization. IT moves objects between two access tiers: frequent access and infrequent access. In this case, since downloads for ringtones older than 90 days are infrequent, IT will automatically move those objects to the less expensive infrequent access tier, reducing storage costs while keeping the most accessed files readily available.

A is not the most cost-effective solution because it doesn't consider the requirement of keeping the most accessed files readily available. S3 Standard-IA is designed for data that is accessed less frequently, but it still incurs higher costs compared to IT.

C is not the most suitable solution for reducing storage costs. S3 inventory provides a list of objects and their metadata, but it does not offer direct cost optimization features.

D is not the most cost-effective solution because it only moves objects from S3 Standard to S3 Standard-IA after 90 days. It doesn't take advantage of the benefits of IT, which automatically optimizes costs based on access patterns.

upvoted 3 times

✉ **pentium75** 3 months ago

B specifically asks you to 'configure Intelligent Tiering to move objects to a less expensive storage tier after 90 days', how do you do that? It's called "intelligent" because it moves files intelligently, not after a schedule you specify.

upvoted 1 times

✉ **kelvintoys93** 9 months, 3 weeks ago

Selected Answer: D

128kB is just a trap.

It cannot be B because:

1. Intelligent-tiering requires no configuration for class transitions - your option is just whether to opt into Archive/Deep Archive Access tier, which does not make sense for the requirement. Those two classes are cheapest in terms of storage but charges high for retrieval.
2. Nowhere has it mentioned that the access pattern is unpredictable. If we really have to assume, I would rather assume that new songs have higher access frequency. In this case, you don't really benefit from the auto-transition feature that Intel-tier provides. You will be paying the same rate as S3 Standard class + additional fee for using Intel-tiering. Since the req is to have the most cost-efficient solution, D is the answer.

upvoted 2 times

✉️ **kelvintoys93** 9 months, 3 weeks ago

To add to my point above, for intel-tiering to move a file from:

Frequent tier > Infrequent tier - requires object to not be accessed for 30 consecutive days

Infrequent tier > Archive/Deep Archive - requires object to not be accessed for 90 days and above.

Can one guarantee that a new song will not be downloaded for 30 consecutive days in order to take advantage of intel-tier's automated storage class transition? Even if that's the case, there is nothing that user need to "configure" .. B would only be a valid solution if the configuration part is taken out.

<https://aws.amazon.com/s3/storage-classes/intelligent-tiering/>

upvoted 1 times

✉️ **Deansylla** 10 months ago

Selected Answer: B

S3 Intelligent-Tiering is designed to optimize costs by automatically moving objects between two access tiers: frequent access and infrequent access. By moving the files to S3 Intelligent-Tiering, the company can take advantage of the automatic tiering feature to save costs on storage. Initially, the files will be stored in the frequent access tier for quick and easy access. However, since downloads for ringtones older than 90 days are infrequent, after that period, the objects will automatically be moved to the infrequent access tier, which offers a lower storage cost compared to the frequent access tier

upvoted 1 times

✉️ **pentium75** 3 months ago

How do you 'configure Intelligent Tiering to move objects to a less expensive storage tier after 90 days'? It's called "intelligent" because it moves files intelligently, not after a schedule you specify.

upvoted 1 times

Question #154

Topic 1

A company needs to save the results from a medical trial to an Amazon S3 repository. The repository must allow a few scientists to add new files and must restrict all other users to read-only access. No users can have the ability to modify or delete any files in the repository. The company must keep every file in the repository for a minimum of 1 year after its creation date.

Which solution will meet these requirements?

- A. Use S3 Object Lock in governance mode with a legal hold of 1 year.
- B. Use S3 Object Lock in compliance mode with a retention period of 365 days.
- C. Use an IAM role to restrict all users from deleting or changing objects in the S3 bucket. Use an S3 bucket policy to only allow the IAM role.
- D. Configure the S3 bucket to invoke an AWS Lambda function every time an object is added. Configure the function to track the hash of the saved object so that modified objects can be marked accordingly.

Correct Answer: B*Community vote distribution*

elmogy 10 months ago

Selected Answer: B

B,

The key is "No users can have the ability to modify or delete any files" and compliance mode supports that.

I remember it this way: (governance is like government, they set the rules but they can allow some people to break it :D)
upvoted 37 times

Burrito69 4 days, 20 hours ago

I liked that thought of yours.. can you do more of these please? Thank you

upvoted 1 times

Praewwara 3 months ago

Amazon S3 Object Lock

1. Governance mode - Only users with special permissions can overwrite, delete, or alter object lock settings
 2. Compliance mode - No user, including the root user in an AWS account, can overwrite, delete, or alter object lock settings
- upvoted 4 times

Qjb8m9h 1 year, 4 months ago

Answer : B

Reason: Compliance Mode. The key difference between Compliance Mode and Governance Mode is that there are NO users that can override the retention periods set or delete an object, and that also includes your AWS root account which has the highest privileges.

upvoted 20 times

Zerotn3 1 year, 2 months ago

How about: The repository must allow a few scientists to add new files

upvoted 1 times

JayBee65 1 year, 2 months ago

Adding is not the same as changing :)

upvoted 7 times

abhishek2021 10 months ago

Compliance mode controls the object life span after creation.

how this option restricts all scientists from adding new file? please explain.

upvoted 2 times

demigodnyi 1 month, 2 weeks ago

Can someone please explain why the answer is not A. It said that The repository must allow a few scientists to add new files. So, i think some user must have permission to change it.

upvoted 1 times

pentium75 3 months ago

Unsure, B would meet the "must keep every file for a minimum of 1 year" requirement. (In theory C would too if you ignore the root user, but administrators could remove the policy.) But what about the 'a few scientists must be able to add new files'? None of the options mentions permissions for a special group.

upvoted 3 times

awsgeek75 2 months, 1 week ago

agree that something is missing for "some users".

ACD are not going to work flat out so B looks like right answer but with some language issues either in the question or the answer.

upvoted 1 times

LoXoL 2 months, 1 week ago

Agree. It looks like it's missing sth here.

upvoted 1 times

Ruffyit 3 months, 4 weeks ago

Both Compliance & Governance mode protect objects against being deleted or changed. But in Governance mode some people can have special permissions. In this question, no user can delete or modify files; so the answer is Compliance mode only. Neither of these modes restrict user from adding new files.

upvoted 2 times

TariqKipkemei 6 months, 2 weeks ago

Selected Answer: B

Compliance Mode best suits this scenario because once an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened.

upvoted 1 times

Guru4Cloud 7 months, 1 week ago

Selected Answer: B

B) seems to be the right option, because: Both option A) & B) allow to:

- Scientists add new files & other users read-only access.
- Keep files for a minimum of 1 year

Only option B allows to:

- Disable all users the ability to modify or delete any file.

If A) were the correct option some scientists will be able to modify files, as if they were in charge of putting an object lock same permission would allow them to remove the lock and consequently delete the file.

upvoted 2 times

MutiverseAgent 8 months, 1 week ago

Selected Answer: B

B) seems to be the right option, because: Both option A) & B) allow to:

- Scientists add new files & other users read-only access.
- Keep files for a minimum of 1 year

Only option B allows to:

- Disable all users the ability to modify or delete any file.

If A) were the correct option some scientists will be able to modify files, as if they were in charge of putting an object lock same permission would allow them to remove the lock and consequently delete the file.

upvoted 1 times

cookieMr 9 months ago

Selected Answer: B

S3 Object Lock provides the necessary features to enforce immutability and retention of objects in an S3. Compliance mode ensures that the locked objects cannot be deleted or modified by any user, including those with write access. By setting a retention period of 365 days, the company can ensure that every file in the repository is kept for a minimum of 1 year after its creation date.

A does not provide the same level of protection as compliance mode. In governance mode, there is a possibility for authorized users to remove the legal hold, potentially allowing objects to be modified or deleted.

C can restrict users from deleting or changing objects, but it does not enforce the retention period requirement. It also does not provide the same level of immutability and protection against accidental or malicious modifications.

D does not address the requirement of preventing users from modifying or deleting files. It provides a mechanism for tracking changes but does not enforce the desired access restrictions or retention period.

upvoted 3 times

norris81 10 months, 1 week ago

Am I the only one to worry about leap years ?

upvoted 1 times

cheese929 10 months, 4 weeks ago

Selected Answer: B

In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode helps ensure that an object version can't be overwritten or deleted for the duration of the retention period.

In governance mode, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary.

In Governance mode, Objects can be deleted by some users with special permissions, this is against the requirement.

upvoted 2 times

darn 11 months, 1 week ago

Selected Answer: B

its B, legal hold has no retention

upvoted 3 times

✉ **Shrestwt** 11 months, 1 week ago

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

upvoted 1 times

✉ **jaswantn** 11 months, 4 weeks ago

Both Compliance & Governance mode protect objects against being deleted or changed. But in Governance mode some people can have special permissions. In this question, no user can delete or modify files; so the answer is Compliance mode only. Neither of these modes restrict user from adding new files.

upvoted 2 times

✉ **ProfXsamson** 1 year, 1 month ago

B. Compliance mode helps ensure that an object version can't be overwritten or deleted for the duration of the retention period.

upvoted 1 times

✉ **aba2s** 1 year, 2 months ago

Selected Answer: B

users can have the ability to modify or delete any files in the repository ==> Compliance Mode

upvoted 1 times

✉ **aba2s** 1 year, 2 months ago

users cannot have the ability to modify or delete any files in the repository ==> Compliance Mode

upvoted 3 times

✉ **Zerotn3** 1 year, 2 months ago

Selected Answer: A

B would also meet the requirement to keep every file in the repository for at least 1 year after its creation date, as you can specify a retention period of 365 days. However, it would not meet the requirement to restrict all users except a few scientists to read-only access. S3 Object Lock in compliance mode only allows you to specify retention periods and does not have any options for controlling access to objects in the bucket.

To meet all the requirements, you should use S3 Object Lock in governance mode and use IAM policies to control access to the objects in the bucket. This would allow you to specify a legal hold with a retention period of at least 1 year and to restrict all users except a few scientists to read-only access.

upvoted 3 times

✉ **notacert** 11 months, 3 weeks ago

Legal hold needs to be removed manually.

"The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed."

upvoted 1 times

Question #155

Topic 1

A large media company hosts a web application on AWS. The company wants to start caching confidential media files so that users around the world will have reliable access to the files. The content is stored in Amazon S3 buckets. The company must deliver the content quickly, regardless of where the requests originate geographically.

Which solution will meet these requirements?

- A. Use AWS DataSync to connect the S3 buckets to the web application.
- B. Deploy AWS Global Accelerator to connect the S3 buckets to the web application.
- C. Deploy Amazon CloudFront to connect the S3 buckets to CloudFront edge servers.
- D. Use Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application.

Correct Answer: C

Community vote distribution

C (100%)

✉️  **rjam**  1 year, 4 months ago

key :caching
Option C
upvoted 14 times

✉️  **Guru4Cloud**  7 months, 1 week ago

Selected Answer: C

The reasons are:

Amazon CloudFront is a content delivery network (CDN) that caches content at edge locations around the world. Connecting the S3 buckets containing the media files to CloudFront will cache the content at global edge locations. This provides fast reliable access to users everywhere by serving content from the nearest edge location. CloudFront integrates tightly with S3 for secure, durable storage. Global Accelerator improves availability and performance for TCP/UDP traffic, not HTTP-based content delivery. DataSync and SQS are not technologies for a global CDN like CloudFront.

upvoted 5 times

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

Selected Answer: C

Amazon CloudFront to the rescue
upvoted 1 times

✉️  **cookieMr** 9 months ago

Selected Answer: C

CloudFront is a content delivery network (CDN) service provided by AWS. It caches content at edge locations worldwide, allowing users to access the content quickly regardless of their geographic location. By connecting the S3 to CloudFront, the media files can be cached at edge locations, ensuring reliable and fast delivery to users.

A. is a data transfer service that is not designed for caching or content delivery. It is used for transferring data between on-premises storage systems and AWS services.

B. is a service that improves the performance and availability of applications for global users. While it can provide fast and reliable access, it is not specifically designed for caching media files or connecting directly to S3.

D. is a message queue service that is not suitable for caching or content delivery. It is used for decoupling and coordinating message-based communication between different components of an application.

Therefore, the correct solution is option C, deploying CloudFront to connect the S3 to CloudFront edge servers.

upvoted 2 times

✉️  **jacky3123213** 9 months, 2 weeks ago

Global Accelerator does not support Edge Caching
upvoted 1 times

✉️  **Bmarodi** 10 months, 1 week ago

Selected Answer: C

Option C is correct answer.
upvoted 1 times

✉️  **warioverde** 1 year ago

As far as I understand, Global Accelerator does not have caching features, so CloudFront would be the recommended service for that purpose

upvoted 2 times

✉ **Americo32** 1 year, 1 month ago

Selected Answer: C

C correto

upvoted 1 times

✉ **ProfXsamson** 1 year, 1 month ago

C, Caching == Edge location == CloudFront

upvoted 2 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: C

C right answer

upvoted 2 times

✉ **k1kavi1** 1 year, 3 months ago

Selected Answer: C

Agreed

upvoted 1 times

✉ **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

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

Selected Answer: C

Answer is C

upvoted 1 times

Question #156

Topic 1

A company produces batch data that comes from different databases. The company also produces live stream data from network sensors and application APIs. The company needs to consolidate all the data into one place for business analytics. The company needs to process the incoming data and then stage the data in different Amazon S3 buckets. Teams will later run one-time queries and import the data into a business intelligence tool to show key performance indicators (KPIs).

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Use Amazon Athena for one-time queries. Use Amazon QuickSight to create dashboards for KPIs.
- B. Use Amazon Kinesis Data Analytics for one-time queries. Use Amazon QuickSight to create dashboards for KPIs.
- C. Create custom AWS Lambda functions to move the individual records from the databases to an Amazon Redshift cluster.
- D. Use an AWS Glue extract, transform, and load (ETL) job to convert the data into JSON format. Load the data into multiple Amazon OpenSearch Service (Amazon Elasticsearch Service) clusters.
- E. Use blueprints in AWS Lake Formation to identify the data that can be ingested into a data lake. Use AWS Glue to crawl the source, extract the data, and load the data into Amazon S3 in Apache Parquet format.

Correct Answer: AC

Community vote distribution



✉ **Wazhija** 1 year, 5 months ago

Selected Answer: AE

I believe AE makes the most sense
upvoted 13 times

✉ **Six_Fingered_Jose** 1 year, 5 months ago

Selected Answer: AE

yeah AE makes sense, only E is working with S3 here and questions wants them to be in S3
upvoted 11 times

✉ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: AE

A is a given due to Athena and QuickSight option.
Between C and E, the AWS Lake Formation is a more managed solution so it should have less operational overhead than writing Custom AWS Lambda.
AE should be preferred over AC.
upvoted 2 times

✉ **awsgeek75** 2 months, 1 week ago

E is only confusing because of Apache Parquet format (like a grid?) what's the point of that in the context of this question?
upvoted 2 times

✉ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: AE

The reasons are:

AWS Lake Formation and Glue provide automated data lake creation with minimal coding. Glue crawlers identify sources and ETL jobs load to S3.
Athena allows ad-hoc queries directly on S3 data with no infrastructure to manage.
QuickSight provides easy cloud BI for dashboards.
Options C and D require significant custom coding for ETL and queries.
Redshift and OpenSearch would require additional setup and management overhead.
upvoted 6 times

✉ **Mia2009687** 8 months, 3 weeks ago

Selected Answer: AE

It combines data from database and stream data, so data lake needs to be used.
And it wants to do one time query, so Athena is better.
upvoted 2 times

✉ **TTaws** 9 months, 1 week ago

@Golcha once the data comes from different sources then you use GLUE
upvoted 1 times

✉ **Jeeva28** 10 months ago

Selected Answer: AC

Less Overhead with option AC .No need to manage
upvoted 1 times

 **pentium75** 3 months ago

But C moves the data to Redshift while the question says you want it in S3 (and Athena from answer A also needs it in S3).
upvoted 3 times

 **Golcha** 11 months, 2 weeks ago

Selected Answer: AC
No specific use case for GLUE
upvoted 1 times

 **TTaws** 9 months, 1 week ago

once the data comes from different sources then you use GLUE
upvoted 2 times

 **pentium75** 3 months ago

C moves the data to Redshift while the question says you want it in S3 (and Athena from answer A also needs it in S3).
upvoted 2 times

 **TECHNOWARRIOR** 11 months, 2 weeks ago

The Apache Parquet format is a performance-oriented, column-based data format designed for storage and retrieval. It is generally faster for reads than writes because of its columnar storage layout and a pre-computed schema that is written with the data into the files. AWS Glue's Parquet writer offers fast write performance and flexibility to handle evolving datasets. You can use AWS Glue to read Parquet files from Amazon S3 and from streaming sources as well as write Parquet files to Amazon S3. When using AWS Glue to build a data lake foundation, it automatically crawls your Amazon S3 data, identifies data formats, and then suggests schemas for use with other AWS analytic services[1][2][3][4].

upvoted 4 times

 **TECHNOWARRIOR** 11 months, 2 weeks ago

ANSWER - AE:Amazon Athena is the best choice for running one-time queries on streaming data. Although Amazon Kinesis Data Analytics provides an easy and familiar standard SQL language to analyze streaming data in real-time, it is designed for continuous queries rather than one-time queries[1]. On the other hand, Amazon Athena is a serverless interactive query service that allows querying data in Amazon S3 using SQL. It is optimized for ad-hoc querying and is ideal for running one-time queries on streaming data[2].AWS Lake Formation uses as a central place to have all your data for analytics purposes (E). Athena integrate perfect with S3 and can makes queries (A).

upvoted 4 times

 **jramos** 11 months, 3 weeks ago

Selected Answer: AE

AWS Lake Formation uses as a central place to have all your data for analytics purposes (E). Athena integrate perfect with S3 and can makes queries (A).

upvoted 2 times

 **jramos** 11 months, 3 weeks ago

Why S3 in Apache Parquet? <https://aws.amazon.com/about-aws/whats-new/2018/12/amazon-s3-announces-parquet-output-format-for-inventory/>
upvoted 1 times

 **JiyuKim** 1 year, 1 month ago

Can anyone please explain me why B cannot be an answer?
upvoted 5 times

 **Shrestwt** 11 months, 1 week ago

Kinesis Data Analytics is designed for continuous queries rather than one-time queries.
upvoted 5 times

 **ashishvineetko** 1 year, 2 months ago

can anyone help me in below question
36. A company has a Java application that uses Amazon Simple Queue Service (Amazon SOS) to parse messages. The application cannot parse messages that are large on 256KB size. The company wants to implement a solution to give the application the ability to parse messages as large as 50 MB.

Which solution will meet these requirements with the FEWEST changes to the code?

- a) Use the Amazon SOS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.
- b) Use Amazon EventBridge to post large messages from the application instead of Aaron SOS
- c) Change the limit in Amazon SQS to handle messages that are larger than 256 KB
- d) Store messages that are larger than 256 KB in Amazon Elastic File System (Amazon EFS) Configure Amazon SQS to reference this location in the messages.

upvoted 1 times

 **skondey** 1 year, 1 month ago

I will do "A" as well.
upvoted 1 times

 **ProfXsamson** 1 year, 1 month ago

A would probably be the best answer. Sqs extended client library is for Java apps.

upvoted 1 times

 **bullrem** 1 year, 2 months ago

Selected Answer: DE

I believe DE makes the most sense

upvoted 1 times

 **pentium75** 3 months ago

Why use OpenSearch service?

upvoted 2 times

 **ShinobiGrappler** 1 year, 2 months ago

Selected Answer: AE

stored in s3 -> data lake -> athena (process the SQL parquet format)-> quicksight visualize

upvoted 5 times

 **Zerotn3** 1 year, 2 months ago

Selected Answer: BE

While Amazon Athena is a fully managed service that makes it easy to analyze data stored in Amazon S3 using SQL, it is primarily designed for running ad-hoc queries on data stored in Amazon S3. It may not be the best choice for running one-time queries on streaming data, as it is not designed to process data in real-time.

Additionally, using Amazon Athena for one-time queries on streaming data could potentially lead to higher operational overhead, as you would need to set up and maintain the necessary infrastructure to stream the data into Amazon S3, and then query the data using Athena.

Using Amazon Kinesis Data Analytics, as mentioned in option B, would be a better choice for running one-time queries on streaming data, as it is specifically designed to process data in real-time and can automatically scale to match the incoming data rate.

upvoted 2 times

 **JayBee65** 1 year, 2 months ago

"Company needs to consolidate all the data into one place" -> S3 bucket, which is happening in E, which means Athena would not have an issue, so A is ok.

upvoted 4 times

 **jainparag1** 1 year, 2 months ago

Absolutely, querying data is after staging and so Athena fits perfectly.

upvoted 1 times

 **techhb** 1 year, 3 months ago

Selected Answer: AE

C can work it out ,but has additional overhead.

upvoted 3 times

Question #157

Topic 1

A company stores data in an Amazon Aurora PostgreSQL DB cluster. The company must store all the data for 5 years and must delete all the data after 5 years. The company also must indefinitely keep audit logs of actions that are performed within the database. Currently, the company has automated backups configured for Aurora.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Take a manual snapshot of the DB cluster.
- B. Create a lifecycle policy for the automated backups.
- C. Configure automated backup retention for 5 years.
- D. Configure an Amazon CloudWatch Logs export for the DB cluster.
- E. Use AWS Backup to take the backups and to keep the backups for 5 years.

Correct Answer: BE

Community vote distribution



✉ **JayBee65** 1 year, 2 months ago

I tend to agree D and E...

A - Manual task that can be automated, so why make life difficult?
 B - The maximum retention period is 35 days, so would not help
 C - The maximum retention period is 35 days, so would not help
 D - Only option that deals with logs, so makes sense
 E - Partially manual but only option that achieves the 5 year goal

upvoted 37 times

✉ **aadityaravi8** 8 months, 3 weeks ago

100% agree

upvoted 6 times

✉ **kmaneith** 1 year, 3 months ago

Selected Answer: DE

dude trust me

upvoted 19 times

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

<https://medium.com/@darekhale91/how-to-pass-amazon-saa-c03-exam-dumps-2023-583619ddbcc8>

upvoted 1 times

✉ **JayBee65** 1 year, 2 months ago

No, please show your reasoning, you may be wrong. Remember, no one thinks they are wrong, but some always are :)

upvoted 13 times

✉ **Priyanshugpt486** 6 months ago

hehe... hehe

upvoted 1 times

✉ **jjcode** 1 month, 1 week ago

My thoughts:

1. AWS backups is designed to make back ups
2. "configure backup retention for 5 years" with what? a script? maybe AWS backups???? are the back ups done with DD and stored in S3? i cannot trust this answer
3. "Take a manual snapshot of the DB cluster" this is not an amazon best practice they want us to use their tools AWS backups
4. "create a life cycle policy" assuming the back ups are stored in S3 (which is not a best practice) cannot trust this

that leaves D and E

upvoted 1 times

✉ **Ruffyit** 3 months, 4 weeks ago

D AND E- makes more sense as we automate backups in Aurora DB

- Export data to CloudWatch to capture all log events and configure CloudWatch to retain logs indefinitely.

upvoted 1 times

✉ **awashenko** 5 months, 2 weeks ago

Selected Answer: DE

D and E.

A would work as well, but D is the better option as its automated.
 E is the only option that gets you to the 5 year retention.

upvoted 1 times

 **kambarami** 6 months, 2 weeks ago

D AND E- makes more sense as we automate backups in Aurora DB
 - Export data to CloudWatch to capture all log events and configure CloudWatch to retain logs indefinitely.

upvoted 1 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: DE
 DE makes more sense
 upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: CD
 The reasons are:

Configuring the automated backups for the Aurora PostgreSQL DB cluster to retain backups for 5 years will meet the requirement to store all data for that duration.

Exporting the database logs to CloudWatch Logs will capture the audit logs of actions performed in the database. CloudWatch Logs retention can be configured to store logs indefinitely.

This meets the need to keep audit logs available beyond the 5 year data retention period.

Additional manual snapshots or using AWS Backup for backups is not necessary since automated backups are already enabled.

A lifecycle policy is useful for transitioning storage classes but does not apply here for a set 5 year retention.

upvoted 2 times

 **neverdie** 1 year ago

Selected Answer: AD
 Automated backup is limited 35 days
 upvoted 3 times

 **Training4aBetterLife** 1 year, 2 months ago

Selected Answer: DE
 Previously, you had to create custom scripts to automate backup scheduling, enforce retention policies, or consolidate backup activity for manual Aurora cluster snapshots, especially when coordinating backups across AWS services. With AWS Backup, you gain a fully managed, policy-based backup solution with snapshot scheduling and snapshot retention management. You can now create, manage, and restore Aurora backups directly from the AWS Backup console for both PostgreSQL-compatible and MySQL-compatible versions of Aurora.
 To get started, select an Amazon Aurora cluster from the AWS Backup console and take an on-demand backup or simply assign the cluster to a backup plan.

upvoted 4 times

 **Training4aBetterLife** 1 year, 2 months ago

https://aws.amazon.com/about-aws/whats-new/2020/06/amazon-aurora-snapshots-can-be-managed-via-aws-backup/?nc1=h_ls
 upvoted 2 times

 **Zerotn3** 1 year, 2 months ago

Selected Answer: DE
 A is not a valid option for meeting the requirements. A manual snapshot of the DB cluster is a point-in-time copy of the data in the cluster. While taking manual snapshots can be useful for creating backups of the data, it is not a reliable or efficient way to meet the requirement of storing all the data for 5 years and deleting it after 5 years. It would be difficult to ensure that manual snapshots are taken regularly and retained for the required period of time. It is recommended to use a fully managed backup service like AWS Backup, which can automate and centralize the process of taking and retaining backups.

upvoted 3 times

 **Zerotn3** 1 year, 2 months ago

Sorry, B and E that correct
 B. Create a lifecycle policy for the automated backups.
 This would ensure that the backups taken using AWS Backup are retained for the desired period of time.

upvoted 1 times

 **JayBee65** 1 year, 2 months ago

I think a lifecycle policy would only keep backups for 35 days
 upvoted 3 times

 **awashenko** 5 months, 2 weeks ago

Thats not correct (i thought it was but I went and looked it up) Aurora only keeps backups from 1-35 days.
 upvoted 1 times

 **techhb** 1 year, 3 months ago

Selected Answer: DE
 D and E only

upvoted 2 times

✉ **Chirantan** 1 year, 3 months ago

AD

is correct as you can keep backup of snapshot indifferently.

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: DE

D and E

upvoted 2 times

✉ **Qjb8m9h** 1 year, 3 months ago

Aurora backups are continuous and incremental so you can quickly restore to any point within the backup retention period. No performance impact or interruption of database service occurs as backup data is being written. You can specify a backup retention period, from 1 to 35 days, when you create or modify a DB cluster.

If you want to retain a backup beyond the backup retention period, you can also take a snapshot of the data in your cluster volume. Because Aurora retains incremental restore data for the entire backup retention period, you only need to create a snapshot for data that you want to retain beyond the backup retention period. You can create a new DB cluster from the snapshot.

upvoted 4 times

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

Selected Answer: DE

D is the only one that resolves the logging situation

"automated backup" = AWS Backup

<https://aws.amazon.com/backup/faqs/?nc=sn&loc=6>

AWS Backup provides a centralized console, automated backup scheduling, backup retention management, and backup monitoring and alerting.

AWS Backup offers advanced features such as lifecycle policies to transition backups to a low-cost storage tier. It also includes backup storage and encryption independent from its source data, audit and compliance reporting capabilities with AWS Backup Audit Manager, and delete protection with AWS Backup Vault Lock.

upvoted 2 times

✉ **Qjb8m9h** 1 year, 3 months ago

AD

Reason: When creating Aurora back up, you will need to specify the retention period which is between 1-35days. This does not meet the 5years retention requirement in this case.

Hence taking a snap manual snap shot is the best solution.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Backups.html>

upvoted 2 times

Question #158

Topic 1

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand streaming?

- A. Amazon CloudFront
- B. AWS Global Accelerator
- C. Amazon Route 53
- D. Amazon S3 Transfer Acceleration

Correct Answer: A

Community vote distribution



✉️ **Nigma** 1 year, 4 months ago

A is right

You can use CloudFront to deliver video on demand (VOD) or live streaming video using any HTTP origin

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

upvoted 32 times

✉️ **mr123dd** 2 months, 2 weeks ago

Selected Answer: A

website = http = cloudfront, if it is UDP, then global accelerator

upvoted 5 times

✉️ **lanceshen** 1 week, 6 days ago

Selected Answer: B

Option A (Amazon CloudFront) is a content delivery network (CDN) service that can improve the performance of on-demand streaming by caching and delivering content from edge locations. While it can accelerate on-demand streaming, it may not provide the same level of optimization for real-time streaming as AWS Global Accelerator.

upvoted 2 times

✉️ **MrPCarrot** 1 month, 3 weeks ago

A is pperfect <https://d1.awsstatic.com/whitepapers/amazon-cloudfront-for-media.pdf>

upvoted 2 times

✉️ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html>

CloudFront solves the problem of streaming over Amazon CDN on global scale.

"B" AWS Global Accelerator won't be suitable for streaming from web server as it does not provide edge caching like CDN. Global Accelerator only points the user to nearest functioning node which is helpful for real-time streaming but not best for on-demand.

upvoted 1 times

✉️ **viru** 3 months, 1 week ago

Selected Answer: A

<https://aws.amazon.com/cloudfront/streaming/>

upvoted 2 times

✉️ **yayaayzo** 3 months, 2 weeks ago

A IS THE RIGHT ANS

. Amazon CloudFront is a content delivery network (CDN) service offered by AWS. It is designed to deliver data, including videos and other media files, with low latency and high transfer speeds. This is a suitable option for optimizing website performance, especially for streaming content globally.

upvoted 1 times

✉️ **MiniYang** 3 months, 3 weeks ago

Selected Answer: B

Although CloudFront is a content delivery network (CDN) that can provide low-latency and high-performance content delivery, its performance for real-time streaming and on-demand streaming may not be as professional as AWS Global Accelerator

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

<https://aws.amazon.com/global-accelerator/>

"AWS Global Accelerator is a networking service that helps you improve the availability, performance, and security of your public applications. 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."

It is Anycast which connect user to closest resource on your server like ALB etc or regional services.

CloudFront is CDN and pushes your content to edge locations near the user. This solves all issues of latency and performance

upvoted 1 times

 **Ruffyit** 3 months, 4 weeks ago

You can use CloudFront to deliver video on demand (VOD) or live streaming video using any HTTP origin

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

upvoted 2 times

 **mhka1988** 5 months, 1 week ago

Selected Answer: A

CloudFront offers several options for streaming your media to global viewers—both pre-recorded files and live events.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/IntroductionUseCases.html#IntroductionUseCasesStreaming>

For video on demand (VOD) streaming, you can use CloudFront to stream in common formats such as MPEG DASH, Apple HLS, Microsoft Smooth Streaming, and CMAF, to any device.

For broadcasting a live stream, you can cache media fragments at the edge, so that multiple requests for the manifest file that delivers the fragments in the right order can be combined, to reduce the load on your origin server.

upvoted 2 times

 **OlehKom** 5 months, 2 weeks ago

Selected Answer: B

Please stop posting answers from ChatGPT.

"The event is expected to attract a global online audience."

Global Accelerator is a service that accelerates traffic to Google Cloud services from users around the world. If you're looking to stream audio content to a global audience, Global Accelerator may be more suitable due to its ability to route traffic through the nearest edge locations and reduce latency. However, if you're looking to stream audio content from a single source to a local audience, CloudFront may be a better option.

upvoted 3 times

 **pentium75** 3 months ago

CloudFront for "local audience"???

upvoted 1 times

 **awashenko** 5 months, 2 weeks ago

Selected Answer: A

Was between A and B here but this link convinced me that A would be correct.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/IntroductionUseCases.html#IntroductionUseCasesStreaming>

upvoted 2 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: A

Amazon CloudFront is a content delivery network (CDN) service that helps you distribute your static and dynamic content quickly and reliably with high speed.

upvoted 1 times

 **Chiquitabandita** 6 months, 3 weeks ago

chatgpt went with cloudfront on this question, so answer A

upvoted 3 times

 **coolkidsclubvip** 6 months, 4 weeks ago

Selected Answer: B

<https://aws.amazon.com/cn/blogs/networking-and-content-delivery/how-flowplayer-improved-live-video-ingest-with-aws-global-accelerator/>

upvoted 3 times

 **Guru4Cloud** 7 months, 1 week ago

The reasons are:

CloudFront is a content delivery network (CDN) that caches content at edge locations around the world.

Caching the video content globally brings it closer to viewers, reducing latency.

This improves performance for both live streaming and on-demand playback for the global audience.

Route 53 provides DNS resolution but does not cache content locally.

Global Accelerator improves TCP traffic routing performance but is not a caching CDN.

S3 Transfer Acceleration optimizes uploads to S3 over long distances but does not help with content delivery.

upvoted 2 times

 **Chan1010** 8 months ago

Selected Answer: B

Global Accelerator good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP

upvoted 2 times

 **fageroff** 5 months ago

a video streaming is udp traffic

upvoted 1 times

Question #159

Topic 1

A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application's traffic recently spiked due to fraudulent requests from botnets.

Which steps should a solutions architect take to block requests from unauthorized users? (Choose two.)

- A. Create a usage plan with an API key that is shared with genuine users only.
- B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.
- C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.
- D. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.
- E. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.

Correct Answer: CD

Community vote distribution



✉️ **jdr75** 11 months, 3 weeks ago

Selected Answer: CE

C) WAF has bot identification and remedial tools, so it's CORRECT.

A) remember the question : "...block requests from unauthorized users?" -- an api key is involved in a authorization process. It's not the more secure process, but it's better than an totally anonymous process. If you don't know the key, you can't authenticate. So the bots, at least the first days/weeks could not access the service (at the end they'll do, cos' the key will be spread informally). So it's CORRECT.

B) Implement a logic in the Lambda to detect fraudulent ip's is almost impossible, cos' it's a dynamic and changing pattern that you cannot handle easily.

D) creating a rol is not going to imply be more protected from unauth. request, because a rol is a "principal", it's not involved in the authorization process.

upvoted 8 times

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

Don't use API keys for authentication or authorization to control access to your APIs. If you have multiple APIs in a usage plan, a user with a valid API key for one API in that usage plan can access all APIs in that usage plan. Instead, to control access to your API, use an IAM role, a Lambda authorizer, or an Amazon Cognito user pool.

upvoted 1 times

✉️ **pentium75** 3 months ago

E "An IAM role for EACH (!) user ATTEMPTING (!) to access the API"? Hello no.

upvoted 3 times

✉️ **MrPCarrot** 1 month, 3 weeks ago

C and D are the perfect answers

upvoted 2 times

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

Don't use API keys for authentication or authorization to control access to your APIs. If you have multiple APIs in a usage plan, a user with a valid API key for one API in that usage plan can access all APIs in that usage plan. Instead, to control access to your API, use an IAM role, a Lambda authorizer, or an Amazon Cognito user pool.

upvoted 1 times

✉️ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: CD

I'll throw a curveball over here. "C" is a given as WAF rules can target malicious usage. For example:

<https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-waf-ip-reputation.html>

"D" Convert existing public API to a private API. This part is same as A. The additional bit over here is to change the DNS record to a new API endpoint which blocks the requests from unauthorised users also. The unauthorised users will not be redirected from public to private API endpoint. I am assuming that the public API endpoint will be used for authorisation and only authorised users will be redirected to private endpoint. This is more robust as the actual API (private endpoint) never gets hit with requests from unauthorised bots and WAF redirects it back to public URL.

Happy to be corrected and challenged

upvoted 4 times

✉️ **sidharthwader** 3 weeks, 1 day ago

It's a globally published API if you make it private how do other people access it ? A would be the better solution than D
upvoted 1 times

ale_brd_ 3 months, 2 weeks ago

Selected Answer: AC

The combination of using an API key and implementing an AWS WAF rule provides the most comprehensive and effective way to block requests from unauthorized users and protect the company's serverless application from botnet attacks.
upvoted 2 times

MiniYang 3 months, 3 weeks ago

Selected Answer: CE

A. Create plans using API keys shared only with real users: While using API keys is a standard way to control access to APIs, using API keys alone may not completely prevent attacks from botnets. Malicious request.

B. Incorporate logic in the Lambda function to ignore requests from fraudulent IP addresses: This may be a solution, but filtering that relies more on IP addresses may not be as flexible as using AWS WAF.

D. Convert an existing public API to a private API. Update DNS records to redirect users to the new API endpoint: This approach makes the API private, but requires user redirects and may inconvenience existing users.

upvoted 1 times

Ruffyit 3 months, 4 weeks ago

C) WAF has bot identification and remedial tools, so it's CORRECT.

A) remember the question : "...block requests from unauthorized users?" -- an api key is involved in a authorization process. It's not the more secure process, but it's better than an totally anonymous process. If you don't know the key, you can't authenticate. So the bots, at least the first days/weeks could not access the service (at the end they'll do, cos' the key will be spread informally). So it's CORRECT.

upvoted 1 times

awashenko 5 months, 2 weeks ago

Selected Answer: AC

Agree A and C

I don't see how E is feasible as its a public API. How would you create an IAM role for each user?

upvoted 4 times

TariqKipkemei 6 months, 2 weeks ago

Selected Answer: AC

AWS WAF rule to target and filter out malicious requests and API key to authorize users.

upvoted 1 times

Guru4Cloud 7 months, 1 week ago

Selected Answer: AC

The reasons are:

An API key with a usage plan limits access to only authorized apps and users. This prevents general public access.

WAF rules can identify and block malicious bot traffic through pattern matching and IP reputation lists.

Together, the API key and WAF provide preventative and detective controls against unauthorized requests.

The other options add complexity or are reactive. IAM roles per user is not feasible for a public API.

Ignoring requests in Lambda and changing DNS are response actions after an attack.

upvoted 2 times

zjcorpuz 8 months ago

AC

it's essential to note that while API keys are commonly associated with private APIs, they can also be used in conjunction with public APIs. In some cases, even public APIs may require API keys to control usage and monitor how the API is being utilized. The API provider might enforce usage limits, track API usage, or monitor for potential misuse, all of which can be managed effectively using API keys.

In summary, API keys are not exclusive to private APIs and can be used for both private and public APIs, depending on the specific requirements and use case of the API provider.

upvoted 1 times

MutiverseAgent 8 months, 1 week ago

Selected Answer: AC

Why option C) vs option E)

- It's simpler

- We want to protect general access to the API and not granular method/user access. The API is already public so If a user API key is in several usage plans that is not a problem (The API is currently public). The objective is to protect API from abuse from malicious internet users and to NOT protect granular method/user access from users that are using the API in the correct way.

upvoted 2 times

Mia2009687 8 months, 3 weeks ago

Selected Answer: CE

Important

Don't use API keys for authentication or authorization for your APIs. If you have multiple APIs in a usage plan, a user with a valid API key for one API in that usage plan can access all APIs in that usage plan. Instead, use an IAM role, a Lambda authorizer, or an Amazon Cognito user pool.

upvoted 2 times

✉️ **Abrar2022** 9 months, 3 weeks ago

Selected Answer: AC

If you're wondering why A. It's because you can configure usage plans and API keys to allow customers to access selected APIs, and begin throttling requests to those APIs based on defined limits and quotas. As for C. It's because AWS WAF has bot detection capabilities.

upvoted 2 times

✉️ **sachin** 1 year ago

It should be A and C

But API Key alone can not help

API keys are alphanumeric string values that you distribute to application developer customers to grant access to your API. You can use API keys together with Lambda authorizers, IAM roles, or Amazon Cognito to control access to your APIs.

upvoted 1 times

✉️ **Steve_4542636** 1 year ago

Selected Answer: CE

Here <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html> it says this:

Don't use API keys for authentication or authorization for your APIs. If you have multiple APIs in a usage plan, a user with a valid API key for one API in that usage plan can access all APIs in that usage plan. Instead, use an IAM role, a Lambda authorizer, or an Amazon Cognito user pool.

API keys are intended for software developers wanting to access an API from their application. This link then goes on to say an IAM role should be used instead.

upvoted 1 times

✉️ **Steve_4542636** 1 year ago

Nevermind my answer. I switch it to A/C because the question states the application is *using* the API Gateway so A will make sense

upvoted 1 times

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

Selected Answer: AC

A/C for security to prevent anonymous access

upvoted 3 times

Question #160

Topic 1

An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format. The company is evaluating a disaster recovery solution to back up the data. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days.

Which solution meets these requirements MOST cost-effectively?

- A. Amazon OpenSearch Service (Amazon Elasticsearch Service)
- B. Amazon S3 Glacier
- C. Amazon S3 Standard
- D. Amazon RDS for PostgreSQL

Correct Answer: C

Community vote distribution



✉ **babaxoxo** 1 year, 4 months ago

Selected Answer: C

Ans C:

Cost-effective solution with milliseconds of retrieval -> it should be s3 standard

upvoted 11 times

✉ **pentium75** 3 months ago

Selected Answer: C

Only Glacier class that would meet the requirement is Instant Retrieval, but it has 90 days minimum storage time which would kill the cost savings.

upvoted 4 times

✉ **xdkonorek2** 4 months, 2 weeks ago

Selected Answer: B

300 MB / month storage without retrieval when file is single 300 MB file:

S3 Standard cost (Monthly): 0.01 USD

S3 Standard cost (Upfront): 0.00 USD

S3 Glacier Instant Retrieval cost (Monthly): 0.00 USD

if it was 3GB:

3 GB / month storage without retrieval when file is single 3GB file:

S3 Standard cost (Monthly): 0.07 USD

S3 Standard cost (Upfront): 0.00 USD

S3 Glacier Instant Retrieval cost (Monthly): 0.01 USD

When assumed no retrieval is required because it's DR solution, and it's a single file, Glacier Instant Retrieval wins, and when they mention S3 glacier we must choose one of the sub-category

upvoted 1 times

✉ **xdkonorek2** 4 months, 2 weeks ago

but if 300 MB is divided into smaller files situation changes which is probably the case..

300 MB / month storage without retrieval when files are 600x0.5MB :

S3 Standard cost (Monthly): 0.01 USD

S3 Standard cost (Upfront): 0.00 USD

S3 Glacier Instant Retrieval cost (Monthly): 0.01 USD

S3 Glacier Instant Retrieval cost (Upfront): 0.02 USD

3 GB / month storage without retrieval when files are 6000x0.5 MB file:

S3 Standard cost (Monthly): 0.10 USD

S3 Standard cost (Upfront): 0.03 USD

S3 Glacier Instant Retrieval cost (Monthly): 0.13 USD

S3 Glacier Instant Retrieval cost (Upfront): 0.25 USD

upvoted 4 times

✉ **pentium75** 3 months ago

Only Glacier Instant Retrieval (which is not mentioned in B) would meet the access requirement, but "Objects that are archived to S3 Glacier Instant Retrieval and S3 Glacier Flexible Retrieval are charged for a minimum storage duration of 90 days."

upvoted 2 times

 **Its_SaKar** 6 months, 2 weeks ago

Selected Answer: C

Answer is not B because S3 glacier and S3 glacier instant storage are two different types of storage class. So, answer here is C: S3 standard upvoted 2 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: C

Data must be accessible in milliseconds and must be kept for 30 days = Amazon S3 Standard
upvoted 1 times

 **chanchal133** 7 months ago

Selected Answer: C

ANS - C
upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: C

The reasons are:

S3 Standard provides high durability and availability for storage
It allows millisecond access to retrieve objects
Objects can be stored for any duration, meeting the 30 day retention need
Storage costs are low, around \$0.023 per GB/month
OpenSearch and RDS require running and managing a cluster for DR storage
Glacier has lower cost but retrieval time is too high at 3-5 hours
S3 Standard's simplicity, high speed access, and low cost make it optimal for this small DR dataset that needs to be accessed quickly
upvoted 2 times

 **Nazmul123** 8 months ago

Selected Answer: C

<https://aws.amazon.com/s3/storage-classes/glacier/instant-retrieval/>
upvoted 1 times

 **pentium75** 3 months ago

Not mentioned in B, and 90 days minimum storage time.
upvoted 1 times

 **cookieMr** 9 months ago

S3 Standard is a highly durable and scalable storage option suitable for backup and disaster recovery purposes. It offers millisecond access to data when needed and provides durability guarantees. It is also cost-effective compared to other storage options like OpenSearch Service, S3 Glacier, and RDS for PostgreSQL, which may have higher costs or longer access times for retrieving the data.

A. OpenSearch Service (Elasticsearch Service): While it offers fast data retrieval, it may incur higher costs compared to storing data directly in S3, especially considering the amount of data being generated.

B. S3 Glacier: While it provides long-term archival storage at a lower cost, it does not meet the requirement of immediate access in milliseconds. Retrieving data from Glacier typically takes several hours.

D. RDS for PostgreSQL: While it can be used for data storage, it may be overkill and more expensive for a backup and disaster recovery solution compared to S3 Standard, which is more suitable and cost-effective for storing and retrieving data.

upvoted 2 times

 **joehong** 9 months, 2 weeks ago

Selected Answer: B

<https://aws.amazon.com/s3/storage-classes/glacier/instant-retrieval/>
upvoted 3 times

 **pentium75** 3 months ago

"Objects that are archived to S3 Glacier Instant Retrieval and S3 Glacier Flexible Retrieval are charged for a minimum storage duration of 90 days." Also Instant Retrieval is not mentioned in B.
upvoted 1 times

 **KZM** 1 year, 1 month ago

A. Incorrect

Amazon OpenSearch Service (Amazon Elasticsearch Service) is designed for full-text search and analytics, but it may not be the most cost-effective solution for this use case

B. Incorrect

S3 Glacier is a cold storage solution that is designed for long-term data retention and infrequent access.

C. Correct

S3 standard is cost-effective and meets the requirement. S3 Standard allows for data retention for a specific number of days.

D. PostgreSQL is a relational database service and may not be the most cost-effective solution.

upvoted 3 times

 **ngochieu276** 1 year, 2 months ago

Selected Answer: B

S3 Glacier Instant Retrieval – Use for archiving data that is rarely accessed and requires milliseconds retrieval.

<https://docs.aws.amazon.com/amazonglacier/latest/dev/introduction.html>

upvoted 3 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

✉ **lapaki** 1 year, 3 months ago

Selected Answer: C

JSON is object notation. S3 stores objects.

upvoted 1 times

✉ **hpipit** 1 year, 3 months ago

Selected Answer: C

c IS correct

upvoted 1 times

✉ **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

✉ **sdasdawa** 1 year, 4 months ago

Selected Answer: C

IMHO

Normally ElasticSearch would be ideal here, however as question states "Most cost-effective"

S3 is the best choice in this case

upvoted 3 times

✉ **Aamee** 1 year, 3 months ago

ElasticSearch is a search service, the question states here about the backup service reqd. for the DR scenario.

upvoted 3 times

Question #161

Topic 1

A company has a small Python application that processes JSON documents and outputs the results to an on-premises SQL database. The application runs thousands of times each day. The company wants to move the application to the AWS Cloud. The company needs a highly available solution that maximizes scalability and minimizes operational overhead.

Which solution will meet these requirements?

- A. Place the JSON documents in an Amazon S3 bucket. Run the Python code on multiple Amazon EC2 instances to process the documents. Store the results in an Amazon Aurora DB cluster.
- B. Place the JSON documents in an Amazon S3 bucket. Create an AWS Lambda function that runs the Python code to process the documents as they arrive in the S3 bucket. Store the results in an Amazon Aurora DB cluster.
- C. Place the JSON documents in an Amazon Elastic Block Store (Amazon EBS) volume. Use the EBS Multi-Attach feature to attach the volume to multiple Amazon EC2 instances. Run the Python code on the EC2 instances to process the documents. Store the results on an Amazon RDS DB instance.
- D. Place the JSON documents in an Amazon Simple Queue Service (Amazon SQS) queue as messages. Deploy the Python code as a container on an Amazon Elastic Container Service (Amazon ECS) cluster that is configured with the Amazon EC2 launch type. Use the container to process the SQS messages. Store the results on an Amazon RDS DB instance.

Correct Answer: D

Community vote distribution



✉ **babaxoxo** Highly Voted 1 year, 4 months ago

Selected Answer: B

solution should remove operation overhead -> s3 -> lambda -> aurora
upvoted 11 times

✉ **markw92** 9 months, 1 week ago

Aurora supports mysql and postgresql but question has database sql server. So, that eliminates B. So, the other logical answer is D. IMHO. Btw, i also thought the answer is B and started re-reading question carefully.

upvoted 3 times

✉ **JIJIJIXI** 5 months, 4 weeks ago

sql database, not sql server
upvoted 4 times

✉ **Zerotn3** Highly Voted 1 year, 2 months ago

Selected Answer: B

By placing the JSON documents in an S3 bucket, the documents will be stored in a highly durable and scalable object storage service. The use of AWS Lambda allows the company to run their Python code to process the documents as they arrive in the S3 bucket without having to worry about the underlying infrastructure. This also allows for horizontal scalability, as AWS Lambda will automatically scale the number of instances of the function based on the incoming rate of requests. The results can be stored in an Amazon Aurora DB cluster, which is a fully-managed, high-performance database service that is compatible with MySQL and PostgreSQL. This will provide the necessary durability and scalability for the results of the processing.

upvoted 9 times

✉ **Anantvir** Most Recent 2 months, 3 weeks ago

Guys I have a question.
We dont know how long the processing of JSON documents is going to take. What if that processing takes more than 15 min ? Lambda can run only for 15 correct ? Based on this the answer could be D

Please correct my understanding.

upvoted 1 times

✉ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: B

"D" has a lot of moving parts and more operational overhead even if each part is a managed service in itself. Also, if something can be done with Lambda, don't use an EC2 instance in any form as it always increases operational overhead (compared to Lambda).
upvoted 2 times

✉ **David_Ang** 5 months, 1 week ago

Selected Answer: B

"D" is just like the most complex one, sometimes the admin make mistakes and don't realize. Lambda is a service made for this

upvoted 1 times

✉ **Mandar15** 6 months ago

Selected Answer: B

B is correc

upvoted 1 times

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

Selected Answer: B

Main requirement is: 'scalability and minimized operational overhead' = serverless = Amazon S3 bucket, AWS Lambda function, Amazon Aurora DB cluster

upvoted 1 times

✉ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

- Using Lambda functions triggered by S3 events allows the Python code to automatically scale up and down based on the number of incoming JSON documents. This provides high availability and maximizes scalability.
- Storing the results in an Amazon Aurora DB cluster provides a managed, scalable, and highly available database.
- This serverless approach minimizes operational overhead since Lambda and Aurora handle provisioning infrastructure, deploying code, monitoring, patching, etc.

upvoted 2 times

✉ **aadityaravi8** 8 months, 3 weeks ago

The answer is B. Place the JSON documents in an Amazon S3 bucket. Create an AWS Lambda function that runs the Python code to process the documents as they arrive in the S3 bucket. Store the results in an Amazon Aurora DB cluster.

This solution is highly available because Lambda functions are automatically scaled up or down based on the number of requests they receive. It is also scalable because you can easily add more Lambda functions to process more documents. Finally, it minimizes operational overhead because you do not need to manage any EC2 instances.

upvoted 1 times

✉ **cookieMr** 9 months ago

Selected Answer: B

Using Lambda eliminates the need to manage and provision servers, ensuring scalability and minimizing operational overhead. S3 provides durable and highly available storage for the JSON documents. Lambda can be triggered automatically whenever new documents are added to the S3 bucket, allowing for real-time processing. Storing the results in an Aurora DB cluster ensures high availability and scalability for the processed data. This solution leverages serverless architecture, allowing for automatic scaling and high availability without the need for managing infrastructure, making it the most suitable choice.

- A. This option requires manual management and scaling of EC2 instances, resulting in higher operational overhead and complexity.
- C. This approach still involves manual management and scaling of EC2 instances, increasing operational complexity and overhead.
- D. This solution requires managing and scaling an ECS cluster, adding operational overhead and complexity. Utilizing SQS adds complexity to the system, requiring custom handling of message consumption and processing in the Python code.

upvoted 3 times

✉ **Bmarodi** 10 months ago

Selected Answer: B

Keywords here are : "maximizes scalability and minimizes operational overhead, hence option B is correct answer.

upvoted 1 times

✉ **channn** 11 months, 2 weeks ago

Selected Answer: D

i vote for D as 'on-premises SQL database' is not mysql/postgre which can replace by aurora

upvoted 2 times

✉ **pentium75** 3 months ago

Why not? It's a "SQL database", NOT necessarily Microsoft SQL Server. But even if it would be SQL server, that could be migrated to Aurora.

upvoted 1 times

✉ **perception** 1 year ago

does somebody had contributor access and want to share. i would really appreciate it.

here's my email

367501tab@gmail.com

Thanks

upvoted 1 times

✉ **kerin** 1 year, 1 month ago

B is the best option. <https://aws.amazon.com/rds/aurora/>

upvoted 1 times

✉ **mp165** 1 year, 2 months ago

Selected Answer: B

agree...B is the best option S3, Lambda , Aurora.

upvoted 1 times

✉️ **techhb** 1 year, 3 months ago

Selected Answer: B

Choosing B as "The company needs a highly available solution that maximizes scalability and minimizes operational overhead"
upvoted 1 times

✉️ **studis** 1 year, 3 months ago

B is tempting but this sentence "runs thousands of times each day." If we use lambda as in B, won't this incur a high bill at the end?
upvoted 1 times

✉️ **techhb** 1 year, 3 months ago

Agree, but question doesn't have Cost as criteria to choose solution. Criteria is "The company needs a highly available solution that maximizes scalability and minimizes operational overhead". Hence B

upvoted 2 times

✉️ **pentium75** 3 months ago

Why would Lambda incur a high bill? If it runs 5000 times each day, each time for 0.5 seconds, you'd pay for 2500 seconds in total.
upvoted 1 times

Question #162

Topic 1

A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.

The company seeks a cloud storage solution that permits the copying of on-premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.

Which combination of AWS services meets these requirements?

- A. Amazon FSx for Lustre integrated with Amazon S3
- B. Amazon FSx for Windows File Server integrated with Amazon S3
- C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
- D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Correct Answer: A

Community vote distribution

A (100%)

 **Marge_Simpson**  1 year, 3 months ago

Selected Answer: A

If you see HPC and Linux both in the question.. Pick Amazon FSx for Lustre
upvoted 30 times

 **HayLLIHuK** 1 year, 2 months ago

yeap, you're right!
upvoted 2 times

 **aba2s**  1 year, 2 months ago

Selected Answer: A

Additional keywords: make data available for processing by all EC2 instances ==> FSx

In absence of EFS, it should be FSx. Amazon FSx For Lustre provides a high-performance, parallel file system for hot data
upvoted 9 times

 **MrPCarrot**  1 month, 3 weeks ago

A is the answer because Amazon FSx for Lustre provides a high-performance, scalable file system optimized for compute-intensive workloads like HPC.
upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

Selected Answer: A

Lustre is default when HPC is involved. <https://aws.amazon.com/fsx/lustre/>

B: mentions Windows and no-one asked for it.

C: S3 Glacier is too slow for HPC

D: I don't think this is possible, unless I'm mistake, how can you connect a VPC endpoint to EBS without an EC2 kind of instance?

upvoted 1 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: A

HPC workloads running on Linux = Amazon FSx for Lustre

upvoted 1 times

 **Jeyaluxshan** 6 months, 3 weeks ago

High performance - Lustre

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

The reasons are:

Amazon FSx for Lustre provides a high-performance, scalable file system optimized for compute-intensive workloads like HPC. It has native integration with Amazon S3.

Data can be copied from on-premises to an S3 bucket, acting as persistent long-term storage.

The FSx for Lustre file system can then access the S3 data for high speed processing of datasets and output files.

FSx for Lustre is designed for the Linux environments used in this HPC workload.

upvoted 2 times

 **cookieMr** 9 months ago

Selected Answer: A

FSx for Lustre is a high-performance file system optimized for compute-intensive workloads. It provides scalable, parallel access to data and is suitable for HPC applications.

By integrating FSx for Lustre with S3, you can easily copy on-premises data to long-term persistent storage in S3, making it available for processing by EC2 instances.

S3 serves as the durable and highly scalable object storage for storing the output files, allowing for analytics and long-term future use.

Option B, FSx for Windows File Server, is not suitable because the workloads run on Linux, and this option is designed for Windows file sharing.

Option C, S3 Glacier integrated with EBS, is not the best choice as it is a low-cost archival storage service and not optimized for high-performance file system requirements.

Option D, using an S3 bucket with a VPC endpoint integrated with an Amazon EBS General Purpose SSD (gp2) volume, does not provide the required high-performance file system capabilities for HPC workloads.

upvoted 2 times

 **Bmarodi** 10 months ago

Selected Answer: A

Option A is right answer.

upvoted 1 times

 **kerin** 1 year, 1 month ago

FSx for Lustre makes it easy and cost-effective to launch and run the popular, high-performance Lustre file system. You use Lustre for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.

Amazon FSx for Lustre is integrated with Amazon S3.

upvoted 2 times

 **SilentMilli** 1 year, 2 months ago

Selected Answer: A

Amazon FSx for Lustre integrated with Amazon S3

upvoted 1 times

 **techhb** 1 year, 3 months ago

Selected Answer: A

A is right choice here.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

Option A is the best high performance storage with integration to S3

upvoted 1 times

 **wly_al** 1 year, 3 months ago

Selected Answer: A

Requirement is File System and workload running on Linux. So S3 and FSx for Windows is not an option

upvoted 1 times

 **Shasha1** 1 year, 3 months ago

A

The Amazon FSx for Lustre service is a fully managed, high-performance file system that makes it easy to move and process large amounts of data quickly and cost-effectively. It provides a fully managed, cloud-native file system with low operational overhead, designed for massively parallel processing and high-performance workloads. The Lustre file system is a popular, open source parallel file system that is well-suited for a variety of applications such as HPC, image processing, AI/ML, media processing, data analytics, and financial modeling, among others. With Amazon FSx for Lustre, you can quickly create and configure new file systems in minutes, and easily scale the size of your file system up or down.

upvoted 2 times

 **Wpcorgan** 1 year, 4 months ago

A is correct

upvoted 1 times

 **BENICE** 1 year, 4 months ago

A - for HPC "Amazon FSx for Lustre" and long-term persistence "S3"

upvoted 1 times

Question #163

Topic 1

A company is building a containerized application on premises and decides to move the application to AWS. The application will have thousands of users soon after it is deployed. The company is unsure how to manage the deployment of containers at scale. The company needs to deploy the containerized application in a highly available architecture that minimizes operational overhead.

Which solution will meet these requirements?

- A. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the AWS Fargate launch type to run the containers. Use target tracking to scale automatically based on demand.
- B. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the Amazon EC2 launch type to run the containers. Use target tracking to scale automatically based on demand.
- C. Store container images in a repository that runs on an Amazon EC2 instance. Run the containers on EC2 instances that are spread across multiple Availability Zones. Monitor the average CPU utilization in Amazon CloudWatch. Launch new EC2 instances as needed.
- D. Create an Amazon EC2 Amazon Machine Image (AMI) that contains the container image. Launch EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon CloudWatch alarm to scale out EC2 instances when the average CPU utilization threshold is breached.

Correct Answer: C

Community vote distribution

A (100%)

✉  goatbernard  1 year, 4 months ago

Selected Answer: A

AWS Fargate

upvoted 13 times

✉  awsgeek75  2 months, 3 weeks ago

Selected Answer: A

A is minimal overhead.

B has EC2 overhead

C EC2 instance overhead + container repository running on EC2 overhead

D AMII, CloudWatch alarm is overhead++

upvoted 4 times

✉  awsgeek75 2 months, 1 week ago

Also, simply speaking, if the company is unsure how to manage deployed containers then Fargate is the only choice.

upvoted 1 times

✉  Ruffyit 3 months, 3 weeks ago

ECR+ECS+Fargate = Less overhead

upvoted 2 times

✉  ACloud_Guru15 4 months, 4 weeks ago

Selected Answer: A

ECR+ECS+Fargate = Less overhead

upvoted 2 times

✉  Sindokuhlep 5 months ago

Selected Answer: A

Fargate

upvoted 1 times

✉  TariqKipkemei 6 months, 2 weeks ago

Selected Answer: A

Highly available architecture that minimizes operational overhead = Serverless = Elastic Container Registry, Amazon Elastic Container Service with AWS Fargate launch type

upvoted 1 times

✉  Guru4Cloud 7 months, 1 week ago

Selected Answer: A

Using ECR provides a fully managed container image registry.

ECS with Fargate launch type allows running containers without managing servers or clusters. Fargate will handle scaling and optimization.

Target tracking autoscaling will allow automatically adjusting capacity based on demand.

The serverless approach with Fargate minimizes operational overhead.

upvoted 2 times

MikeDu 7 months, 2 weeks ago

Selected Answer: A

AWF Fargate should be the best choice

upvoted 1 times

aadityaravi8 8 months, 3 weeks ago

A is the right answer undoubtedly.

upvoted 1 times

cookieMr 9 months ago

Selected Answer: A

ECR provides a secure and scalable repository to store and manage container images. ECS with the Fargate launch type allows you to run containers without managing the underlying infrastructure, providing a serverless experience. Target tracking in ECS can automatically scale the number of tasks or services based on a target value such as CPU or memory utilization, ensuring that the application can handle increasing demand without manual intervention.

Option B is not the best choice because using the EC2 launch type requires managing and scaling EC2 instances, which increases operational overhead.

Option C is not the optimal solution as it involves managing the container repository on an EC2 instance and manually launching EC2 instances, which adds complexity and operational overhead.

Option D also requires managing EC2 instances, configuring ASGs, and setting up manual scaling rules based on CloudWatch alarms, which is not as efficient or scalable as using Fargate in combination with ECS.

upvoted 4 times

Bmarodi 8 months, 2 weeks ago

Nice explanations!

upvoted 1 times

Bmarodi 10 months ago

Selected Answer: A

ECS + Fargate satisfy requirements, hence option A is the best solution.

upvoted 1 times

studynoplay 10 months, 2 weeks ago

Selected Answer: A

minimize operational overhead = Serverless

Fargate is Serverless

upvoted 1 times

NoinNothing 11 months, 2 weeks ago

Selected Answer: A

Correct is "A"

upvoted 1 times

jaswantn 11 months, 3 weeks ago

You can place Fargate launch type all in one AZ, or across multiple AZs. But Option A does not take care of High Availability requirement of question. With Option C we have multi AZ.

upvoted 2 times

wizcloudifa 3 weeks, 3 days ago

that was my doubt too, is Fargate by default highly available? I chose D as option C didn't have a scalability option in it, option D has an autoscaling group in it C doesn't

upvoted 1 times

SkyZeroZx 11 months, 3 weeks ago

Selected Answer: A

A

Why?

Because fargate provisioned on demand resource

upvoted 2 times

CheckpointMaster 1 year, 2 months ago

Option A

AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers. This removes the need to choose server types, decide when to scale your clusters, or optimize cluster packing.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

Option A

upvoted 1 times

Question #164

Topic 1

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed: If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.
- B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).
- C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
- D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

Correct Answer: C

Community vote distribution



aba2s Highly Voted 1 year, 2 months ago

Selected Answer: C

Amazon SQS supports dead-letter queues (DLQ), which other queues (source queues) can target for messages that can't be processed (consumed) successfully.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>
upvoted 11 times

dkw2342 Most Recent 3 weeks, 4 days ago

C) This option works. There is a 12h maximum visibility timeout, but:

"If you don't know how long it takes to process a message, create a heartbeat for your consumer process: Specify the initial visibility timeout (for example, 2 minutes) and then—as long as your consumer still works on the message—keep extending the visibility timeout by 2 minutes every minute."

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/working-with-messages.html>
upvoted 2 times

dkw2342 3 weeks, 4 days ago

None of the options fit.

- A) Not operationally efficient
- B) Kinesis is for real-time processing
- C) SNS is not suitable for work queuing.

C) While this may be the "correct" answer, it also doesn't really fit the problem statement.

Maximum visibility timeout for SQS is 12h, also can't be extended by the consumer.

"If your consumer needs longer than 12 hours, consider using Step Functions."

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>
upvoted 1 times

awsgeek75 2 months, 3 weeks ago

Selected Answer: C

C is the only option with dead letter que which meets the requirement of retaining messages that fail to process without impacting other messages.

upvoted 2 times

TariqKipkemei 6 months, 2 weeks ago

Selected Answer: C

Implement an AWS service to handle messages between the two applications = Amazon Simple Queue Service
If the messages fail to process, they must be retained = a dead-letter queue
upvoted 3 times

Guru4Cloud 7 months, 1 week ago

Selected Answer: C

SQS provides a fully managed message queuing service that meets all the requirements:

SQS can handle the sending and processing of 1,000 messages per hour
Messages can be retained for up to 14 days to allow the full 2 days for processing
Using a dead-letter queue will retain failed messages without impacting other processing
SQS requires minimal operational overhead compared to running your own message queue server
upvoted 2 times

MutiverseAgent 8 months, 1 week ago

Selected Answer: B

Answer is B), the reason is:

- Because messages might up to 2 days to be processed. Visibility timeout of SQS is 12 hours, so after 12 hours another consumer might take a message from the queue which is currently being processed.

upvoted 1 times

cookieMr 9 months ago

Selected Answer: C

By integrating both the sender and processor applications with an SQS, messages can be reliably sent from the sender to the processor application for processing. SQS provides at-least-once delivery, ensuring that messages are not lost in transit. If a message fails to process, it can be retained in the queue and retried without impacting the processing of other messages. Configuring a DLQ allows for the collection of messages that repeatedly fail to process, providing visibility into failed messages for troubleshooting and analysis.

A is not the optimal choice as it involves managing and configuring an EC2 instance running a Redis, which adds operational overhead and maintenance requirements.

B is not the most operationally efficient solution as it introduces additional complexity by using Amazon Kinesis data streams and integrating with the Kinesis Client Library for message processing.

D, using SNS, is not the best fit for the scenario as it is more suitable for pub/sub messaging and broadcasting notifications rather than the specific requirement of message processing between two applications.

upvoted 4 times

Bmarodi 8 months, 2 weeks ago

Nice explanations always, thanks a lot!

upvoted 1 times

Bmarodi 7 months, 2 weeks ago

Nice explanations always, thanks a lot

upvoted 1 times

Jeeva28 10 months ago

Selected Answer: C

Answer C, In Question if Keyword have Processing Failed >> SQS

upvoted 1 times

Bmarodi 10 months ago

Selected Answer: C

solution that meets these requirements and is the MOST operationally efficient will be option C. SQS is buffer between 2 APPs.

upvoted 1 times

norris81 10 months, 1 week ago

The visibility timeout must not be more than 12 hours. (For SQS)

Jobs may take 2 days to process

upvoted 2 times

studynoplay 10 months, 2 weeks ago

Selected Answer: C

operationally efficient = Serverless
SQS is serverless

upvoted 1 times

studynoplay 10 months, 2 weeks ago

SNS too is serverless, but it is obvious that it is not the correct answer in this case

upvoted 1 times

apchandana 11 months ago

Selected Answer: C

more realistic option is C.

only problem with this is the limit of the visibility timeout is 12H max. as the second application take 2 days to process, there will be a duplicate of processing messages in the queue. this might complicate things.

upvoted 2 times

 **nilandd44gg** 8 months, 1 week ago

Amazon SQS automatically deletes messages that have been in a queue for more than the maximum message retention period. The default message retention period is 4 days. However, you can set the message retention period to a value from 60 seconds to 1,209,600 seconds (14 days) using the SetQueueAttributes action.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-architecture.html>

upvoted 1 times

 **vherman** 1 year ago

SQS has a limit 12h for visibility time out

upvoted 1 times

 **bullrem** 1 year, 2 months ago

Selected Answer: B

Option C, using Amazon SQS, is a valid solution that meets the requirements of the company. However, it may not be the most operationally efficient solution because SQS is a managed message queue service that requires additional operational overhead to handle the retention of messages that failed to process. Option B, using Amazon Kinesis Data Streams, is more operationally efficient for this use case because it can handle the retention of messages that failed to process automatically and provides the ability to process and analyze streaming data in real-time.

upvoted 1 times

 **UnluckyDucky** 1 year ago

Kinesis stream save data for up to 24 hours, doesn't meet the 2 day requirement.

Kinesis streams don't have fail-safe for failed processing, unlike SQS.

The correct answer is C - SQS.

upvoted 3 times

 **apchandana** 11 months ago

this is not a correct statement.

A data stream is a logical grouping of shards. There are no bounds on the number of shards within a data stream (request a limit increase if you need more). A data stream will retain data for 24 hours by default, or optionally up to 365 days.

Shard

<https://aws.amazon.com/kinesis/data-streams/getting-started/>

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

There's no way for kinesis to know whether the message processing failed.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: C

Option C.

upvoted 1 times

 **ocbn3wby** 1 year, 3 months ago

Selected Answer: C

This matches mostly the job of Dead Letter Q:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

vs

<https://docs.aws.amazon.com/streams/latest/dev/shared-throughput-kcl-consumers.html>

upvoted 4 times

Question #165

Topic 1

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF.

How should the solutions architect comply with these requirements?

- A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
- B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
- C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
- D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Correct Answer: D

Community vote distribution



✉️ **Nigma** 1 year, 4 months ago

Answer D. Use an OAI to lockdown CloudFront to S3 origin & enable WAF on CF distribution
upvoted 29 times

✉️ **FNJ1111** 1 year, 2 months ago

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/> confirms use of OAI (and option D).
upvoted 12 times

✉️ **cookieMr** 9 months ago

Selected Answer: B

By configuring CloudFront to forward all incoming requests to AWS WAF, the traffic will be inspected by AWS WAF before reaching the S3 origin, complying with the security policy requirement. This approach ensures that all website traffic is inspected by AWS WAF, providing an additional layer of security before accessing the content stored in the S3 origin.

Option A is not the correct choice as configuring an S3 bucket policy to accept requests from the AWS WAF ARN only would bypass the inspection of traffic by AWS WAF. It does not ensure that all website traffic is inspected.

Option C is not the optimal solution as it focuses on controlling access to S3 using a security group. Although it associates AWS WAF with CloudFront, it does not guarantee that all incoming requests are inspected by AWS WAF.

Option D is not the recommended solution as configuring an OAI in CloudFront and restricting access to the S3 bucket does not ensure that all website traffic is inspected by AWS WAF. The OAI is used for restricting direct access to S3 content, but the traffic should still pass through AWS WAF for inspection.

upvoted 8 times

✉️ **escalibran** 1 week, 6 days ago

Option B does use the WAF through Cloudfront, but it does not mention anything to prevent direct access to the objects without going through Cloudfront.
upvoted 1 times

✉️ **bogobob** 4 months, 2 weeks ago

Apparently you can only point to a custom host that is "not an Amazon Simple Storage Service (Amazon S3) bucket" (other than for static hosting). <https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/>. Answer should be D
upvoted 1 times

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

agreed. Must be D as per above security blog
upvoted 3 times

✉️ **Uzbekistan** 2 days, 7 hours ago

Selected Answer: B

Option B ensures that all incoming requests to the static website served through Amazon CloudFront are first forwarded to AWS WAF for inspection before the content is requested from the S3 origin. This ensures that all website traffic is inspected by AWS WAF as required by the company's security policy.
upvoted 1 times

✉️ **drdz13** 1 week, 5 days ago

D is not possible since you cannot set OAC or OAI if S3 bucket is used as static website host

upvoted 1 times

 bujuman 2 months, 1 week ago

Selected Answer: D

WAF is associated to a Cloudfront Distribution

upvoted 1 times

 awsgEEK75 2 months, 1 week ago

Selected Answer: D

A: Doesn't make sense in context with CF.

B: You configure WAF on CF for HTTP status handling so this may be right be is badly worded

C: You might as well re-engineer S3 and CloudFront!

D: The requirement for WAF usage is met with this. Doesn't have to be smart usage, just enabled.

upvoted 1 times

 vip2 2 months, 1 week ago

Selected Answer: D

some people use below link as supported point, but when you look into link, AWF is in front of CloudFront from traffic view. So, B is incorrect because 'there is no CloudFront forward requesting to ACL.'

<https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/>

upvoted 1 times

 Parul25 1 month, 3 weeks ago

A content delivery network is typically deployed before a web application firewall (WAF). Refer to the "Here's how the solution works" section provided in your linked resource.

upvoted 1 times

 ale_brd_ 3 months, 2 weeks ago

Selected Answer: B

B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.

This option ensures that all website traffic passes through AWS WAF for inspection before reaching the S3 origin, complying with the security policy requirements. I appreciate your thorough analysis.

upvoted 1 times

 wearrexdzw3123 4 months, 2 weeks ago

Selected Answer: D

It's storage, not web endpoint.so It's [http://\[bucket-name\].s3.\[region\].amazonaws.com](http://[bucket-name].s3.[region].amazonaws.com) , and

oai can be used

upvoted 1 times

 wearrexdzw3123 4 months, 2 weeks ago

This resolution doesn't apply to S3 origins that are configured as a website endpoint. For example, AWSDOC-EXAMPLE-BUCKET.s3-website-us-east-1.amazonaws.com.

upvoted 1 times

 rlamberti 5 months ago

Selected Answer: D

WAF is not a destination.

WAF is attached to something to inspect traffic (ALB, CloudFront etc), so D is the correct answer.

upvoted 5 times

 fageroff 5 months ago

If your origin is an Amazon S3 bucket configured as a website endpoint, you must set it up with CloudFront as a custom origin. That means you can't use OAC (or OAI).

upvoted 2 times

 Ramdi1 5 months, 3 weeks ago

Selected Answer: B

voting B because of inspecting traffic

upvoted 1 times

 javiems 5 months, 4 weeks ago

Selected Answer: D

Answer D. By configuring an OAI, you restrict direct access to your S3 bucket, ensuring that only CloudFront can access the content in the bucket. This enhances security by preventing direct access to the S3 origin. Enabling AWS WAF on the CloudFront distribution allows you to inspect all incoming traffic through CloudFront before it reaches the S3 origin. This ensures that all website traffic is inspected for security threats as required by the company's security policy.

upvoted 3 times

 vijaykamal 6 months ago

Answer is D. B option doesn't involve S3 or the use of an origin access identity (OAI) to restrict access to the S3 bucket. It's important to ensure that unauthorized users cannot access S3 objects directly.

upvoted 2 times

✉  **JKevin778** 6 months ago

Selected Answer: D

<https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html>

D

upvoted 1 times

✉  **BrijMohan08** 6 months, 1 week ago

Selected Answer: D

Using an Origin Access Identity (OAI) allows you to restrict direct access to the S3 bucket and ensure all traffic comes through CloudFront.

AWS WAF can then be enabled on the CloudFront distribution to inspect all incoming traffic.

The correct answer is D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

upvoted 1 times

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

Selected Answer: D

Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

upvoted 1 times

Question #166

Topic 1

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files.
- B. Use cross-Region replication to all Regions.
- C. Use the geoproximity feature of Amazon Route 53.
- D. Use Amazon CloudFront with the S3 bucket as its origin.

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

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

Selected Answer: D

The most effective and efficient solution would be Option D (Use Amazon CloudFront with the S3 bucket as its origin.)

Amazon CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as HTML pages, images, and videos. By using CloudFront, the HTML pages will be served to users from the edge location that is closest to them, resulting in faster delivery and a better user experience. CloudFront can also handle the high traffic and large number of requests expected for the global event, ensuring that the HTML pages are available and accessible to users around the world.

upvoted 8 times

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

Selected Answer: D

Global users = Amazon CloudFront

upvoted 1 times

✉️  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

CloudFront is the best solution for this use case because:

CloudFront is a content delivery network (CDN) that caches content at edge locations around the world. This brings content closer to users for fast performance.

For high traffic global events with millions of viewers, a CDN is necessary for effective distribution.

Using the S3 bucket as the origin, CloudFront can fetch the files once and cache them globally.

upvoted 1 times

✉️  **cookieMr** 9 months ago

Selected Answer: D

CloudFront is well-suited for efficiently serving static HTML pages to users around the world. By using it with the S3 as its origin, the static HTML pages can be cached and distributed globally to edge locations, reducing latency and improving performance for users accessing the pages from different regions. This solution ensures efficient and effective delivery of the daily reports to millions of users worldwide, providing a scalable and high-performance solution for the global event.

A would allow temporary access to the files, but it does not address the scalability and performance requirements of serving millions of views globally.

B is not necessary for this scenario as the goal is to distribute the static HTML pages efficiently to users worldwide, not replicate the files across multiple Regions.

C is primarily used for routing DNS traffic based on the geographic location of users, but it does not provide the caching and content delivery capabilities required for this use case.

upvoted 4 times

✉️  **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

✉️  **k1kavi1** 1 year, 3 months ago

Selected Answer: D

Agreed

upvoted 1 times

 **Sahilbhai** 1 year, 3 months ago

answer is D agree with Shasha1

upvoted 1 times

 **Shasha1** 1 year, 3 months ago

D

CloudFront is a content delivery network (CDN) offered by Amazon Web Services (AWS). It functions as a reverse proxy service that caches web content across AWS's global data centers, improving loading speeds and reducing the strain on origin servers. CloudFront can be used to efficiently deliver large amounts of static or dynamic content anywhere in the world.

upvoted 2 times

 **Wpcorgan** 1 year, 4 months ago

D is correct

upvoted 2 times

 **Nigma** 1 year, 4 months ago

D

Static content on S3 and hence Cloudfront is the best way

upvoted 2 times

 **Pamban** 1 year, 4 months ago

Selected Answer: D

D is the correct answer

upvoted 2 times

Question #167

Topic 1

A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.

Which solution meets these requirements MOST cost-effectively?

- A. Use Spot Instances exclusively to handle the maximum capacity required.
- B. Use Reserved Instances exclusively to handle the maximum capacity required.
- C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
- D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

Correct Answer: C*Community vote distribution*

HayLLIHuK 1 year, 2 months ago

Selected Answer: C

"without any downtime" - Reserved Instances for the baseline capacity
 "MOST cost-effectively" - Spot Instances to handle additional capacity
 upvoted 28 times

LuckyAro 1 year, 2 months ago

Dude, read the question, cost consideration was not mentioned in the question.
 upvoted 1 times

ShinobiGrappler 1 year, 2 months ago

Dude, read the question, "Which solution meets these requirements MOST cost-effectively?"
 upvoted 26 times

kraken21 11 months, 3 weeks ago

I am leaning towards C because the idea of having a queue is to decouple the processing. If an instance goes down(spot) while processing will it not show up back after the visibility timeout? So using spot meets the cost-effective objective.
 upvoted 5 times

Sutariya 6 months, 3 weeks ago

Intermediate data stored in SQS queue so once free then it take data and process.
 upvoted 1 times

MrSaint 11 months ago

cost-effectively means, Cheapest solution (cost) that achieve all the requirements (effectively). Its not cost-effectively if is just cheapest solution that fail to address all the requirements, in this case. (This application should continually process messages without any downtime) no matter the volume, since it is unpredictable. B for example, address the requirement but not the cheapest solution that achieve it. D is the cheaper choice that address the requirement (without any downtime). and C is cheaper than D but do not guarantee that you wont have downtime since it is SPOT instances.
 upvoted 8 times

kraken21 12 months ago

How can you have baseline capacity when your message volume is unpredictable and often has intermittent traffic?
 upvoted 4 times

MutiverseAgent 8 months, 1 week ago

For this reason I think correct answer is A
 upvoted 1 times

Macadam 4 months, 1 week ago

Spot instances cannot be an option as it is unreliable and the question requires the messages to be continuously processed
 upvoted 3 times

taer 1 year, 4 months ago

Selected Answer: D

D is the correct answer
 upvoted 24 times

Drayen25 1 year, 1 month ago

C is correct, read for cost effectiveness

upvoted 6 times

 **diabloexodia** 8 months, 1 week ago

AWS has stopped issuing spot instances so i think C

upvoted 1 times

 **diabloexodia** 8 months, 1 week ago

so i think C is incorrect*. the Correct ans is D.

upvoted 1 times

 **sezer** 12 months ago

if you cannot find enough spot instance you will have downtime

you cannot always find spot instance

upvoted 10 times

 **Kumaran1508** 10 months ago

Why downtime when there are baseline reserved instances?

upvoted 3 times

 **Sutariya** 6 months, 3 weeks ago

Baseline reserved instances and ondemand Spot instance is cost saver

upvoted 2 times

 **Uzbekistan** Most Recent 2 days, 7 hours ago

Selected Answer: C

Using Reserved Instances (RIs) for baseline capacity ensures a lower cost for the instances that are constantly required to maintain the application's baseline workload. RIs offer significant cost savings compared to On-Demand instances, making them a cost-effective choice for steady-state workloads.

Spot Instances can then be utilized to handle additional capacity during periods of higher message volume. Spot Instances provide spare EC2 capacity at significantly reduced prices compared to On-Demand instances, allowing for cost savings during peak workloads. Since the message volume is unpredictable and often intermittent, Spot Instances can efficiently handle the fluctuating demand without incurring high costs.

upvoted 1 times

 **escalibran** 1 week, 6 days ago

Missing some information to make a proper decision. What does "without downtime" mean? We are already outside of Realtime processing, and messages can remain in the queue until picked up. Purely using Spot instances _might_ do just fine, but there could be times when no spare capacity is available. How much delay is acceptable? I'd go with reserved+spot, but reserved+on demand may be required for priority on bursty load.

B is the one option i would rule out completely. The workload is unpredictable, we can't reserve infinity instances for all eternity.

upvoted 1 times

 **Hrishi_707** 2 weeks, 3 days ago

Keywords are - Production, without any downtime. I would prefer D option as AWS itself recommends, spot instances should not be used in Prod environment.

upvoted 1 times

 **NayeraB** 1 month, 1 week ago

Selected Answer: D

I think this phrase "This application should continually process messages without any downtime." killed the idea of using Spot instances, not 100% sure though.

upvoted 4 times

 **MrPCarrot** 1 month, 3 weeks ago

Answer is C Reserved Instances for the baseline capacity can be used to handle downtime issue and Spot Instances to handle additional capacity is the most cost effective

upvoted 1 times

 **Charumathi** 1 month, 4 weeks ago

Selected Answer: D

Reserved Instances for Baseline + On-Demand for unpredictable volume and intermittent traffic without downtime.

Keywords:

1. Production Application
2. Unpredictable Volume and intermittent traffic
3. Without any down-time

Spot-instances is a cheaper option, but cannot guarantee downtime, and it is subject to availability too, hence the best choice is to go for On-Demand instances.

upvoted 3 times

 **Leybiuk** 2 months ago

Selected Answer: C

Cheaper option which meets requirement

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: D

reserved for baseline + on-demand for additional
C will work but spot does not guarantee "continually process messages without any downtime"
spot instance may not even be available so what happens with the messages which exceed baseline requirements?

upvoted 1 times

 **SVDK** 2 months, 2 weeks ago

C is correct. Because
- This application should continually process messages without any downtime -> RI for baseline workload
- The message volume is unpredictable and often has intermittent traffic. -> Spot instances or on demand instances
- Which solution meets these requirements MOST cost-effectively -> Spot instances (ruling out/dismissing on demand instances)

upvoted 1 times

 **farnamjam** 2 months, 4 weeks ago

Selected Answer: D

Although Spot instance is cheaper, but it might be terminated so it's not a reliable solution.

upvoted 3 times

 **bi11** 3 months ago

Selected Answer: C

cccccccccccc

upvoted 1 times

 **ale_brd_** 3 months, 2 weeks ago

Selected Answer: C

On-Demand Instances are generally more expensive compared to Spot Instances. In scenarios with unpredictable and intermittent traffic, using On-Demand Instances for additional capacity may result in higher costs than leveraging Spot Instances.

In summary, Option C is more cost-effective because it leverages the potential cost savings of Spot Instances for handling increased demand during unpredictable traffic spikes, providing a balance between cost predictability (with Reserved Instances) and cost efficiency (with Spot Instances).

upvoted 1 times

 **ansagr** 3 months, 2 weeks ago

Selected Answer: C

This option combines the cost savings of Reserved Instances for the baseline workload with the flexibility and potential cost savings of Spot Instances for handling bursts of additional capacity. It provides a balance between cost-effectiveness and ensuring continuous processing even during peak periods.

Messages are read from SQS, meaning that if a Spot instance is terminated while processing a message, the message will remain in the queue for retry.

upvoted 1 times

 **Marco_St** 4 months ago

Selected Answer: C

The traffic itself is also intermittent so for additional capacity, spot instance along with SQS should be good to go to handle these traffic to avoid downtime and also have least cost of instances. Of course for based line capacity, reserved instance is reliable and also cheaper than on-demand. C

upvoted 1 times

 **slots** 4 months, 1 week ago

Selected Answer: D

spot instance is not reliable solution

upvoted 1 times

Question #168

Topic 1

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Correct Answer: D

Community vote distribution

D (100%)

✉️  **Nigma**  1 year, 4 months ago

D. Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. See https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html.
upvoted 18 times

✉️  **cookieMr**  9 months ago

By creating an SCP in the root organizational unit, the security team can define and enforce fine-grained permissions that limit access to specific services or actions across all member accounts. The SCP acts as a guardrail, denying access to specified services or actions, ensuring that the permissions are consistent and applied uniformly across the organization. SCPs are scalable and provide a single point of control for managing permissions, allowing the security team to centrally manage access restrictions without needing to modify individual account settings.

Option A and option B are not suitable for controlling access across multiple accounts in AWS Organizations. ACLs and security groups are typically used for managing network traffic and access within a single account or a specific resource.

Option C is not the recommended approach. Cross-account roles are used for granting access, and denying access through cross-account roles can be complex and less manageable compared to using SCPs.

upvoted 8 times

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

This was a good explanation of why A and B are not correct. I was thinking A but after reading this I agree with you D is correct.

upvoted 1 times

✉️  **Ruffyt**  3 months, 3 weeks ago

D. Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. See https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html.

upvoted 1 times

✉️  **mach2022** 4 months, 3 weeks ago

is D because of Deeznuts

upvoted 2 times

✉️  **the_bong_lord** 2 months ago

gottem

upvoted 1 times

✉️  **xplusfb** 5 months, 1 week ago

Selected Answer: D

Its very clear question answer is D

upvoted 1 times

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

Selected Answer: D

<https://medium.com/@darekhale91/how-to-pass-amazon-saa-c03-exam-dumps-2023-583619ddbcc8>

upvoted 1 times

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

Selected Answer: D

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.

upvoted 1 times

Guru4Cloud 7 months, 1 week ago

Selected Answer: D

D. Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. See https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html.

upvoted 1 times

Bmarodi 10 months ago

Selected Answer: D

I vote for option D by Creating a service control policy (SCP) in the root organizational unit to deny access to the services or actions, meets the requirements.

upvoted 1 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Selected Answer: D

To limit access to specific services or actions in all of the team's AWS accounts and maintain a single point where permissions can be managed, the solutions architect should create a service control policy (SCP) in the root organizational unit to deny access to the services or actions (Option D).

Service control policies (SCPs) are policies that you can use to set fine-grained permissions for your AWS accounts within your organization. SCPs are attached to the root of the organizational unit (OU) or to individual accounts, and they specify the permissions that are allowed or denied for the accounts within the scope of the policy. By creating an SCP in the root organizational unit, the security team can set permissions for all of the accounts in the organization from a single location, ensuring that the permissions are consistently applied across all accounts.

upvoted 4 times

career360guru 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 1 times

Wpcorgan 1 year, 4 months ago

D is correct

upvoted 1 times

babaxoxo 1 year, 4 months ago

an organization and requires single point place to manage permissions

upvoted 2 times

goatbernard 1 year, 4 months ago

Selected Answer: D

SCP for organization

upvoted 3 times

Question #169

Topic 1

A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application.

What should the solutions architect do to meet this requirement?

- A. Add an Amazon Inspector agent to the ALB.
- B. Configure Amazon Macie to prevent attacks.
- C. Enable AWS Shield Advanced to prevent attacks.
- D. Configure Amazon GuardDuty to monitor the ALB.

Correct Answer: C

Community vote distribution

C (100%)

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

What's going on, suddenly the questions are so easy
upvoted 7 times

✉  **Sutariya** 8 months ago

Its due to confidence level going up after experience.
upvoted 6 times

✉  **Ruffy**  3 months, 3 weeks ago

When you see DDOS immediately think Shield
upvoted 4 times

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

Selected Answer: C

When you see DDOS immediately think Shield
upvoted 3 times

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

Selected Answer: C

AWS Shield is a managed DDoS protection service that safeguards applications running on AWS.
upvoted 1 times

✉  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: C

Enable AWS Shield Advanced to prevent attacks.
upvoted 1 times

✉  **cookieMr** 9 months ago

Selected Answer: C

By enabling Shield Advanced, the web application benefits from automatic protection against common and sophisticated DDoS attacks. It utilizes advanced detection and mitigation techniques, including ML algorithms and traffic analysis, to provide effective DDoS protection.
It also includes features like real-time monitoring, attack notifications, and detailed attack reports.

A is not related to DDoS protection. Amazon Inspector is a security assessment service that helps identify vulnerabilities and security issues in applications and EC2.

B is also not the appropriate solution. Macie is a service that uses machine learning to discover, classify, and protect sensitive data stored in AWS. It focuses on data security and protection, not specifically on DDoS prevention.

D is not the most effective solution. GuardDuty is a threat detection service that analyzes events and network traffic to identify potential security threats and anomalies. While it can provide insights into potential DDoS attacks, it does not actively prevent or mitigate them.

upvoted 3 times

✉  **techhb** 1 year, 2 months ago

Explained in details here <https://medium.com/@tshemku/aws-waf-vs-firewall-manager-vs-shield-vs-shield-advanced-4c86911e94c6>
upvoted 2 times

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

Selected Answer: C

To reduce the risk of DDoS attacks against the application, the solutions architect should enable AWS Shield Advanced (Option C).

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that helps protect web applications running on AWS from DDoS attacks. AWS Shield Advanced is an additional layer of protection that provides enhanced DDoS protection capabilities, including proactive monitoring and automatic inline mitigations, to help protect against even the largest and most sophisticated DDoS attacks. By enabling AWS Shield Advanced, the solutions architect can help protect the application from DDoS attacks and reduce the risk of disruption to the application.

upvoted 4 times

 **career360guru** 1 year, 3 months ago

Selected Answer: C

C is right answer

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

 **goatbernard** 1 year, 4 months ago

Selected Answer: C

AWS Shield Advanced

upvoted 3 times

 **Nigma** 1 year, 4 months ago

DDOS = AWS Shield

upvoted 4 times

Question #170

Topic 1

A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.

Which configuration will meet this requirement?

- A. Configure the security group for the EC2 instances.
- B. Configure the security group on the Application Load Balancer.
- C. Configure AWS WAF on the Application Load Balancer in a VPC.
- D. Configure the network ACL for the subnet that contains the EC2 instances.

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

Geographic (Geo) Match Conditions in AWS WAF. This new condition type allows you to use AWS WAF to restrict application access based on the geographic location of your viewers. With geo match conditions you can choose the countries from which AWS WAF should allow access.
<https://aws.amazon.com/about-aws/whats-new/2017/10/aws-waf-now-supports-geographic-match/>

upvoted 24 times

✉️  **Ruffyt**  3 months, 3 weeks ago

Geographic (Geo) Match Conditions in AWS WAF. This new condition type allows you to use AWS WAF to restrict application access based on the geographic location of your viewers. With geo match conditions you can choose the countries from which AWS WAF should allow access.
<https://aws.amazon.com/about-aws/whats-new/2017/10/aws-waf-now-supports-geographic-match/>

upvoted 2 times

✉️  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: C

C. Configure AWS WAF on the Application Load Balancer in a VPC

upvoted 1 times

✉️  **Sutariya** 8 months ago

We can use AWS WAF to configure access control rule to access from specific location.

upvoted 1 times

✉️  **cookieMr** 9 months ago

Selected Answer: C

By configuring AWS WAF on the ALB in a VPC, you can apply access control rules based on the geographic location of the incoming requests. AWS WAF allows you to create rules that include conditions based on the IP addresses' country of origin. You can specify the desired country and deny access to requests originating from any other country by leveraging AWS WAF's Geo Match feature.

Option A and option B focus on network-level access control and do not provide country-specific filtering capabilities.

Option D is not the ideal solution for restricting access based on country. Network ACLs primarily control traffic at the subnet level based on IP addresses and port numbers, but they do not have built-in capabilities for country-based filtering.

upvoted 4 times

✉️  **Abrar2022** 10 months ago

Configure AWS WAF for Geo Match Policy

upvoted 1 times

✉️  **aba2s** 1 year, 2 months ago

Selected Answer: C

Source from an AWS link

Geographic (Geo) Match Conditions in AWS WAF. This condition type allows you to use AWS WAF to restrict application access based on the geographic location of your viewers.

With geo match conditions you can choose the countries from which AWS WAF should allow access.

upvoted 2 times

✉️  **techhb** 1 year, 3 months ago

Selected Answer: C

WAF Shield Advanced for DDOS,

GuardDuty is a continuous monitoring service that alerts you of potential threats, while Inspector is a one-time assessment service that provides a

report of vulnerabilities and deviations from best practices.

upvoted 1 times

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

Selected Answer: C

To meet the requirement of allowing the web application to be accessed from one specific country only, the company should configure AWS WAF (Web Application Firewall) on the Application Load Balancer in a VPC (Option C).

AWS WAF is a web application firewall service that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF allows you to create rules that block or allow traffic based on the values of specific request parameters, such as IP address, HTTP header, or query string value. By configuring AWS WAF on the Application Load Balancer and creating rules that allow traffic from a specific country, the company can ensure that the web application is only accessible from that country.

upvoted 4 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: C

OptionC. Configure WAF for Geo Match Policy

upvoted 1 times

✉ **Wpcorgan** 1 year, 4 months ago

C is correct

upvoted 1 times

✉ **mricee9** 1 year, 4 months ago

Selected Answer: C

C

<https://aws.amazon.com/about-aws/whats-new/2017/10/aws-waf-now-supports-geographic-match/>

upvoted 2 times

✉ **Nigma** 1 year, 4 months ago

C. WAF with ALB is the right option

upvoted 1 times

Question #171

Topic 1

A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.

What should the solutions architect do to accomplish this?

- A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.
- B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.
- C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
- D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

Correct Answer: D

Community vote distribution

B (96%) 4%

✉ **bullrem** 1 year, 2 months ago

Selected Answer: B

Option D is similar to option B in that it uses Amazon API Gateway to handle the API requests, but it also includes an EC2 instance to perform the tax computations. However, using an EC2 instance in this way is less scalable and less elastic than using AWS Lambda to perform the computations. An EC2 instance is a fixed resource and requires manual scaling and management, while Lambda is an event-driven, serverless compute service that automatically scales with the number of requests, making it more suitable for handling variable workloads and reducing response times during high traffic periods. Additionally, Lambda is more cost-efficient than EC2 instances, as you only pay for the compute time consumed by your functions, making it a more cost-effective solution.

upvoted 22 times

✉ **Uzbekistan** 1 day, 8 hours ago

Selected Answer: B

Option B leverages AWS Lambda, which is a serverless compute service that automatically scales in response to incoming requests. When a request is made to the API hosted on Amazon API Gateway, API Gateway triggers the associated AWS Lambda function, passing the item names as input parameters. The Lambda function then performs the tax computations based on the provided item names. AWS Lambda automatically manages the compute capacity, ensuring that there is no need to provision or manage servers. This serverless architecture offers scalability and elasticity, as Lambda functions can scale out to handle a larger number of inquiries during the holiday season and scale in during periods of lower demand. Additionally, AWS Lambda is a fully managed service, reducing operational overhead for the company.

upvoted 1 times

✉ **app12** 2 months ago

The thing that bothers me about B is that the request sends the name and then based on the name, the tax is calculated. How do you calculate a value e.g. tax if you just have a name...

upvoted 2 times

✉ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: B

EC2 without autoscaling is not elastic so A, C & D won't be suitable. B uses AWS Lambda which is elastic and scalable by design.

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

Selected Answer: B

Though EC2 can scale (even if less flexible than Lambda), neither A, C nor D involve scaling. All these answers are about a single EC2 instance or a pair of EC2 instances. The only answer that includes scaling and elasticity is B.

upvoted 3 times

✉ **LoXoL** 2 months, 1 week ago

I agree.

upvoted 1 times

✉ **Ruffyit** 3 months, 3 weeks ago

scalable and elastic = serverless = API gateway and AWS Lambda

upvoted 2 times

✉ **paniya93** 5 months, 3 weeks ago

Selected Answer: B

in 002 answer is B. Why is that?

upvoted 1 times

  **vijaykamal** 6 months ago**Selected Answer: B**

Options A, C, and D involve EC2 instances, which are not as inherently scalable and elastic as serverless AWS Lambda functions, and they would require more manual management and operational overhead. Therefore, option B is the most appropriate choice for a scalable and elastic API solution.

upvoted 2 times

  **Guru4Cloud** 6 months, 2 weeks ago**Selected Answer: B**

REST API using Amazon API Gateway and integrating it with AWS Lambda (option B) is the recommended approach to achieve a scalable and elastic solution for the company's API during the holiday season.

No good EC2 in this case

using an EC2 instance in this way is less scalable and less elastic than using AWS Lambda to perform the computations

upvoted 2 times

  **TariqKipkemei** 6 months, 2 weeks ago**Selected Answer: B**

scalable and elastic = serverless = API gateway and AWS Lambda

upvoted 1 times

  **Guru4Cloud** 7 months, 1 week ago

B) Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.

This option provides the most scalable and elastic solution:

API Gateway handles creating the REST API frontend to receive requests

Lambda functions scale automatically to handle spikes in traffic during peak seasons

No servers to manage for the computations, providing high scalability

upvoted 2 times

  **cookieMr** 9 months ago**Selected Answer: B**

Option A (hosting an API on an Amazon EC2 instance) would require manual management and scaling of the EC2 instances, making it less scalable and elastic compared to a serverless solution.

Option C (creating an Application Load Balancer with EC2 instances for tax computations) also involves manual management of the instances and does not offer the same level of scalability and elasticity as a serverless solution.

Option D (designing a REST API using API Gateway and connecting it with an API hosted on an EC2 instance) adds unnecessary complexity and management overhead. It is more efficient to directly integrate API Gateway with AWS Lambda for tax computations.

Therefore, designing a REST API using Amazon API Gateway and integrating it with AWS Lambda (option B) is the recommended approach to achieve a scalable and elastic solution for the company's API during the holiday season.

upvoted 2 times

  **Bmarodi** 10 months ago**Selected Answer: B**

Option B is the solution that is scalable and elastic, hence this meets requirements.

upvoted 1 times

  **jayce5** 11 months ago**Selected Answer: B**

I also prefer B over D. However, it is quite vague since the question doesn't provide the processing time. The maximum processing time for AWS Lambda is 15 minutes.

upvoted 1 times

  **ProfXsamson** 1 year, 1 month ago

B. Serverless option wins over EC2

upvoted 4 times

  **sona21** 1 year, 3 months ago

Lambda is serverless is scalable so answer should be B.

upvoted 2 times

  **Buruguduystunstugudunstuy** 1 year, 3 months ago**Selected Answer: D**

To design a scalable and elastic solution for providing an API for tax computations, the solutions architect should design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance (Option D).

API Gateway is a fully managed service that makes it easy to create, publish, maintain, monitor, and secure APIs at any scale. By designing a REST API using API Gateway, the solutions architect can create an API that is scalable, flexible, and easy to use. The API Gateway can accept and pass the item names to the EC2 instance for tax computations, and the EC2 instance can perform the required computations when the API request is made.

upvoted 2 times

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

Option A (providing an API hosted on an EC2 instance) would not be a suitable solution as it may not be scalable or elastic enough to handle the increased demand during the holiday season.

Option B (designing a REST API using API Gateway that passes item names to Lambda for tax computations) would not be a suitable solution as it may not be suitable for computations that require a larger amount of resources or longer execution times.

Option C (creating an Application Load Balancer with two EC2 instances behind it) would not be a suitable solution as it may not provide the necessary scalability and elasticity. Additionally, it would not provide the benefits of using API Gateway, such as API management and monitoring capabilities.

upvoted 1 times

✉ **JayBee65** 1 year, 2 months ago

But Option D is not scalable. The requirements state "A solutions architect needs to design a solution that is scalable and elastic". D fails to meet these requirements. C on the other hand is scalable. There is nothing in the question to suggest that a longer execution than lambda can handle happens. Therefore D is wrong, and C is possible.

upvoted 3 times

✉ **JayBee65** 1 year, 2 months ago

Sorry, it should say "Therefore D is wrong, and B is possible."

upvoted 3 times

✉ **markw92** 9 months, 1 week ago

You are only explained the "front" part of scalable, unless you have end to end scalable solution it doesn't matter how scalable is your front end. Here in D it ONLY covers the api front end but the constraint is EC2 instance which is ONE and not in a scalable mode. I think B is more suitable given how little information is provided.

upvoted 2 times

Question #172

Topic 1

A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.

Which action should the solutions architect take?

- A. Configure a CloudFront signed URL.
- B. Configure a CloudFront signed cookie.
- C. Configure a CloudFront field-level encryption profile.
- D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.

Correct Answer: A*Community vote distribution*

Bobbybash Highly Voted 1 year, 4 months ago

CCCCCC

Field-level encryption allows you to enable your users to securely upload sensitive information to your web servers. The sensitive information provided by your users is encrypted at the edge, close to the user, and remains encrypted throughout your entire application stack. This encryption ensures that only applications that need the data—and have the credentials to decrypt it—are able to do so.

upvoted 43 times

huzaifaharoun Most Recent 3 weeks ago

C:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

upvoted 1 times

NayeraB 1 month, 1 week ago

Selected Answer: C

C is the only one that addresses handling sensitive information.

upvoted 1 times

bujuman 2 months, 1 week ago

Selected Answer: C

Reviewing my first vote after research. It seems that C is the best answer:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

upvoted 1 times

awsgeek75 2 months, 3 weeks ago

Selected Answer: C

A if for fetch. B requires cookies. D just enforces HTTPS which is already mentioned for the solution (CloudFront only allows HTTPS) and does not add another layer of security.

C provides field level encryption security which is another layer of security.

upvoted 1 times

master9 3 months, 1 week ago

Selected Answer: A

Please go through below link:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html>

upvoted 2 times

pentium75 2 months, 4 weeks ago

This is about controlling access for downloads (making sure that the download request is coming from an authenticated user), it has nothing to do with protecting data that is sent to the application.

upvoted 2 times

Leo1688 3 months, 2 weeks ago

cccc, this link <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

upvoted 2 times

vijaykamal 6 months ago

Selected Answer: C

Options A and B (signed URL and signed cookie) are used for controlling access to specific resources and are typically used for restricting access based on URLs or cookies. They do not provide field-level encryption for sensitive data within HTTP requests.

Option D (configuring CloudFront with the Origin Protocol Policy set to HTTPS Only for the Viewer Protocol Policy) is related to enforcing HTTPS communication between CloudFront and the viewer (end-user). While important for security, it doesn't address the specific requirement of protecting sensitive data within the application stack.

upvoted 3 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: C

C) Configure a CloudFront field-level encryption profile.

Field-level encryption allows you to encrypt sensitive information at the edge before distributing content through CloudFront. It provides an additional layer of security for sensitive user-submitted data.

The other options would not provide field-level encryption

upvoted 1 times

 **mr_D3v1n3** 8 months ago

Would the HTTPS imply that the cert was signed by a CA

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: C

Option A and Option B are used for controlling access to specific resources or content based on signed URLs or cookies. While they provide security and access control, they do not provide field-level encryption for sensitive data within the requests.

Option D ensures that communication between the viewer and CloudFront is encrypted with HTTPS. However, it does not specifically address the protection and encryption of sensitive information within the application stack.

Therefore, the most appropriate action to protect sensitive information throughout the entire application stack and restrict access to certain applications is to configure a CloudFront field-level encryption profile (Option C).

upvoted 2 times

 **Jeeva28** 10 months ago

Selected Answer: C

With Amazon CloudFront, you can enforce secure end-to-end connections to origin servers by using HTTPS. Field-level encryption adds an additional layer of security that lets you protect specific data throughout system processing so that only certain applications can see it.

upvoted 1 times

 **WheretcanIstart** 1 year ago

Selected Answer: C

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

"Field-level encryption allows you to enable your users to securely upload sensitive information to your web servers. The sensitive information provided by your users is encrypted at the edge, close to the user, and remains encrypted throughout your entire application stack".

upvoted 3 times

 **bdp123** 1 year, 1 month ago

Selected Answer: C

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

"With Amazon CloudFront, you can enforce secure end-to-end connections to origin servers by using HTTPS. Field-level encryption adds an additional layer of security that lets you protect specific data throughout system processing so that only certain applications can see it."

upvoted 3 times

 **ProfXsamson** 1 year, 1 month ago

C, field-level encryption should be used when necessary to protect sensitive data.

upvoted 1 times

 **ayanshbhaiji** 1 year, 2 months ago

It should be C

upvoted 2 times

 **HayLLIHuK** 1 year, 2 months ago

Selected Answer: C

C!

CloudFront's field-level encryption further encrypts sensitive data in an HTTPS form using field-specific encryption keys (which you supply) before a POST request is forwarded to your origin. This ensures that sensitive data can only be decrypted and viewed by certain components or services in your application stack.

<https://aws.amazon.com/about-aws/whats-new/2017/12/introducing-field-level-encryption-on-amazon-cloudfront/>

upvoted 3 times

Question #173

Topic 1

A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in Amazon S3. This content is the same for all users.

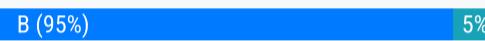
The application has increased in popularity, and millions of users worldwide accessing these media files. The company wants to provide the files to the users while reducing the load on the origin.

Which solution meets these requirements MOST cost-effectively?

- A. Deploy an AWS Global Accelerator accelerator in front of the web servers.
- B. Deploy an Amazon CloudFront web distribution in front of the S3 bucket.
- C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.
- D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.

Correct Answer: B

Community vote distribution



✉️ **Nigma** Highly Voted 1 year, 4 months ago

B. Cloud front is best for content delivery. Global Accelerator is best for non-HTTP (TCP/UDP) cases and supports HTTP cases as well but with static IP (elastic IP) or anycast IP address only.

upvoted 21 times

✉️ **rlamberti** Most Recent 5 months ago

Selected Answer: B

CloudFront will cache the data in Edge Locations, offloading it partially from the source location (s3)

B looks good to me.

upvoted 1 times

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

Selected Answer: B

Deploy an Amazon CloudFront web distribution in front of the S3 bucket

upvoted 1 times

✉️ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

B) Deploy an Amazon CloudFront web distribution in front of the S3 bucket.

CloudFront is the most cost-effective solution for this use case because:

CloudFront can cache static assets like videos and images at edge locations closer to users. This improves performance.

Serving files from the CloudFront cache reduces load on the S3 origin.

CloudFront pricing is very low for data transfer and requests.

upvoted 1 times

✉️ **Kiki_Pass** 8 months ago

Selected Answer: B

ElasticCache is for DB Cache(RDS) nor for S3

upvoted 1 times

✉️ **cookieMr** 9 months ago

Selected Answer: B

Option A is not the most cost-effective solution for this scenario. While Global Accelerator can improve global application performance, it is primarily used for accelerating TCP and UDP traffic, such as gaming and real-time applications, rather than serving static media files.

Options C and D are used for caching frequently accessed data in-memory to improve application performance. However, they are not specifically designed for caching and serving media files like CloudFront, and therefore, may not provide the same cost-effectiveness and scalability for this use case.

Hence, deploying an CloudFront web distribution in front of the S3 is the most cost-effective solution for delivering media files to millions of users worldwide while reducing the load on the origin.

upvoted 4 times

✉️ **kruasan** 11 months ago

Selected Answer: B

ElastiCache, enhances the performance of web applications by quickly retrieving information from fully-managed in-memory data stores. It utilizes Memcached and Redis, and manages to considerably reduce the time your applications would, otherwise, take to read data from disk-based databases.

Amazon CloudFront supports dynamic content from HTTP and WebSocket protocols, which are based on the Transmission Control Protocol (TCP) protocol. Common use cases include dynamic API calls, web pages and web applications, as well as an application's static files such as audio and images. It also supports on-demand media streaming over HTTP.

AWS Global Accelerator supports both User Datagram Protocol (UDP) and TCP-based protocols. It is commonly used for non-HTTP use cases, such as gaming, IoT and voice over IP. It is also good for HTTP use cases that need static IP addresses or fast regional failover

upvoted 4 times

 **LuckyAro** 1 year, 2 months ago

Selected Answer: C

The company wants to provide the files to the users while reducing the load on the origin.
 Cloudfront speeds-up content delivery but I'm not sure it reduces the load on the origin.
 Some form of caching would cache content and deliver to users without going to the origin for each request.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

CloudFront's only main purpose is to serve these kind of scenarios!

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

"Some form of caching would cache content and deliver to users without going to the origin for each request", isn't this EXACTLY what CloudFront does?

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

ElastiCache for Redis (C) can be used by an application to store key-value pairs. It does not cache videos or images and it is not an automatic process (the application can put and retrieve values).

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: B

To provide media files to users while reducing the load on the origin and meeting the requirements cost-effectively, the gaming company should deploy an Amazon CloudFront web distribution in front of the S3 bucket (Option B).

CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as images and videos, to users. By using CloudFront, the media files will be served to users from the edge location that is closest to them, resulting in faster delivery and a better user experience. CloudFront can also handle the high traffic and large number of requests expected from the millions of users, ensuring that the media files are available and accessible to users around the world.

upvoted 3 times

 **techhb** 1 year, 3 months ago

Please dont post ChatGPT answers here,chatgpt keeps on changing its answers,its not the right way to copy paste,thanks.

upvoted 2 times

 **ocbn3wby** 1 year, 1 month ago

Woaaaa! I always wondered where this kind of logic and explanation came from in this guy's answers. Nice catch TECHHB!

upvoted 2 times

 **ocbn3wby** 1 year, 1 month ago

Answers are mostly correct. Only a small percentage were wrong

upvoted 1 times

 **Bofi** 1 year ago

why not? if the answers are correct and offer best possible explanation for the wrong options, I see no reason why it shouldn't be posted here. Also, most of his answers were right, although reasons for the wrong options were sometimes lacking, but all in all, his responses were very good.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: B

Agreed

upvoted 1 times

 **rewdboy** 1 year, 4 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

Question #174

Topic 1

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions.
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Correct Answer: B

Community vote distribution



B (100%)

 **Nigma**  1 year, 4 months ago

B. auto scaling groups can not span multi region
upvoted 25 times

 **cookieMr**  9 months ago

Selected Answer: B

Option A (creating an Auto Scaling group across two Regions) introduces additional complexity and potential replication challenges, which may not be necessary for achieving high availability within a single Region.

Option C (creating an Auto Scaling template for another Region) suggests multi-region redundancy, which may not be the most straightforward solution for achieving high availability without modifying the application.

Option D (changing the ALB to a round-robin configuration) does not provide the desired high availability. Round-robin configuration alone does not ensure fault tolerance and does not leverage multiple Availability Zones for resilience.

Hence, modifying the Auto Scaling group to use three instances across each of two Availability Zones is the appropriate choice to provide high availability for the multi-tier application.

upvoted 7 times

 **TariqKipkemei**  6 months, 2 weeks ago

Selected Answer: B

Modify the Auto Scaling group to use three instances across each of two Availability Zones
upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

Option B. Modify the Auto Scaling group to use three instances across each of the two Availability Zones.
upvoted 2 times

 **techhb** 1 year, 3 months ago

B. auto scaling groups cannot span multi region
upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: B

Option B. Modify the Auto Scaling group to use three instances across each of the two Availability Zones.

This option would provide high availability by distributing the front-end web servers across multiple Availability Zones. If there is an issue with one Availability Zone, the other Availability Zone would still be available to serve traffic. This would ensure that the application remains available and highly available even if there is a failure in one of the Availability Zones.

upvoted 4 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B
upvoted 1 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: B

Agreed

upvoted 1 times

  **Shasha1** 1 year, 3 months ago

B

option B This architecture provides high availability by having multiple Availability Zones hosting the same application. This allows for redundancy in case one Availability Zone experiences downtime, as traffic can be served by the other Availability Zone. This solution also increases scalability and performance by allowing traffic to be spread across two Availability Zones.

upvoted 1 times

  **mricee9** 1 year, 4 months ago**Selected Answer: B**

B is rightt

upvoted 1 times

  **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

  **xua81376** 1 year, 4 months ago

B auto scaling i multiple AZ

upvoted 1 times

Question #175

Topic 1

An ecommerce company has an order-processing application that uses Amazon API Gateway and an AWS Lambda function. The application stores data in an Amazon Aurora PostgreSQL database. During a recent sales event, a sudden surge in customer orders occurred. Some customers experienced timeouts, and the application did not process the orders of those customers.

A solutions architect determined that the CPU utilization and memory utilization were high on the database because of a large number of open connections. The solutions architect needs to prevent the timeout errors while making the least possible changes to the application.

Which solution will meet these requirements?

- A. Configure provisioned concurrency for the Lambda function. Modify the database to be a global database in multiple AWS Regions.
- B. Use Amazon RDS Proxy to create a proxy for the database. Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint.
- C. Create a read replica for the database in a different AWS Region. Use query string parameters in API Gateway to route traffic to the read replica.
- D. Migrate the data from Aurora PostgreSQL to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS). Modify the Lambda function to use the DynamoDB table.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability.

<https://aws.amazon.com/id/rds/proxy/>

upvoted 30 times

✉️  **rexxxx_x** 2 months ago

Are you sure?

upvoted 1 times

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

Selected Answer: B

Issue related to opening many connections and the solution requires least code changes so B satisfies the conditions

upvoted 7 times

✉️  **awsgeek75**  2 months, 1 week ago

Selected Answer: B

Connection problems causing high CPU and Memory usage? Use RDS proxy!

upvoted 1 times

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

Selected Answer: B

Use Amazon RDS Proxy to create a proxy for the database. Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint.

upvoted 2 times

✉️  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

using Amazon RDS Proxy and modifying the Lambda function to use the RDS Proxy endpoint is the recommended solution to prevent timeout errors and reduce the impact on the database during peak loads.

upvoted 1 times

✉️  **cookieMr** 9 months ago

Selected Answer: B

Option A (configuring provisioned concurrency and creating a global database) does not directly address the high connection utilization issue on the database, and creating a global database may introduce additional complexity without immediate benefit to solving the timeout errors.

Option C (creating a read replica in a different AWS Region) introduces additional data replication and management complexity, which may not be

necessary to address the timeout errors.

Option D (migrating to Amazon DynamoDB) involves a significant change in the data storage technology and requires modifying the application to use DynamoDB instead of Aurora PostgreSQL. This may not be the most suitable solution when the goal is to make minimal changes to the application.

Therefore, using Amazon RDS Proxy and modifying the Lambda function to use the RDS Proxy endpoint is the recommended solution to prevent timeout errors and reduce the impact on the database during peak loads.

upvoted 6 times

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

its there anyone that would love to share his/her contributor access? please write me frankobinnaeze@gmail.com thanks

upvoted 1 times

✉ **sairam** 1 year, 2 months ago

I also think the answer is B. However can RDS Proxy be used with Amazon Aurora PostgreSQL database?

upvoted 1 times

✉ **everfly** 1 year ago

RDS Proxy can be used with Aurora

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 4 times

✉ **gustavtd** 1 year, 2 months ago

Selected Answer: B

I expect a answer with database replica but there is not, so B is most suitable

upvoted 1 times

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

Selected Answer: B

Option B. Use Amazon RDS Proxy to create a proxy for the database. Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint.

Using Amazon RDS Proxy can help reduce the number of connections to the database and improve the performance of the application. RDS Proxy establishes a connection pool to the database and routes connections to the available connections in the pool. This can help reduce the number of open connections to the database and improve the performance of the application. The Lambda function can be modified to use the RDS Proxy endpoint instead of the database endpoint to take advantage of this improvement.

upvoted 1 times

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

Option A is not a valid solution because configuring provisioned concurrency for the Lambda function does not address the issue of high CPU utilization and memory utilization on the database.

Option C is not a valid solution because creating a read replica in a different Region does not address the issue of high CPU utilization and memory utilization on the database.

Option D is not a valid solution because migrating the data from Aurora PostgreSQL to DynamoDB would require significant changes to the application and may not be the best solution for this particular problem.

upvoted 2 times

✉ **BENICE** 1 year, 3 months ago

Option --- B

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: B

As it is mentioned that issue was due to high CPU and Memory due to many open corrections to DB, B is the right answer.

upvoted 1 times

✉ **Shasha1** 1 year, 3 months ago

B

Using Amazon RDS Proxy will allow the application to handle more connections and higher loads without timeouts, while making the least possible changes to the application. The RDS Proxy will enable connection pooling, allowing multiple connections from the Lambda function to be served from a single proxy connection. This will reduce the number of open connections on the database, which is causing high CPU and memory utilization

upvoted 3 times

✉ **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

✉ **xua81376** 1 year, 4 months ago

B - Proxy to manage connections

upvoted 2 times

✉ **Nigma** 1 year, 4 months ago

Correct B

upvoted 1 times

Question #176

Topic 1

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table.

What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

- A. Use a VPC endpoint for DynamoDB.
- B. Use a NAT gateway in a public subnet.
- C. Use a NAT instance in a private subnet.
- D. Use the internet gateway attached to the VPC.

Correct Answer: D

Community vote distribution

A (100%)

 **mabotega**  1 year, 4 months ago

Selected Answer: A

VPC endpoints for service in private subnets

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

upvoted 13 times

 **cookieMr**  9 months ago

Option B (using a NAT gateway in a public subnet) and option C (using a NAT instance in a private subnet) are not the most secure options because they involve routing traffic through a network address translation (NAT) device, which requires an internet gateway and traverses the public internet.

Option D (using the internet gateway attached to the VPC) would require routing traffic through the internet gateway, which would result in the traffic leaving the AWS network.

Therefore, the recommended and most secure approach is to use a VPC endpoint for DynamoDB to ensure private and secure access to the DynamoDB table from your EC2 instances in private subnets, without the need to traverse the internet or leave the AWS network.

upvoted 6 times

 **vijaykamal**  6 months ago

Selected Answer: A

Using an internet gateway (Option D) is used for enabling outbound internet connectivity from resources in your VPC. It's not the appropriate choice for securely accessing DynamoDB within your VPC.

upvoted 2 times

 **Ramdi1** 6 months, 1 week ago

Selected Answer: A

A gateway VPC Endpoint is designed for supported AWS service such as dynamo db or s3 in this case i assume the endpoint is still the valid option

upvoted 1 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: A

Use a VPC endpoint for DynamoDB. A VPC endpoint enables customers to privately connect to supported AWS services: Amazon DynamoDB or Amazon Simple Storage Service (Amazon S3).

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

A VPC endpoint enables private connectivity between VPCs and AWS services without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect. Traffic remains within the AWS network.

upvoted 1 times

 **MikeDu** 7 months, 2 weeks ago

Selected Answer: A

VPC endpoints for service in private subnets

upvoted 1 times

 **RashiJaiswal** 8 months, 2 weeks ago

Selected Answer: A

VPC endpoint for dynamodb and S3

upvoted 1 times

markw92 9 months, 1 week ago

VPC endpoints for DynamoDB can alleviate these challenges. A VPC endpoint for DynamoDB enables Amazon EC2 instances in your VPC to use their private IP addresses to access DynamoDB with no exposure to the public internet. Your EC2 instances do not require public IP addresses, and you don't need an internet gateway, a NAT device, or a virtual private gateway in your VPC. You use endpoint policies to control access to DynamoDB. Traffic between your VPC and the AWS service does not leave the Amazon network.

upvoted 3 times

dmt6263 10 months, 2 weeks ago

AAAAAAA

upvoted 1 times

gx2222 11 months, 3 weeks ago

Selected Answer: A

Option A: Use a VPC endpoint for DynamoDB - This is the correct option. A VPC endpoint for DynamoDB allows communication between resources in your VPC and Amazon DynamoDB without traversing the internet or a NAT instance, which is more secure.

upvoted 2 times

GalileoEC2 1 year ago

A

The most secure way to access an Amazon DynamoDB table from Amazon EC2 instances in private subnets while ensuring that the traffic does not leave the AWS network is to use Amazon VPC Endpoints for DynamoDB.

Amazon VPC Endpoints enable private communication between Amazon EC2 instances in a VPC and Amazon services such as DynamoDB, without the need for an internet gateway, NAT device, or VPN connection. When you create a VPC endpoint for DynamoDB, traffic from the EC2 instances to the DynamoDB table remains within the AWS network and does not traverse the public internet.

upvoted 1 times

AllGOD 1 year, 1 month ago

private...backend Answer A

upvoted 1 times

bpd123 1 year, 1 month ago

Selected Answer: A

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpointsdynamodb.html>

A VPC endpoint for DynamoDB enables Amazon EC2 instances in your VPC to use their private IP addresses to access DynamoDB with no exposure to the public internet. Your EC2 instances do not require public IP addresses, and you don't need an internet gateway, a NAT device, or a virtual private gateway in your VPC. You use endpoint policies to control access to DynamoDB. Traffic between your VPC and the AWS service does not leave the Amazon network.

upvoted 2 times

ProfXsamson 1 year, 1 month ago

ExamTopics.com should be sued for this answer tagged as Correct answer.

upvoted 4 times

mp165 1 year, 2 months ago

Selected Answer: A

A is correct. VPC end point. D exposed to the internet

upvoted 3 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Selected Answer: A

The most secure way to access the DynamoDB table while ensuring that the traffic does not leave the AWS network is Option A (Use a VPC endpoint for DynamoDB.)

A VPC endpoint for DynamoDB allows you to privately connect your VPC to the DynamoDB service without requiring an Internet Gateway, VPN connection, or AWS Direct Connect connection. This ensures that the traffic between the application and the DynamoDB table stays within the AWS network and is not exposed to the public Internet.

upvoted 2 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Option B, using a NAT gateway in a public subnet, would allow the traffic to leave the AWS network and traverse the public Internet, which is less secure.

Option C, using a NAT instance in a private subnet, would also allow the traffic to leave the AWS network but would require you to manage the NAT instance yourself.

Option D, using the internet gateway attached to the VPC, would also expose the traffic to the public Internet.

upvoted 2 times

Question #177

Topic 1

An entertainment company is using Amazon DynamoDB to store media metadata. The application is read intensive and experiencing delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.

What should a solutions architect recommend to meet this requirement?

- A. Use Amazon ElastiCache for Redis.
- B. Use Amazon DynamoDB Accelerator (DAX).
- C. Replicate data by using DynamoDB global tables.
- D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Correct Answer: B

Community vote distribution


 B (100%)

✉  **techhb**  1 year, 3 months ago

Selected Answer: B

DAX stands for DynamoDB Accelerator, and it's like a turbo boost for your DynamoDB tables. It's a fully managed, in-memory cache that speeds up the read and write performance of your DynamoDB tables, so you can get your data faster than ever before.

upvoted 20 times

✉  **cookieMr**  9 months ago

Selected Answer: B

A. Using Amazon ElastiCache for Redis would require modifying the application code and is not specifically designed to enhance DynamoDB performance.

C. Replicating data with DynamoDB global tables would require additional configuration and operational overhead.

D. Using Amazon ElastiCache for Memcached with Auto Discovery enabled would also require application code modifications and is not specifically designed for improving DynamoDB performance.

In contrast, option B, using Amazon DynamoDB Accelerator (DAX), is the recommended solution as it is purpose-built for enhancing DynamoDB performance without the need for application reconfiguration. DAX provides a managed caching layer that significantly reduces read latency and offloads traffic from DynamoDB tables.

upvoted 9 times

✉  **awsgeek75**  2 months, 3 weeks ago

B: <https://aws.amazon.com/dynamodb/dax/>
improve 10x performance (marketing pitch on above link) with fully managed service so no reconfiguration or operational overhead involved.
upvoted 1 times

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

Selected Answer: B

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available caching service built for Amazon DynamoDB. DAX delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second.

[https://aws.amazon.com/dynamodb/dax/#:~:text=Amazon%20DynamoDB%20Accelerator%20\(-,DAX\),-is%20a%20fully](https://aws.amazon.com/dynamodb/dax/#:~:text=Amazon%20DynamoDB%20Accelerator%20(-,DAX),-is%20a%20fully)
upvoted 1 times

✉  **Abrar2022** 9 months, 4 weeks ago

Selected Answer: B

improve the performance efficiency of DynamoDB
upvoted 1 times

✉  **gx2222** 11 months, 3 weeks ago

Selected Answer: B

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that helps improve the read performance of DynamoDB tables. DAX provides a caching layer between the application and DynamoDB, reducing the number of read requests made directly to DynamoDB. This can significantly reduce read latencies and improve overall application performance.

upvoted 2 times

✉  **osmk** 1 year ago

B-->Applications that are read-intensive==><https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.html#DAX.use-cases>

upvoted 1 times

✉ **LuckyAro** 1 year, 2 months ago

Selected Answer: B

DynamoDB Accelerator, less overhead.

upvoted 2 times

✉ **wmp7039** 1 year, 2 months ago

Option B is incorrect as the constraint in the question is not to recode the application. DAX requires application to be reconfigured and point to DAX instead of DynamoDB

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.client.modify-your-app.html>

Answer should be A

upvoted 2 times

✉ **LoXoL** 2 months, 1 week ago

DAX does not require application logic modification (compatible with existing DynamoDB APIs). ElastiCache would work after changes on app's code.

upvoted 1 times

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

Selected Answer: B

To improve the performance efficiency of DynamoDB without reconfiguring the application, a solutions architect should recommend using Amazon DynamoDB Accelerator (DAX) which is Option B as the correct answer.

DAX is a fully managed, in-memory cache that can be used to improve the performance of read-intensive workloads on DynamoDB. DAX stores frequently accessed data in memory, allowing the application to retrieve data from the cache rather than making a request to DynamoDB. This can significantly reduce the number of read requests made to DynamoDB, improving the performance and reducing the latency of the application.

upvoted 3 times

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

Option A, using Amazon ElastiCache for Redis, would not be a good fit because it is not specifically designed for use with DynamoDB and would require reconfiguring the application to use it.

Option C, replicating data using DynamoDB global tables, would not directly improve the performance of reading requests and would require additional operational overhead to maintain the replication.

Option D, using Amazon ElastiCache for Memcached with Auto Discovery enabled, would also not be a good fit because it is not specifically designed for use with DynamoDB and would require reconfiguring the application to use it.

upvoted 1 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 2 times

✉ **k1kavi1** 1 year, 3 months ago

Selected Answer: B

Agreed

upvoted 2 times

✉ **Shasha1** 1 year, 3 months ago

B

DAX is a fully managed, highly available, in-memory cache for DynamoDB that delivers lightning-fast performance and consistent low-latency responses. It provides fast performance without requiring any application reconfiguration

upvoted 3 times

✉ **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

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

Selected Answer: B

DAX is the cache for this

upvoted 1 times

✉ **nhlegend** 1 year, 4 months ago

B is correct, DAX provides caching + no changes

upvoted 2 times

Question #178

Topic 1

A company's infrastructure consists of Amazon EC2 instances and an Amazon RDS DB instance in a single AWS Region. The company wants to back up its data in a separate Region.

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

- A. Use AWS Backup to copy EC2 backups and RDS backups to the separate Region.
- B. Use Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region.
- C. Create Amazon Machine Images (AMIs) of the EC2 instances. Copy the AMIs to the separate Region. Create a read replica for the RDS DB instance in the separate Region.
- D. Create Amazon Elastic Block Store (Amazon EBS) snapshots. Copy the EBS snapshots to the separate Region. Create RDS snapshots. Export the RDS snapshots to Amazon S3. Configure S3 Cross-Region Replication (CRR) to the separate Region.

Correct Answer: A

Community vote distribution

A (97%)

cookieMr Highly Voted 9 months ago

Selected Answer: A

Using AWS Backup to copy EC2 and RDS backups to the separate Region is the solution that meets the requirements with the least operational overhead. AWS Backup simplifies the backup process and automates the copying of backups to another Region, reducing the manual effort and operational complexity involved in managing separate backup processes for EC2 instances and RDS databases.

Option B is incorrect because Amazon Data Lifecycle Manager (Amazon DLM) is not designed for directly copying RDS backups to a separate region.

Option C is incorrect because creating Amazon Machine Images (AMIs) and read replicas adds complexity and operational overhead compared to a dedicated backup solution.

Option D is incorrect because using Amazon EBS snapshots, RDS snapshots, and S3 Cross-Region Replication (CRR) involves multiple manual steps and additional configuration, increasing complexity.

upvoted 7 times

thewalker Most Recent 1 month, 3 weeks ago

Selected Answer: A

The easiest way to backup an EC2 instance and RDS Database would be to use AWS Backup. With AWS Backup you can:

Create a backup plan and select both the EC2 volume and RDS database for backup.

Choose a backup schedule that meets your requirements, such as daily or weekly backups.

AWS Backup will automatically take snapshots of the EC2 volume and backups of the RDS database as per the configured schedule.

The backups will be stored in S3 for long term retention based on your backup plan configuration.

upvoted 1 times

thewalker 1 month, 3 weeks ago

You can easily restore the EC2 volume or RDS database from these backups in case of data loss or corruption.

AWS manages the entire backup process so there is no operational overhead for you.

Some other options include using cron jobs to trigger snapshots and backups. But AWS Backup provides a fully managed service to centrally backup both EC2 and RDS with minimal effort.

The above is the output from Amazon Q.

upvoted 2 times

Guru4Cloud 7 months, 1 week ago

Selected Answer: A

AWS Backup provides a fully managed, centralized backup service across AWS services. It can be configured to automatically copy backups across Regions.

This requires minimal operational overhead compared to the other options:

upvoted 2 times

oguzbeliren 7 months, 3 weeks ago

D would have been a great option but the questions requires less manual effort. So, A is better.
upvoted 1 times

cheese929 10 months, 3 weeks ago

Selected Answer: A

A is correct
upvoted 2 times

kruasan 11 months ago

Selected Answer: A

Option B, using Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region, would require more operational overhead because DLM is primarily designed for managing the lifecycle of Amazon EBS snapshots, and would require additional configuration to manage RDS backups.

Option C, creating AMIs of the EC2 instances and read replicas of the RDS DB instance in the separate Region, would require more manual effort to manage the backup and disaster recovery process, as it requires manual creation and management of AMIs and read replicas.

upvoted 3 times

kruasan 11 months ago

Option D, creating EBS snapshots and RDS snapshots, exporting them to Amazon S3, and configuring S3 Cross-Region Replication (CRR) to the separate Region, would require more configuration and management effort. Additionally, S3 CRR can have additional charges for data transfer and storage in the destination region.

Therefore, option A is the best choice for meeting the company's requirements with the least operational overhead.

upvoted 3 times

gx2222 11 months, 3 weeks ago

Selected Answer: A

Option A, using AWS Backup to copy EC2 backups and RDS backups to the separate region, is the correct answer for the given scenario.

Using AWS Backup is a simple and efficient way to backup EC2 instances and RDS databases to a separate region. It requires minimal operational overhead and can be easily managed through the AWS Backup console or API. AWS Backup can also provide automated scheduling and retention management for backups, which can help ensure that backups are always available and up to date.

upvoted 3 times

vtbk 1 year, 2 months ago

Selected Answer: A

Cross-Region backup

Using AWS Backup, you can copy backups to multiple different AWS Regions on demand or automatically as part of a scheduled backup plan. Cross-Region backup is particularly valuable if you have business continuity or compliance requirements to store backups a minimum distance away from your production data.

<https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html>

upvoted 4 times

dan80 1 year, 2 months ago

A is correct - you need to find a backup solution for EC2 and RDS. DLM doesn't work with RDS, only with snapshots.

upvoted 1 times

techhb 1 year, 3 months ago

Selected Answer: A

using Amazon DLM to copy EC2 backups and RDS backups to the separate region, is not a valid solution because Amazon DLM does not support backing up data across regions.

upvoted 1 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Selected Answer: B

Option B. Use Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region.

Amazon DLM is a fully managed service that helps automate the creation and retention of Amazon EBS snapshots and RDS DB snapshots. It can be used to create and manage backup policies that specify when and how often snapshots should be created, as well as how long they should be retained. With Amazon DLM, you can easily and automatically create and manage backups of your EC2 instances and RDS DB instances in a separate Region, with minimal operational overhead.

upvoted 1 times

HayLLIHuK 1 year, 2 months ago

Buruguduystunstugudunstuy, sorry, but I haven't found any info about copying RDS backups by DLM. The DLM works only with EBS.

So the only answer is A - AWS Backup

upvoted 1 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Option A, using AWS Backup to copy EC2 backups and RDS backups to the separate Region, would also work, but it may require more manual configuration and management.

Option C, creating AMIs of the EC2 instances and copying them to the separate Region, and creating a read replica for the RDS DB instance in the separate Region, would work, but it may require more manual effort to set up and maintain.

Option D, creating EBS snapshots and copying them to the separate Region, creating RDS snapshots, and exporting them to Amazon S3, and configuring S3 CRR to the separate Region, would also work, but it would involve multiple steps and may require more manual effort to set up and maintain. Overall, using Amazon DLM is likely to be the easiest and most efficient option for meeting the requirements with the least operational overhead.

upvoted 1 times

PassNow1234 1 year, 3 months ago

Some of your answers are very detailed. Can you back them up with a reference?

upvoted 2 times

jwu413 1 year, 1 month ago

All of their answers are from ChatGPT

upvoted 5 times

techhb 1 year, 3 months ago

using Amazon DLM to copy EC2 backups and RDS backups to the separate region, is not a valid solution because Amazon DLM does not support backing up data across regions.

upvoted 4 times

PassNow1234 1 year, 2 months ago

Thanks techhb

upvoted 1 times

egmiranda 1 year, 2 months ago

I choose A, but DLM support cross regions. DLM doesn't support RDS. Cross region copy rules it's a feature of DLM ("For each schedule, you can define the frequency, fast snapshot restore settings (snapshot lifecycle policies only), cross-Region copy rules, and tags")
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>

upvoted 1 times

Kruiz29 1 year, 2 months ago

This guy is giving wrong answers in detail...lol

upvoted 5 times

YogK 10 months, 1 week ago

AWS DLM does not support RDS backups, only works with EBS storage. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>

upvoted 1 times

career360guru 1 year, 3 months ago

Selected Answer: A

Option A as it is fully managed service with least operational overhead

upvoted 1 times

Shasha1 1 year, 3 months ago

A

AWS Backup is a fully managed service that handles the process of copying backups to a separate Region automatically

upvoted 1 times

babaxoxo 1 year, 4 months ago

Selected Answer: A

Ans A with least operational overhead

upvoted 1 times

rjam 1 year, 4 months ago

AWS Backup supports Supports cross-region backups

upvoted 3 times

rjam 1 year, 4 months ago

Selected Answer: A

Option A

Aws back up supports , EC2, RDS

upvoted 3 times

rjam 1 year, 4 months ago

AWS Backup suports Supports cross-region backups

upvoted 1 times

Question #179

Topic 1

A solutions architect needs to securely store a database user name and password that an application uses to access an Amazon RDS DB instance. The application that accesses the database runs on an Amazon EC2 instance. The solutions architect wants to create a secure parameter in AWS Systems Manager Parameter Store.

What should the solutions architect do to meet this requirement?

- A. Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance.
- B. Create an IAM policy that allows read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM policy to the EC2 instance.
- C. Create an IAM trust relationship between the Parameter Store parameter and the EC2 instance. Specify Amazon RDS as a principal in the trust policy.
- D. Create an IAM trust relationship between the DB instance and the EC2 instance. Specify Systems Manager as a principal in the trust policy.

Correct Answer: A

Community vote distribution

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

Selected Answer: A

CORRECT Option A

To securely store a database user name and password in AWS Systems Manager Parameter Store and allow an application running on an EC2 instance to access it, the solutions architect should create an IAM role that has read access to the Parameter Store parameter and allow Decrypt access to an AWS KMS key that is used to encrypt the parameter. The solutions architect should then assign this IAM role to the EC2 instance.

This approach allows the EC2 instance to access the parameter in the Parameter Store and decrypt it using the specified KMS key while enforcing the necessary security controls to ensure that the parameter is only accessible to authorized parties.

upvoted 13 times

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

Option B, would not be sufficient, as IAM policies cannot be directly attached to EC2 instances.

Option C, would not be a valid solution, as the Parameter Store parameter and the EC2 instance are not entities that can be related through an IAM trust relationship.

Option D, would not be a valid solution, as the trust policy would not allow the EC2 instance to access the parameter in the Parameter Store or decrypt it using the specified KMS key.

upvoted 6 times

✉️ **sdasdawa** Highly Voted 1 year, 4 months ago

Selected Answer: A

Agree with A, IAM role is for services (EC2 for example)

IAM policy is more for users and groups

upvoted 7 times

✉️ **awsgeek75** Most Recent 2 months, 1 week ago

Selected Answer: A

policy needs to be assigned to something so B is inaccurate

CD are just made up things

upvoted 1 times

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

Selected Answer: A

Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance

upvoted 1 times

✉️ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

CORRECT Option A

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: A

By creating an IAM role with read access to the Parameter Store parameter and Decrypt access to the associated AWS KMS key, the EC2 will have the necessary permissions to securely retrieve and decrypt the database user name and password from the Parameter Store. This approach ensures that the sensitive information is protected and can be accessed only by authorized entities.

Answers B, C, and D are not correct because they do not provide a secure way to store and retrieve the database user name and password from the Parameter Store. IAM policies, trust relationships, and associations with the DB instance are not the appropriate mechanisms for securely managing sensitive credentials in this scenario. Answer A is the correct choice as it involves creating an IAM role with the necessary permissions and assigning it to the EC2 instance to access the Parameter Store securely.

upvoted 2 times

 **cheese929** 10 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **kruasan** 11 months ago

Selected Answer: A

By creating an IAM role and assigning it to the EC2 instance, the application running on the EC2 instance can access the Parameter Store parameter securely without the need for hard-coding the database user name and password in the application code.

The IAM role should have read access to the Parameter Store parameter and Decrypt access to an AWS KMS key that is used to encrypt the parameter to ensure that the parameter is protected at rest.

upvoted 1 times

 **HayLLIHuK** 1 year, 2 months ago

There should be the Decrypt access to KMS.

"If you choose the SecureString parameter type when you create your parameter, Systems Manager uses AWS KMS to encrypt the parameter value."

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

IAM role - for EC2

upvoted 1 times

 **BENICE** 1 year, 3 months ago

A -- is correct option

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Option A.

upvoted 1 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: A

A is correct

upvoted 1 times

 **Shasha1** 1 year, 3 months ago

Answer A

Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance. This solution will allow the application to securely access the database user name and password stored in the parameter store.

upvoted 1 times

 **[Removed]** 1 year, 3 months ago

Selected Answer: B

i think policy

upvoted 1 times

 **turalmth** 1 year, 3 months ago

can you attach policy to ec2 directly ?

upvoted 2 times

 **[Removed]** 1 year, 3 months ago

<https://aws.amazon.com/blogs/compute/managing-secrets-for-amazon-ecs-applications-using-parameter-store-and-iam-roles-for-tasks/>

upvoted 1 times

 **JayBee65** 1 year, 2 months ago

This link gives the example "Walkthrough: Securely access Parameter Store resources with IAM roles for tasks" - essentially A above. It does not show how this can be done using a policy (B) alone.

upvoted 1 times

 **[Removed]** 1 year, 3 months ago

Access to Parameter Store is enabled by IAM policies and supports resource level permissions for access. An IAM policy that grants permissions to specific parameters or a namespace can be used to limit access to these parameters. CloudTrail logs, if enabled for the service, record any attempt to access a parameter.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

IAM Policies can be attached to IAM roles, and EC2 instances can be allowed to use IAM roles. You can't attach an IAM policy to an EC2 instance.

upvoted 1 times

 **EKA_CloudGod** 1 year, 4 months ago

Selected Answer: A

A. Attach IAM role to EC2 Instance

<https://aws.amazon.com/blogs/security/digital-signing-asymmetric-keys-aws-kms/>

upvoted 1 times

 **babaxoxo** 1 year, 4 months ago

Selected Answer: A

Attach IAM role to EC2 Instance profile

upvoted 3 times

 **goatbernard** 1 year, 4 months ago

Selected Answer: B

IAM policy

upvoted 1 times

Question #180

Topic 1

A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.

Which combination of solutions provides the MOST protection? (Choose two.)

- A. Use AWS WAF to protect the NLB.
- B. Use AWS Shield Advanced with the NLB.
- C. Use AWS WAF to protect Amazon API Gateway.
- D. Use Amazon GuardDuty with AWS Shield Standard
- E. Use AWS Shield Standard with Amazon API Gateway.

Correct Answer: BC

Community vote distribution



✉️ **babaxoxo** Highly Voted 1 year, 4 months ago

Selected Answer: BC

Shield - Load Balancer, CF, Route53
AWS - CF, ALB, API Gateway

upvoted 41 times

✉️ **Ouk** 1 year, 2 months ago

Thank u U meant WAF* - CloudFormation, right? haha
upvoted 5 times

✉️ **YogK** 10 months, 1 week ago

Shield - Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53.
WAF - Amazon CloudFront, the Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync
upvoted 8 times

✉️ **rjam** Highly Voted 1 year, 4 months ago

Selected Answer: BC

AWS Shield Advanced - DDos attacks
AWS WAF to protect Amazon API Gateway, because WAF sits before the API Gateway and then comes NLB.
upvoted 7 times

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

don't agree that NLB sits before API gateway. it should be other way around
upvoted 3 times

✉️ **aadityaravi8** 8 months, 3 weeks ago

yes.. coming from outside to inside... first of all DDos protection is required so the outer most NLB with Shield Advanced and then filter particular request doing SQL injection and all i.e API Gateway with WAF
upvoted 1 times

✉️ **Guru4Cloud** Most Recent 7 months, 1 week ago

Selected Answer: BC

B) Use AWS Shield Advanced with the NLB

C) Use AWS WAF to protect Amazon API Gateway

The key reasons are:

AWS Shield Advanced provides expanded DDoS protection against larger and more sophisticated attacks
Using it with the NLB helps protect against network floods
WAF still provides critical protection against exploits at the API layer
upvoted 3 times

✉️ **Sat897** 7 months, 2 weeks ago

Selected Answer: BC

WAF - can't support NLB and its supports API Gateway

AWS Shield Advanced - NLB - DDOS

upvoted 1 times

 **cookieMr** 9 months ago

B. AWS Shield Advanced provides advanced DDoS protection for the NLB, making it the appropriate choice for protecting against large and sophisticated DDoS attacks at the network layer.

C. AWS WAF is designed to provide protection at the application layer, making it suitable for securing the API Gateway against web exploits like SQL injection.

A. AWS WAF is not compatible with NLB as it operates at the application layer, whereas NLB operates at the transport layer.

D. While GuardDuty helps detect threats, it does not directly protect against web exploits or DDoS attacks. Shield Standard focuses on edge resources, not specifically NLBs.

E. Shield Standard provides basic DDoS protection for edge resources, but it does not directly protect the NLB or address web exploits at the application layer.

upvoted 4 times

 **cheese929** 10 months, 2 weeks ago

Selected Answer: BC

B and C is correct

upvoted 1 times

 **kruasan** 11 months ago

Selected Answer: BC

NLB is a Layer 3/4 component while WAF is a Layer 7 protection component.

That is why WAF is only available for Application Load Balancer in the ELB portfolio. NLB does not terminate the TLS session therefore WAF is not capable of acting on the content. I would consider using AWS Shield at Layer 3/4.

<https://repost.aws/questions/QU2fYXwSWUS0q9vZiWDoaEzA/nlb-need-to-attach-aws-waf>

upvoted 4 times

 **jdr75** 11 months, 3 weeks ago

Selected Answer: C

- A. Use AWS WAF to protect the NLB.

INCORRECT, cos' WAF not integrate with network LB

- B. Use AWS Shield Advanced with the NLB.

YES. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running in AWS. The doubt is : why apply the protection in the NLB when the facing of the app. is the API Gateway?, because Shield should be in front of the communications, not behind.

Nevertheless, this is the best option.

- C. Use AWS WAF to protect Amazon API Gateway.

YES, <https://aws.amazon.com/es/waf/faqs/>

- D. Use Amazon GuardDuty with AWS Shield Standard

INCORRECT, GuardDuty not prevent attacks.

- E. Use AWS Shield Standard with Amazon API Gateway.

INCORRECT. It could be, in principle, a good option, cos' it's in front of the gateway, but the questions said explicitly:

"wants to detect and mitigate large, sophisticated DDoS attacks",

and Standard not provide this feature.

upvoted 1 times

 **kerl** 1 year, 1 month ago

for those who select A, it is wrong, WAF is Layer 7, it only support ABL, APIGateway, CloudFront, COgnito User Pool and AppSync graphQL API (<https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html>). NLB is NOT supported. Answer is BC

upvoted 4 times

 **bullrem** 1 year, 2 months ago

Selected Answer: AB

A and B are the best options to provide the greatest protection for the platform against web vulnerabilities and large, sophisticated DDoS attacks.

Option A: Use AWS WAF to protect the NLB. This will provide protection against common web vulnerabilities such as SQL injection.

Option B: Use AWS Shield Advanced with the NLB. This will provide additional protection against large and sophisticated DDoS attacks.

upvoted 2 times

 **bullrem** 1 year, 2 months ago

The best protection for the platform would be to use A and C together because it will protect both the NLB and the API Gateway from web vulnerabilities and DDoS attacks.

upvoted 1 times

 **omoakin** 10 months ago

correct

upvoted 1 times

 **bullrem** 1 year, 2 months ago

A and C are the best options for protecting the platform against web vulnerabilities and detecting and mitigating large and sophisticated DDoS attacks.

A: AWS WAF can be used to protect the NLB from web vulnerabilities such as SQL injection.

C: AWS WAF can be used to protect Amazon API Gateway and also provide protection against DDoS attacks.

B: AWS Shield Advanced is used to protect resources from DDoS attacks, but it is not specific to the NLB and may not provide the same level of protection as using WAF specifically on the NLB.

D and E: Amazon GuardDuty and AWS Shield Standard are primarily used for threat detection and may not provide the same level of protection as using WAF and Shield Advanced.

upvoted 1 times

 **Arifzefen** 8 months, 2 weeks ago

A is not correct as WAF doesn't support Network Load Balancer

upvoted 2 times

 **drabi** 1 year, 3 months ago

Selected Answer: BC

WS Shield Advanced can help protect your Amazon EC2 instances and Network Load Balancers against infrastructure-layer Distributed Denial of Service (DDoS) attacks. Enable AWS Shield Advanced on an AWS Elastic IP address and attach the address to an internet-facing EC2 instance or Network Load Balancer.<https://aws.amazon.com/blogs/security/tag/network-load-balancers/>

upvoted 2 times

 **duriselvan** 1 year, 3 months ago

Regional resources

You can protect regional resources in all Regions where AWS WAF is available. You can see the list at AWS WAF endpoints and quotas in the Amazon Web Services General Reference.

You can use AWS WAF to protect the following regional resource types:

Amazon API Gateway REST API

Application Load Balancer

AWS AppSync GraphQL API

Amazon Cognito user pool

You can only associate a web ACL to an Application Load Balancer that's within AWS Regions. For example, you cannot associate a web ACL to an Application Load Balancer that's on AWS Outposts.

upvoted 1 times

 **duriselvan** 1 year, 3 months ago

Ans:-a and C

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: AC

CORRECT

A. Use AWS WAF to protect the NLB.

C. Use AWS WAF to protect Amazon API Gateway.

AWS WAF is a web application firewall that helps protect web applications from common web exploits such as SQL injection and cross-site scripting attacks. By using AWS WAF to protect the NLB and Amazon API Gateway, the company can provide an additional layer of protection for its cloud communications platform against these types of web exploits.

upvoted 1 times

 **PassNow1234** 1 year, 3 months ago

Your answer is wrong.

Sophisticated DDOS = Shield Advanced (DDOS attacks the front!) What happens if your load balances goes down?

Your API gateway is on the BACK further behind the NLB. SQL Protect that with the WAF

B and C are right.

upvoted 5 times

 **jwu413** 1 year, 1 month ago

This guy just copies and pastes from ChatGPT.

upvoted 5 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

About AWS Shield Advanced and Amazon GuardDuty

AWS Shield Advanced is a managed DDoS protection service that provides additional protection for Amazon EC2 instances, Amazon RDS DB instances, Amazon Elastic Load Balancers, and Amazon CloudFront distributions. It can help detect and mitigate large, sophisticated DDoS attacks, "but it does not provide protection against web exploits like SQL injection."

Amazon GuardDuty is a threat detection service that uses machine learning and other techniques to identify potentially malicious activity in your AWS accounts. It can be used in conjunction with AWS Shield Standard, which provides basic DDoS protection for Amazon EC2 instances, Amazon RDS DB instances, and Amazon Elastic Load Balancers. However, neither Amazon GuardDuty nor AWS Shield Standard provides protection against web exploits like SQL injection.

Overall, the combination of using AWS WAF to protect the NLB and Amazon API Gateway provides the most protection against web exploits and large, sophisticated DDoS attacks.

upvoted 1 times

 **BENICE** 1 year, 3 months ago

Option B and C

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: BC

B and C

upvoted 1 times

 **tz1** 1 year, 3 months ago

B & C is the answer

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B and C

upvoted 1 times

Question #181

Topic 1

A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.

The company's developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS).

What should a solutions architect recommend for communication between the microservices?

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Add code to the data producers, and publish notifications to the topic. Add code to the data consumers to subscribe to the topic.
- C. Create an AWS Lambda function to pass messages. Add code to the data producers to call the Lambda function with a data object. Add code to the data consumers to receive a data object that is passed from the Lambda function.
- D. Create an Amazon DynamoDB table. Enable DynamoDB Streams. Add code to the data producers to insert data into the table. Add code to the data consumers to use the DynamoDB Streams API to detect new table entries and retrieve the data.

Correct Answer: A

Community vote distribution



Buruguduystunstugudunstuy Highly Voted 1 year, 3 months ago

Selected Answer: A

Option B, using Amazon Simple Notification Service (SNS), would not be suitable for this use case, as SNS is a pub/sub messaging service that is designed for one-to-many communication, rather than point-to-point communication between specific microservices.

Option C, using an AWS Lambda function to pass messages, would not be suitable for this use case, as it would require the data producers and data consumers to have a direct connection and invoke the Lambda function, rather than being decoupled through a message queue.

Option D, using an Amazon DynamoDB table with DynamoDB Streams, would not be suitable for this use case, as it would require the data consumers to continuously poll the DynamoDB Streams API to detect new table entries, rather than being notified of new data through a message queue.

upvoted 15 times

Buruguduystunstugudunstuy 1 year, 3 months ago

Hence, Option A is the correct answer.

Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue.

upvoted 8 times

scar0909 Most Recent 2 weeks, 2 days ago

Selected Answer: A

A for sure

upvoted 1 times

reviewmine 1 month ago

Selected Answer: A

To Decouple a monolithic application - SQS

- SQS standard - not in order
- SQS FIFO - in order

upvoted 1 times

upliftinghut 1 month, 4 weeks ago

Selected Answer: A

Data is processed sequentially, but the order of results does not matter => SQS; if order matters => SQL FIFO

upvoted 1 times

Cloud_A 2 months, 2 weeks ago

Selected Answer: A

A is the answer.

upvoted 1 times

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

Selected Answer: A

Data is processed sequentially, but the order of results does not matter = Amazon Simple Queue Service

upvoted 1 times

✉ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

A) Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue.

For asynchronous communication between decoupled microservices, an SQS queue is the most appropriate service to use.

SQS provides a scalable, highly available queue to buffer messages between producers and consumers.

The order of processing does not matter, so a queue model fits well.

The consumers can scale independently to process messages from the queue.

upvoted 3 times

✉ **cookieMr** 9 months ago

Selected Answer: A

A. Creating an Amazon SQS queue allows for asynchronous communication between microservices, decoupling the data producers and consumers. It provides scalability, flexibility, and ensures that data processing can happen independently and at a desired pace.

B. Amazon SNS is more suitable for pub/sub messaging, where multiple subscribers receive the same message. It may not be the best fit for sequential data processing.

C. Using AWS Lambda functions for communication introduces unnecessary complexity and may not be the optimal solution for sequential data processing.

D. Amazon DynamoDB with DynamoDB Streams is primarily designed for real-time data streaming and change capture scenarios. It may not be the most efficient choice for sequential data processing in a microservices architecture.

upvoted 4 times

✉ **omoakin** 10 months ago

BBBBBBBBBB

upvoted 1 times

✉ **Bmarodi** 10 months ago

Selected Answer: A

SQS for decoupling a monolithic architecture, hence option A is the right answer.

upvoted 1 times

✉ **Madhuaws** 11 months, 3 weeks ago

it also says 'the order of results does not matter'. Option B is correct.

upvoted 1 times

✉ **asoli** 1 year ago

Selected Answer: A

The answer is A.

B is wrong because SNS cannot send events "directly" to ECS.

<https://docs.aws.amazon.com/sns/latest/dg/sns-event-destinations.html>

upvoted 1 times

✉ **user_deleted** 1 year ago

Selected Answer: B

it doesn't say it is one-one relationships , SNS is better

upvoted 3 times

✉ **markw92** 9 months, 1 week ago

watch out for this sentence in the question..."Data needs to process sequentially...."

upvoted 2 times

✉ **career360guru** 1 year, 3 months ago

Selected Answer: A

Best answer is A.

Though C or D is possible it requires additional components and integration and so they are not efficient. Assuming that rate of incoming requests is within limits that SQS can handle A is best option.

upvoted 1 times

✉ **k1kavi1** 1 year, 3 months ago

Selected Answer: A

A is correct

upvoted 1 times

 **Shasha1** 1 year, 3 months ago

answer is B.

An Amazon Simple Notification Service (Amazon SNS) topic can be used for communication between the microservices in this scenario. The data producers can be configured to publish notifications to the topic, and the data consumers can be configured to subscribe to the topic and receive notifications as they are published. This allows for asynchronous communication between the microservices. Question here focus on communication between microservices

upvoted 2 times

 **xua81376** 1 year, 4 months ago

We need decoupling so ok to use SQS

upvoted 2 times

Question #182

Topic 1

A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

- A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
- B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
- C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
- D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Correct Answer: B

Community vote distribution

B (97%)

✉️ **rjam** Highly Voted 1 year, 4 months ago

Selected Answer: B

Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data
Standby DB in Multi-AZ- synchronous replication

Read Replica always asynchronous. so option C is ignored.

upvoted 17 times

✉️ **studynoplay** Highly Voted 10 months, 2 weeks ago

Selected Answer: B

RDS Multi-AZ = Synchronous = Disaster Recovery (DR)
Read Replica = Asynchronous = High Availability
upvoted 11 times

✉️ **pentium75** 2 months, 4 weeks ago

B is correct but the explanation is flawed ;)

RDS Multi-AZ = Synchronous = High Availability
Read Replica = Asynchronous = Disaster Recovery (DR)
upvoted 4 times

✉️ **scar0909** Most Recent 2 weeks, 2 days ago

Selected Answer: B

Multi AZ for availability
upvoted 1 times

✉️ **riyasara** 5 months ago

Option A is incorrect because Amazon RDS does not support synchronous replication to three nodes in three Availability Zones.
Option C is incorrect because while you can create a read replica in a separate AWS Region1, the replication from the primary DB instance to the read replica is asynchronous, not synchronous.
upvoted 3 times

✉️ **cookieMr** 9 months ago

Selected Answer: B

B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.

Enabling Multi-AZ functionality in Amazon RDS ensures synchronous replication of data to a standby replica in a different Availability Zone. This provides high availability and minimizes data loss in the event of a database outage.

A. Creating an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones would provide even higher availability but is not necessary for the stated requirements.

C. Creating a read replica in a separate AWS Region would provide disaster recovery capabilities but does not ensure synchronous replication or meet the requirement of storing every transaction on at least two nodes.

D. Using an EC2 instance with a MySQL engine and triggering an AWS Lambda function for replication introduces unnecessary complexity and is not the most suitable solution for ensuring reliable and synchronous replication.

upvoted 2 times

✉️  **channn** 11 months, 2 weeks ago

Selected Answer: B

B
since all other answers r wrong
upvoted 2 times

✉️  **jayce5** 12 months ago

Selected Answer: B

B
Since read replica is async.
upvoted 1 times

✉️  **LuckyAro** 1 year, 2 months ago

Selected Answer: C

Multi AZ is not as protected as Multi-Region Read Replica.
upvoted 1 times

✉️  **pentium75** 2 months, 4 weeks ago

But is IS protected. Read replica is asynchronous, fails to meet the "store EVERY transaction on at least two nodes" requirement.
upvoted 1 times

✉️  **JayBee65** 1 year, 2 months ago

I curios to know why A isn't right. Is it just that it would take more effort?
upvoted 3 times

✉️  **pentium75** 2 months, 4 weeks ago

How would you implement A?
upvoted 1 times

✉️  **techhb** 1 year, 3 months ago

B is correct C requires more wokr.
upvoted 1 times

✉️  **BENICE** 1 year, 3 months ago

Option B
upvoted 1 times

✉️  **bammy** 1 year, 3 months ago

Multi-AZ will give at least two nodes as required by the question. The answer is B.

Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments with a single standby DB instance.
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>
upvoted 3 times

✉️  **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B
upvoted 1 times

✉️  **Shasha1** 1 year, 3 months ago

Option A is the correct answer in this scenario because it meets the requirements specified in the question. It creates an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones, which will provide high availability and durability for the database, ensuring that the data is stored on multiple nodes and automatically replicated across Availability Zones.

Option B is not a correct answer because it creates an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled, which only provides failover capabilities. It does not enable synchronous replication to multiple nodes, which is required in this scenario.
upvoted 2 times

✉️  **JayBee65** 1 year, 2 months ago

Option B is not incorrect: "The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy and minimize latency spikes during system backups" from
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>
upvoted 1 times

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

I would go with Option B since it meets the company's requirements and is the most suitable solution.

By creating an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled, the solutions architect will ensure that data is automatically synchronously replicated across multiple AZs within the same Region. This provides high availability and data durability, minimizing the risk of data loss and ensuring that every transaction is stored on at least two nodes.
upvoted 1 times

✉️  **stepman** 1 year, 3 months ago

Maybe C since Amazon RDC now supports cross region read replica <https://aws.amazon.com/about-aws/whats-new/2022/11/amazon-rds-sql-server-cross-region-read-replica/>

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **EKA_CloudGod** 1 year, 4 months ago

Selected Answer: B

Option B is the correct answer:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>

upvoted 1 times

Question #183

Topic 1

A company is building a new dynamic ordering website. The company wants to minimize server maintenance and patching. The website must be highly available and must scale read and write capacity as quickly as possible to meet changes in user demand.

Which solution will meet these requirements?

- A. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon DynamoDB with on-demand capacity for the database. Configure Amazon CloudFront to deliver the website content.
- B. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon Aurora with Aurora Auto Scaling for the database. Configure Amazon CloudFront to deliver the website content.
- C. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon DynamoDB with provisioned write capacity for the database.
- D. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon Aurora with Aurora Auto Scaling for the database.

Correct Answer: A

Community vote distribution

A (93%)

7%

✉️  **romko**  1 year, 4 months ago

Selected Answer: A

A - is correct, because Dynamodb on-demand scales write and read capacity
 B - Aurora auto scaling scales only read replicas

upvoted 41 times

✉️  **klayytech** 12 months ago

That's not correct. Amazon Aurora with Aurora Auto Scaling can scale both read and write replicas. Is there anything else you would like me to help you with?

upvoted 5 times

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

That's why Dynamo DB is best suited option

upvoted 1 times

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

Correct...Both can serve purpose but note the keyword "must scale read and write capacity as quickly as possible to meet changes in user demand". DynamoDB can scale quickly than Aurora. Remember "PUSH BUTTON SCALING FEATURE" of Dynamo DB.

upvoted 5 times

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

please is this dump enough to pass the exam?

upvoted 11 times

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

I HOPE SO

upvoted 8 times

✉️  **LuckyAro** 1 year, 1 month ago

You can tell us now ? Going by the date of your post I guess you would have challenged the exam by now ? so how did it go ?

upvoted 8 times

✉️  **Cloud_A**  2 months, 2 weeks ago

Selected Answer: A

[https://aws.amazon.com/blogs/database/how-to-determine-if-amazon-dynamodb-is-appropriate-for-your-needs-and-then-plan-your-migration/#:~:text=Are%20working%20with%20an%20online%20transaction%20processing%20\(OLTP\)%20workload.%20High%2Dperformance%20reads%20and%20writes%20are%20easy%20to%20manage%20with%20DynamoDB%2C%20and%20you%20can%20expect%20performance%20that%20is%20effectively%20constant%20across%20widely%20varying%20loads.](https://aws.amazon.com/blogs/database/how-to-determine-if-amazon-dynamodb-is-appropriate-for-your-needs-and-then-plan-your-migration/#:~:text=Are%20working%20with%20an%20online%20transaction%20processing%20(OLTP)%20workload.%20High%2Dperformance%20reads%20and%20writes%20are%20easy%20to%20manage%20with%20DynamoDB%2C%20and%20you%20can%20expect%20performance%20that%20is%20effectively%20constant%20across%20widely%20varying%20loads.)

upvoted 1 times

✉️  **awsgeek75** 2 months, 3 weeks ago

Selected Answer: A

C,D are out due to EC2 scaling which is not ideal for static content scaling.

A and B are logical choices. B uses Aurora which is more for relational database and comes with the baggage and limitations of RDBMS scaling.

Dynamodb (no SQL) is easier to scale for both read and write. A is simply better than B for an ordering website so that is the better option. Note that B would have been good if A wasn't a choice.

upvoted 2 times

 **tom_cruise** 5 months, 2 weeks ago

Selected Answer: A
dynamodb is serverless
upvoted 2 times

 **Angryasianxd** 6 months, 1 week ago

Selected Answer: A
Hi all! The answer is A and NOT B on this one as the company is building an ordering website (OLTP). DynamoDB's high performance read and writes are perfect for an OLTP use case.

<https://aws.amazon.com/blogs/database/how-to-determine-if-amazon-dynamodb-is-appropriate-for-your-needs-and-then-plan-your-migration/>
upvoted 2 times

 **n0pz** 6 months, 1 week ago

S3 is discarded since the question says: A company is building a new dynamic ordering website,
upvoted 1 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: A
minimize server maintenance and patching, highly available, scale read and write = serverless = Amazon S3, Amazon API Gateway, AWS Lambda, Amazon DynamoDB
upvoted 1 times

 **DebAwsAccount** 6 months, 2 weeks ago

Selected Answer: A
Key phrase in the Question is must scale read and write capacity. Aurora is only for Read.
Amazon DynamoDB has two read/write capacity modes for processing reads and writes on your tables:
On-demand
Provisioned (default, free-tier eligible)
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>
upvoted 2 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A
Minimize maintenance & Patching = Serverless
S3, DynamoDB are serverless
upvoted 1 times

 **ravindrabagale** 7 months, 2 weeks ago

Minimize maintenance & Patching = Serverless services
Serverless services with no sql database is perfect combination
upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: A
B. This solution leverages serverless technologies like API Gateway and Lambda for hosting dynamic content, reducing server maintenance and patching. Aurora with Aurora Auto Scaling provides a highly available and scalable database solution. Hosting static content in S3 and configuring CloudFront for content delivery ensures high availability and efficient scaling.

A. Using DynamoDB with on-demand capacity may provide scalability, but it does not offer the same level of flexibility and performance as Aurora. Additionally, it does not address the hosting of dynamic content using serverless technologies.

C. Hosting all the website content on EC2 instances requires server maintenance and patching. While using ASG and an ALB helps with availability and scalability, it does not minimize server maintenance as requested.

D. Hosting all the website content on EC2 instances introduces server maintenance and patching. Using Aurora with Aurora Auto Scaling is a good choice for the database, but it does not address the need to minimize server maintenance and patching for the overall infrastructure.
upvoted 1 times

 **dydzah** 9 months, 4 weeks ago

B isn't correct because of cooldown
You can tune the responsiveness of a target-tracking scaling policy by adding cooldown periods that affect scaling your Aurora DB cluster in and out. A cooldown period blocks subsequent scale-in or scale-out requests until the period expires. These blocks slow the deletions of Aurora Replicas in your Aurora DB cluster for scale-in requests, and the creation of Aurora Replicas for scale-out requests.
upvoted 1 times

 **Abrar2022** 9 months, 4 weeks ago

Key word in question "storing ordering data"
DynamoDB is perfect for storing ordering data (key-values)
upvoted 2 times

 **studynoplay** 10 months, 2 weeks ago

Selected Answer: A

Minimize maintenance & Patching = Serverless
S3, DynamoDB are serverless

upvoted 2 times

✉ **lucdt4** 10 months, 2 weeks ago

The company wants to minimize server maintenance and patching -> Serverless (minimize)
C,D are wrong because these are not serverless
B is wrong because RDS is not serverless
-> A full serverless

upvoted 1 times

✉ **yyuussaaa** 6 months, 2 weeks ago

For anyone who is confused about Option B, there's a serverless Aurora service called "Aurora Serverless v2". This will bring us an equivalent solution to option A. But the Option B in the question only states the Aurora, therefore by default we need to manage the servers underneath.
Ref: <https://www.projectpro.io/article/aws-aurora-vs-rds/737#:~:text=RDS%20is%20a%20fully%2Dmanaged,manual%20management%20of%20database%20servers>.

upvoted 2 times

✉ **DavidNamy** 1 year, 2 months ago

Selected Answer: B

The correct answer is B.

The option A would also meet the company's requirements of minimizing server maintenance and patching, and providing high availability and quick scaling for read and write capacity. However, there are a few reasons why option B is a more optimal solution:

In option A, it uses Amazon DynamoDB with on-demand capacity for the database, which may not provide the same level of scalability and performance as using Amazon Aurora with Aurora Auto Scaling.
Amazon Aurora offers additional features such as automatic failover, read replicas, and backups that makes it a more robust and resilient option than DynamoDB. Additionally, the auto scaling feature is better suited to handle the changes in user demand.
Additionally, option B provides a more cost-effective solution, as Amazon Aurora can be more cost-effective for high read and write workloads than Amazon DynamoDB, and also it's providing more features.

upvoted 3 times

✉ **Joxtat** 1 year, 1 month ago

The answer is A.

Key phrase in the Question is must scale read and write capacity. Aurora is only for Read.

Amazon DynamoDB has two read/write capacity modes for processing reads and writes on your tables:

On-demand

Provisioned (default, free-tier eligible)

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>

upvoted 3 times

Question #184

Topic 1

A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections. All non-VPC traffic routes to the virtual private gateway.

A development team recently created an AWS Lambda function through the console. The development team needs to allow the function to access a database that runs in a private subnet in the company's data center.

Which solution will meet these requirements?

- A. Configure the Lambda function to run in the VPC with the appropriate security group.
- B. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.
- C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
- D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Correct Answer: C

Community vote distribution



✉️ **Gil80** 1 year, 3 months ago

Selected Answer: A

To configure a VPC for an existing function:

1. Open the Functions page of the Lambda console.
2. Choose a function.
3. Choose Configuration and then choose VPC.
4. Under VPC, choose Edit.
5. Choose a VPC, subnets, and security groups. <-- **That's why I believe the answer is A**.

Note:

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 16 times

✉️ **markw92** 9 months, 1 week ago

The question says on-prem database...how do we create a SG for that instance in AWS? C make sense. my 2 cents..

upvoted 4 times

✉️ **AZ_Master** 4 months ago

A is correct. To configure SG for Lambda , go to Lambda function -> Configure -> Edit VPC and scroll down to see "security groups" where you can configure Lambda for VPC.

Also see here

<https://repost.aws/questions/QUSSaj1a6jBQ92Kp56klbZFNw/aws-lambda-to-on-premise-via-direct-connect-and-aws-privatelink>

upvoted 1 times

✉️ **javitech83** 1 year, 3 months ago

Selected Answer: A

it is A. C is not correct at all as in the question it metions that the VPC already has connectivity with on-premises

upvoted 9 times

✉️ **LuckyAro** 1 year, 2 months ago

C says to "update the route table" not create a new connection. C is correct.

upvoted 3 times

✉️ **ruqui** 9 months, 3 weeks ago

C is wrong. Lambda can't connect by default to resources in a private VPC, so you have to do some specific setup steps to run in a private VPC, Answer A is correct

upvoted 2 times

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

No need to do route updates. This is because the route to the destination on-premises is already set.

upvoted 4 times

✉️ **awsgeek75** 2 months, 1 week ago

Every time I read this question the badly phrased options make no sense at all. I now want to vote for A but it makes no sense.
 Question says: All non-VPC traffic routes to the virtual private gateway
 So Lambda is technically a non VPC traffic too. This means it already goes through the VPGW but we don't know what it connects. Assuming it connect the data-centre to AWS then A makes sense. BUT all this is based on different interpretation now for me.
 upvoted 5 times

 **pentium75** 2 months, 2 weeks ago

Selected Answer: A

The wording is strange because technically, the Lambda function does not "run in the VPC", rather it is connected to the VPC, but otherwise A is what relevant documentation says - connect the Lambda function to the VPN and allow traffic in the security group.

Not B, we have Direct Connect, no need for VPN.

Not C, route is already in place. And route alone does not help - the "route tables in the VPC" are completely irrelevant as long as we don't connect the Lambda function to the VPC.

Not D, an "Elastic IP address" is always connected to an "elastic network interface", such is created automatically with A.

upvoted 4 times

 **Kanagarajd** 2 weeks, 2 days ago

I agree with explanation!

upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

Selected Answer: C

The question and options are very badly worded so it makes C a possible candidate (unconvincingly though!).

B: VPN is not needed as Direct Connect is already there

D: Irrelevant

A is too generic (appropriate security group for what?) Lambda has fixed VPC or ENI

C is logically relevant

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

A says "configure the Lambda function to RUN IN the VPC", but "a Lambda function ALWAYS runs inside a VPC owned by the Lambda service" (<https://docs.aws.amazon.com/lambda/latest/dg/foundation-networking.html>). "You can configure a Lambda function to CONNECT TO private subnets in a virtual private cloud (VPC) in your AWS account", but "connect to" is not the same as "run in" (<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html>). Otherwise A would make sense (you CAN assign a security group to the Elastic Network Interface that Lambda uses to connect to your VPC).

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

B We already have Direct Connect, so why set up VPN

C doesn't make sense because "all non-VPC traffic [already] routes to the virtual private gateway" (which is obviously connected to the Direct Connect gateway), so why should you "update the route tables"?

D sounds plausible; however, an Elastic IP address is associated with an Elastic Network Interface (though that is automatically provided by AWS). So the "without an elastic network interface" makes D wrong.

My best guess is that there's a typo or misunderstanding in the answers. It's either A but it should read "connect to the VPC" instead of "run in the VPC", or it's D but it should read "without CREATING an elastic network interface" or "WITH an elastic network interface".

upvoted 1 times

 **xdkonorek2** 4 months, 2 weeks ago

Selected Answer: C

it's not A:

A Lambda function always runs inside a VPC owned by the Lambda service.

<https://docs.aws.amazon.com/lambda/latest/dg/foundation-networking.html>

upvoted 1 times

 **liux99** 4 months, 2 weeks ago

The answer is C. The question is to allow lambda to access the database running in private subnet in the corporate data center. The only connectivity with the data center is Direct connect.

upvoted 2 times

 **Igogor** 5 months, 1 week ago

Answer C is correct:

<https://repost.aws/questions/QUSSaj1a6jBQ92Kp56klbZFNw/aws-lambda-to-on-premise-via-direct-connect-and-aws-privatelink>

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

Go to the Lambda console.

Click the Functions tab.

Select the Lambda function that you want to configure.

Click the Configuration tab.

In the Network section, select the VPC that you want the function to run in.

In the Security groups section, select the security group that you want to allow the function to access the database subnet.

Click the Save button.

upvoted 3 times

 **zjcorpuz** 8 months ago

Correct answer is A

Lambda is available in the Region by default.. if you want to connect it to your private subnet or to on prem data center you must configure your Lambda with vpc..

C is wrong because there is no help adding routes to VPC without configuring your lambda to vpc.

upvoted 2 times

 **cookieMr** 9 months ago

Selected Answer: A

Option A: Configure the Lambda function to run in the VPC with the appropriate security group. This allows the Lambda function to access the database in the private subnet of the company's data center. By running the Lambda function in the VPC, it can communicate with resources in the private subnet securely.

Option B is incorrect because setting up a VPN connection and routing the traffic from the Lambda function through the VPN would add unnecessary complexity and overhead.

Option C is incorrect because updating the route tables in the VPC to allow access to the on-premises data center through Direct Connect would affect the entire VPC's routing, potentially exposing other resources to the on-premises network.

Option D is incorrect because creating an Elastic IP address and sending traffic through it without an elastic network interface is not a valid configuration for accessing resources in a private subnet.

upvoted 4 times

 **cheese929** 10 months, 3 weeks ago

Selected Answer: C

My answer is C. Refer to the steps in the link. need to configure the routing table to route traffic to the destination.

<https://aws.amazon.com/blogs/compute/running-aws-lambda-functions-on-aws-outposts-using-aws-iot-greengrass/>

A is wrong as it says configure the lambda function in the VPC. the requirement to run in the database that is on-premise.

upvoted 6 times

 **kruasan** 11 months ago

Selected Answer: A

once you have configured your Lambda to be deployed (or connected) to your VPC [1], as long as your VPC has connectivity to your data center, it will be allowed to route the traffic towards it - whether it uses Direct Connect or other connections, like VPN.

<https://repost.aws/questions/QU8aj1a6jBQ92Kp56klbZFNw/questions/QU8aj1a6jBQ92Kp56klbZFNw/aws-lambda-to-on-premise-via-direct-connect-and-aws-privatelink?>

upvoted 2 times

 **Jinius83** 11 months, 1 week ago

C

AWS -> 회사 데이터 센터로 나가는 트래픽이기 때문에

upvoted 3 times

 **darn** 11 months, 1 week ago

english please

upvoted 4 times

 **youdelin** 5 months, 2 weeks ago

dude, english

upvoted 1 times

 **4fad2f8** 2 months, 2 weeks ago

zzzzzzz

upvoted 1 times

 **datz** 11 months, 3 weeks ago

Selected Answer: A

CORRECT ANSWER = A,

C = WRONG because in question, it is telling non VPN traffic is being sent through virtual private gateway(Direct Connect), meaning all routes are looking towards on prem where out destination service is located. So no routing change will be needed.

When you create Lambda(Function) - > you need to choose VPN and than Security group inside VPC.

Link for better understanding :

https://www.youtube.com/watch?v=beV1AYyhgYA&ab_channel=DigitalCloudTraining

upvoted 4 times

 **datz** 11 months, 3 weeks ago

it is telling non "VPC" traffic, really wish there was edit function lol

upvoted 1 times

 **Devsin2000** 1 year ago

In my opinion this question is flawed. Non of the answers makes any sense to me. However, if I have to choose one I will choose C. There is no option of associating Security Group with Lambda function.

upvoted 2 times

Question #185

Topic 1

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.

How can a solutions architect ensure that the application has permission to access Amazon S3?

- A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
- B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.
- C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
- D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

To ensure that an Amazon Elastic Container Service (ECS) application has permission to access Amazon Simple Storage Service (S3), the correct solution is to create an AWS Identity and Access Management (IAM) role with the necessary S3 permissions and specify that role as the taskRoleArn in the task definition for the ECS application.

Option B, creating an IAM role with S3 permissions and specifying that role as the taskRoleArn in the task definition, is the correct solution to meet the requirement.

upvoted 7 times

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

Option A, updating the S3 role in IAM to allow read/write access from ECS and relaunching the container, is not the correct solution because the S3 role is not associated with the ECS application.

Option C, creating a security group that allows access from ECS to S3 and updating the launch configuration used by the ECS cluster, is not the correct solution because security groups are used to control inbound and outbound traffic to resources, and do not grant permissions to access resources.

Option D, creating an IAM user with S3 permissions and relaunching the EC2 instances for the ECS cluster while logged in as this account, is not the correct solution because it is generally considered best practice to use IAM roles rather than IAM users to grant permissions to resources.

upvoted 8 times

✉  **Guru4Cloud** Most Recent 6 months, 2 weeks ago

Selected Answer: B

B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition

upvoted 2 times

✉  **cookieMr** 9 months ago

Selected Answer: B

Option B: Create an IAM role with S3 permissions and specify that role as the taskRoleArn in the task definition. This approach allows the ECS task to assume the specified role and gain the necessary permissions to access Amazon S3.

Option A is incorrect because updating the S3 role in IAM and relaunching the container does not associate the updated role with the ECS task.

Option C is incorrect because creating a security group that allows access from Amazon ECS to Amazon S3 does not grant the necessary permissions to the ECS task.

Option D is incorrect because creating an IAM user with S3 permissions and relaunching the EC2 instances for the ECS cluster does not associate the IAM user with the ECS task.

upvoted 2 times

✉  **dydzah** 9 months, 4 weeks ago

<https://repost.aws/knowledge-center/ecs-fargate-access-aws-services>

upvoted 1 times

✉  **k1kavi1** 1 year, 3 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/27954-exam-aws-certified-solutions-architect-associate-saa-c02/>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ecs-taskdefinition.html>

upvoted 1 times

 **techhb** 1 year, 3 months ago

Selected Answer: B

The short name or full Amazon Resource Name (ARN) of the AWS Identity and Access Management role that grants containers in the task permission to call AWS APIs on your behalf.

upvoted 2 times

 **BENICE** 1 year, 3 months ago

Option B

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B.

upvoted 2 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: B

Agreed

upvoted 1 times

 **lighrz** 1 year, 3 months ago

Selected Answer: B

B is the best answer

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **taer** 1 year, 4 months ago

Selected Answer: B

The answer is B.

upvoted 1 times

 **Nigma** 1 year, 4 months ago

B is the answer

upvoted 2 times

Question #186

Topic 1

A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zone:

What should a solutions architect do to meet this requirement?

- A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.
- B. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.
- C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.
- D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Correct Answer: B

Community vote distribution



B (100%)

✉️  **Nigma**  1 year, 4 months ago

Correct is B
 FSx --> shared Windows file system (SMB)
 EFS --> Linux NFS
 upvoted 8 times

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

Selected Answer: B
 Windows file system = Amazon FSx for Windows File Server
 upvoted 1 times

✉️  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B
 Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.
 upvoted 1 times

✉️  **cookieMr** 9 months ago

Selected Answer: B
 Option B: Configure Amazon FSx for Windows File Server. This service provides a fully managed Windows file system that can be easily shared across multiple EC2 Windows instances. It offers high performance and supports Windows applications that require file storage.

Option A is incorrect because AWS Storage Gateway in volume gateway mode is not designed for shared file systems.

Option C is incorrect because while Amazon EFS can be mounted to multiple instances, it is a Linux-based file system and may not be suitable for Windows applications.

Option D is incorrect because attaching and mounting an Amazon EBS volume to multiple instances simultaneously is not supported.
 upvoted 2 times

✉️  **Bmarodi** 10 months ago

Selected Answer: B
 Option B is right answer.
 upvoted 1 times

✉️  **k1kavi1** 1 year, 3 months ago

Selected Answer: B
 References :
<https://www.examtopics.com/discussions/amazon/view/28006-exam-aws-certified-solutions-architect-associate-saa-c02/>
<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/wfsx-volumes.html>
 upvoted 1 times

✉️  **techhb** 1 year, 3 months ago

Selected Answer: B
 EFS is not compatible with Windows.
<https://pilotcoresystems.com/insights/ebs-efs-fsx-s3-how-these-storage-options-differ/#:~:text=EFS%20works%20with%20Linux%20and,with%20all%20Windows%20Server%20platforms.>
 upvoted 1 times

 **Burugduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: B

A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.

This option is incorrect because AWS Storage Gateway is not a file storage service. It is a hybrid storage service that allows you to store data in the cloud while maintaining low-latency access to frequently accessed data. It is designed to integrate with on-premises storage systems, not to provide file storage for Amazon EC2 instances.

B. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.

This is the correct answer. Amazon FSx for Windows File Server is a fully managed file storage service that provides a native Windows file system that can be accessed over the SMB protocol. It is specifically designed for use with Windows-based applications, and it can be easily integrated with existing applications by mounting the file system to each EC2 instance.

upvoted 3 times

 **Burugduystunstugudunstuy** 1 year, 3 months ago

C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.

This option is incorrect because Amazon EFS is a file storage service that is designed for use with Linux-based applications. It is not compatible with Windows-based applications, and it cannot be accessed over the SMB protocol.

D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

This option is incorrect because Amazon EBS is a block storage service, not a file storage service. It is designed for storing raw block-level data that can be accessed by a single EC2 instance at a time. It is not designed for use as a shared file system that can be accessed by multiple instances.

upvoted 1 times

 **BENICE** 1 year, 3 months ago

B - is correct

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: B

Option B

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

B is correct

upvoted 1 times

 **xua81376** 1 year, 4 months ago

B FSx for windows

upvoted 1 times

 **BENICE** 1 year, 4 months ago

B is correct option

upvoted 1 times

 **rjam** 1 year, 4 months ago

Selected Answer: B

Amazon FSx for Windows File Server

upvoted 3 times

Question #187

Topic 1

A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.

Which solutions meet these requirements? (Choose two.)

- A. Create an Amazon RDS DB instance in Multi-AZ mode.
- B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
- C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
- E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Correct Answer: AD

Community vote distribution

AD (100%)

✉️  **techhb**  1 year, 3 months ago

Selected Answer: AD

<https://containersonaws.com/introduction/ec2-or-aws-fargate/>

A.(O) multi-az <= 'little intervention'

B.(X) read replica <= Promoting a read replica to be a standalone DB instance

You can promote a read replica into a standalone DB instance. When you promote a read replica, the DB instance is rebooted before it becomes available.

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

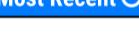
C.(X) use Amazon ECS instead of EC2-based docker for little human intervention

D.(O) Amazon ECS on AWS Fargate : AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances.

E.(X) EC2 launch type

The EC2 launch type can be used to run your containerized applications on Amazon EC2 instances that you register to your Amazon ECS cluster and manage yourself.

upvoted 11 times

✉️  **lostmagnet001**  1 month, 3 weeks ago

Selected Answer: AD

Highly available application - Amazon RDS DB instance in Multi-AZ

little manual intervention - Fargate

upvoted 1 times

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

Selected Answer: AD

highly available application, little manual intervention = serverless = Amazon Elastic Container Service with Fargate and Amazon RDS DB instance in Multi-AZ mode

upvoted 1 times

✉️  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: AD

The correct answers are A and D.

A) Creating an RDS DB instance in Multi-AZ mode provides automatic failover to a standby replica in another Availability Zone, providing high availability.

D) Using ECS Fargate removes the need to provision and manage EC2 instances, allowing the service to scale dynamically based on demand. ECS handles load balancing and availability out of the box.

upvoted 1 times

✉️  **jkirancdev** 8 months ago

Selected Answer: AD

AD is the correct answer

upvoted 1 times

✉️  **cookieMr** 9 months ago

Selected Answer: AD

A. Create an Amazon RDS DB instance in Multi-AZ mode. This ensures that the database is highly available with automatic failover to a standby replica in another Availability Zone.

D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load. Fargate abstracts the underlying infrastructure, automatically scaling and managing the containers, making it a highly available and low-maintenance option.

Option B is not the best choice as it only creates replicas in another Availability Zone without the automatic failover capability provided by Multi-AZ mode.

Option C is not the best choice as managing a Docker cluster on EC2 instances requires more manual intervention compared to using the serverless capabilities of Fargate in option D.

Option E is not the best choice as it uses the EC2 launch type, which requires managing and scaling the EC2 instances manually. Fargate, as mentioned in option D, provides a more automated and scalable solution.

upvoted 3 times

 **studynoplay** 10 months, 2 weeks ago

Selected Answer: AD

little manual intervention = Serverless

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: AD

Option A&D

upvoted 1 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: AD

A and D

upvoted 1 times

 **Gabs90** 1 year, 4 months ago

Selected Answer: AD

A and D

upvoted 1 times

 **Wpcorgan** 1 year, 4 months ago

A and D

upvoted 1 times

 **BENICE** 1 year, 4 months ago

A and D are the options

upvoted 1 times

 **Danny23132412141_2312** 1 year, 4 months ago

AD for sure

Link: <https://www.examtopics.com/discussions/amazon/view/43729-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 4 times

Question #188

Topic 1

A company uses Amazon S3 as its data lake. The company has a new partner that must use SFTP to upload data files. A solutions architect needs to implement a highly available SFTP solution that minimizes operational overhead.

Which solution will meet these requirements?

- A. Use AWS Transfer Family to configure an SFTP-enabled server with a publicly accessible endpoint. Choose the S3 data lake as the destination.
- B. Use Amazon S3 File Gateway as an SFTP server. Expose the S3 File Gateway endpoint URL to the new partner. Share the S3 File Gateway endpoint with the new partner.
- C. Launch an Amazon EC2 instance in a private subnet in a VPC. Instruct the new partner to upload files to the EC2 instance by using a VPN. Run a cron job script, on the EC2 instance to upload files to the S3 data lake.
- D. Launch Amazon EC2 instances in a private subnet in a VPC. Place a Network Load Balancer (NLB) in front of the EC2 instances. Create an SFTP listener port for the NLB. Share the NLB hostname with the new partner. Run a cron job script on the EC2 instances to upload files to the S3 data lake.

Correct Answer: D

Community vote distribution

A (100%)

 **roxx529** Highly Voted  10 months ago

For Exam :
Whenever you see SFTP , FTP look for "Transfer" in options available
upvoted 43 times

 **LoXoL** 2 months, 1 week ago
+ FTPS
upvoted 2 times

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

Answer is A
AWS Transfer Family securely scales your recurring business-to-business file transfers to AWS Storage services using SFTP, FTPS, FTP, and AS2 protocols.
<https://aws.amazon.com/aws-transfer-family/>
upvoted 14 times

 **oguzbeliren** 7 months, 3 weeks ago

Answer A is not an answer because it requires more manual effort. While AWS Transfer Family simplifies the setup of an SFTP server, it still requires management and monitoring. This includes handling scaling, backups, patching, and other administrative tasks associated with managing an SFTP server.
upvoted 2 times

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

Selected Answer: A

The key advantages of AWS Transfer Family are:
It provides a fully managed file transfer service that eliminates the need to manage your own file transfer infrastructure. This reduces operational overhead.
It supports multiple protocols like SFTP, FTPS, FTP and AS2, allowing easy and secure exchange of data with business partners and customers.
File transfers happen directly into Amazon S3 buckets or Amazon EFS file systems, so the transferred data can be easily accessed by other AWS services for analytics, processing etc.
AWS Transfer Family maintains existing client-side configurations, so file transfer workflows remain unchanged for end users and partners.
It provides high availability and auto-scaling capabilities to handle varying transfer workloads.
upvoted 1 times

 **thewalker** 1 month, 3 weeks ago

Storing transferred files in AWS allows using a broad range of services for compliance, archiving and deriving insights from the data.
AWS manages the file transfer infrastructure so you don't have to provision, operate and maintain file transfer servers.
For more details on AWS Transfer Family features, pricing and quotas, please refer to the documentation at <https://aws.amazon.com/transfer-family>
upvoted 1 times

 **ansagr** 3 months, 2 weeks ago

Selected Answer: A

Amazon S3 File Gateway, involves deploying an on-premises gateway that interfaces with S3. While it's a valid solution, it introduces a level of on-premises infrastructure that may require more operational management.

upvoted 1 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: A

AWS Transfer Family securely scales your recurring business-to-business file transfers to AWS Storage services using SFTP, FTPS, FTP, and AS2 protocols.

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

A is the correct answer.

AWS Transfer Family provides a fully managed SFTP service that can integrate directly with S3. It handles scaling, availability, and security automatically with minimal overhead.

upvoted 2 times

 **oguzbeliren** 7 months, 3 weeks ago

AWS Transfer Family is a fully managed service that makes it easy to set up and manage secure file transfers. It provides a high-availability SFTP server that can be accessed from the public internet. However, this solution does not minimize operational overhead, as it requires the solutions architect to manage the SFTP server.

upvoted 1 times

 **cookieMr** 8 months, 3 weeks ago

Selected Answer: A

This solution provides a highly available SFTP solution without the need for manual management or operational overhead. AWS Transfer Family allows you to easily set up an SFTP server with authentication, authorization, and integration with S3 as the storage backend.

Option B is not the best choice as it suggests using Amazon S3 File Gateway, which is primarily used for file-based access to S3 storage over NFS or SMB protocols, not for SFTP access.

Option C is not the best choice as it requires manual management of an EC2 instance, VPN setup, and cron job script for uploading files, introducing operational overhead and potential complexity.

Option D is not the best choice as it also requires manual management of EC2 instances, Network Load Balancer, and cron job scripts for file uploads. It is more complex and involves additional components compared to the simpler and fully managed solution provided by AWS Transfer Family in option A.

upvoted 3 times

 **cookieMr** 9 months ago

This solution provides a highly available SFTP solution without the need for manual management or operational overhead. AWS Transfer Family allows you to easily set up an SFTP server with authentication, authorization, and integration with S3 as the storage backend.

Option B is not the best choice as it suggests using Amazon S3 File Gateway, which is primarily used for file-based access to S3 storage over NFS or SMB protocols, not for SFTP access.

Option C is not the best choice as it requires manual management of an EC2 instance, VPN setup, and cron job script for uploading files, introducing operational overhead and potential complexity.

Option D is not the best choice as it also requires manual management of EC2 instances, Network Load Balancer, and cron job scripts for file uploads. It is more complex and involves additional components compared to the simpler and fully managed solution provided by AWS Transfer Family in option A.

upvoted 2 times

 **cookieMr** 9 months ago

A is correct

upvoted 1 times

 **markw92** 9 months, 1 week ago

I can't wrap my head around why the answer is D? this is so frustrating to see where i went wrong. I vote for A.

upvoted 3 times

 **studynoplay** 10 months, 2 weeks ago

Selected Answer: A

minimizes operational overhead = Serverless

AWS Transfer Family is serverless

upvoted 1 times

 **Rahulbit34** 10 months, 3 weeks ago

AWS Transfer Family is compatible for SFTP<FTPS<FTP. A is the answer

upvoted 1 times

 **kruasan** 11 months ago

Selected Answer: A

AWS Transfer Family is a fully managed AWS service that you can use to transfer files into and out of Amazon Simple Storage Service (Amazon S3) storage or Amazon Elastic File System (Amazon EFS) file systems over the following protocols:

Secure Shell (SSH) File Transfer Protocol (SFTP): version 3
File Transfer Protocol Secure (FTPS)
File Transfer Protocol (FTP)
Applicability Statement 2 (AS2)
upvoted 2 times

 **Oyz** 11 months, 2 weeks ago

Selected Answer: A

A - is the correct answer.
upvoted 2 times

 **BENICE** 1 year, 3 months ago

A -- is the option
upvoted 3 times

 **career360guru** 1 year, 3 months ago

Selected Answer: A

Option A
upvoted 3 times

 **mj98** 1 year, 3 months ago

Selected Answer: A

AWS Transfer Family - SFTP
upvoted 2 times

Question #189

Topic 1

A company needs to store contract documents. A contract lasts for 5 years. During the 5-year period, the company must ensure that the documents cannot be overwritten or deleted. The company needs to encrypt the documents at rest and rotate the encryption keys automatically every year.

Which combination of steps should a solutions architect take to meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Store the documents in Amazon S3. Use S3 Object Lock in governance mode.
- B. Store the documents in Amazon S3. Use S3 Object Lock in compliance mode.
- C. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure key rotation.
- D. Use server-side encryption with AWS Key Management Service (AWS KMS) customer managed keys. Configure key rotation.
- E. Use server-side encryption with AWS Key Management Service (AWS KMS) customer provided (imported) keys. Configure key rotation.

Correct Answer: CE

Community vote distribution



✉️ [Removed] Highly Voted 1 year, 3 months ago

Selected Answer: BD

Originally answered B and C due to least operational overhead. after research its bugging me that the s3 key rotation is determined based on AWS master Key rotation which cannot guarantee the key is rotated with in a 365 day period. stated as "varies" in the documentation. also its impossible to configure this in the console.

KMS-C is a tick box in the console to turn on annual key rotation but requires more operational overhead than SSE-S3.

C - will not guarantee the questions objectives but requires little overhead.

D - will guarantee the questions objective with more overhead.

upvoted 22 times

✉️ [vadiminski_a] 1 year, 3 months ago

I'd have to disagree on that. It states here that aws managed keys are rotated every year which is what the question asks:
<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html> so C would be correct.

However, it also states that you cannot enable or disable rotation for aws managed keys which would again point towards D

upvoted 3 times

✉️ [jdr75] 11 months, 3 weeks ago

You can't use this link
<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>
 to said that "sse-s3" rotates every year, cos' precisely that link refers to "KMS", that is covered with option D.
 That the reason the solution is B+D.

upvoted 2 times

✉️ [LeGlopier] Highly Voted 1 year, 4 months ago

Selected Answer: BD

should be BD

C could have been fine, but key rotation is activate per default on SSE-S3, and no way to deactivate it if I am not wrong

upvoted 7 times

✉️ [scar0909] Most Recent 2 weeks, 1 day ago

Selected Answer: BD

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

upvoted 1 times

✉️ [thewalker] 1 month, 3 weeks ago

Selected Answer: BD

The best option to encrypt data at rest in Amazon S3 and rotate the keys every year is to use AWS KMS (Key Management Service).

With AWS KMS:

You can create a customer master key (CMK) and schedule automatic key rotation every year. This ensures the data is encrypted with a new key annually.

When storing objects in S3, you can choose server-side encryption with AWS KMS (SSE-KMS). This will encrypt the data with the CMK you created.

Even if the encrypted data is copied or transferred, it will remain encrypted since the keys are managed by KMS.

You have full control over the keys and can define IAM policies for key access.

AWS manages the encryption, key operations and auditing through integrated services like CloudTrail.

It provides an end-to-end encryption solution within AWS without needing to handle encryption/decryption yourself.

upvoted 1 times

omarshaban 2 months, 1 week ago

THIS WAS IN MY EXAM

upvoted 2 times

pentium75 2 months, 4 weeks ago

Selected Answer: BD

A - Governance mode allows exceptions

B - Yes

C - SSE-S3 rotates keys when AWS thinks is right, not when customer wants ("every year")

D - Yes

E - "customer provided (imported) keys" can obviously not be 'rotated automatically', the customer would have to provide/import new keys.

upvoted 6 times

celestial39 1 month, 2 weeks ago

KMS indeed rotates keys every year, but the reason why C is wrong is that the Amazon managed keys can't be configured to rotate or not.

REF: <https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html#rotate-keys-how-it-works>

upvoted 1 times

LoXoL 2 months, 1 week ago

Agree with pentium75

upvoted 2 times

Mikado211 3 months, 1 week ago

File cannot be overwritten = s3 compliance mode

encryption AT REST = user-side encryption

upvoted 1 times

Mikado211 3 months, 1 week ago

so the correct answer is BD

upvoted 1 times

awsgeek75 2 months, 1 week ago

user side encryption?

upvoted 1 times

Mikado211 3 months, 1 week ago

Selected Answer: BD

File cannot be overwritten = compliance mode

Encryption AT REST = user-side encryption

upvoted 2 times

ale_brd_ 3 months, 1 week ago

Selected Answer: BD

Question might be outdated.

Amazon S3 now automatically applies server-side encryption with Amazon S3 managed keys (SSE-S3) as the default encryption for all buckets since January 5, 2023.

Additionally, it encrypts the key itself with another key that undergoes regular rotation, enhancing security.

Regarding key rotation, the document specifies that the key used to encrypt the S3 Encryption Key undergoes regular rotation. However, it does not explicitly mention the rotation frequency or the ability to customize it.

Therefore, considering the requirement for key rotation and the lack of explicit details about rotation frequency, options B and D would be suitable choices.

upvoted 3 times

Leo1688 3 months, 2 weeks ago

answer ce is wrong, i voted bd

upvoted 1 times

ansagr 3 months, 2 weeks ago

Selected Answer: BD

While SSE-S3 provides encryption at rest, it doesn't support key rotation for the customer to manage.

upvoted 1 times

Ruffyit 4 months, 2 weeks ago

B. By using S3 Object Lock in compliance mode, it enforces a strict retention policy on the objects, preventing any modifications or deletions.

D. By using server-side encryption with AWS KMS customer managed keys, the documents are encrypted with a customer-controlled key. Enabling key rotation ensures that a new encryption key is generated automatically at the defined rotation interval, enhancing security.

Option A: S3 Object Lock in governance mode does not provide the required immutability for the documents, allowing potential modifications or deletions.

Option C: Server-side encryption with SSE-S3 alone does not fulfill the requirement of encryption key rotation, which is explicitly specified.

Option E: Server-side encryption with customer-provided (imported) keys (SSE-C) is not necessary when AWS KMS customer managed keys (Option D) can be used, which provide a more integrated and manageable solution.

upvoted 1 times

tom_cruise 4 months, 3 weeks ago

Selected Answer: BD

Mentioned by Tom123456ac below: "You cannot automatically rotate asymmetric KMS keys, HMAC KMS keys, KMS keys with imported key material, or KMS keys in custom key stores. However, you can rotate them manually.

not just overhead, or too many steps, kms cannot rotate it automatically like ACM with imported certificates"

upvoted 1 times

awashenko 5 months, 1 week ago

Selected Answer: BC

You SSE S3 rotates their keys every 365 days or you can manually rotate the keys for your objects at any time. It encrypts the key itself with a root key and rotates that root key regularly

upvoted 2 times

Tom123456ac 5 months, 3 weeks ago

E is not correct

You cannot automatically rotate asymmetric KMS keys, HMAC KMS keys, KMS keys with imported key material, or KMS keys in custom key stores. However, you can rotate them manually.

not just overhead, or too many steps, kms cannot rotate it automatically like ACM with imported certificates

upvoted 3 times

paniya93 5 months, 3 weeks ago

Selected Answer: BC

Cis more cost-effective than AWS KMS

upvoted 2 times

TariqKipkemei 6 months, 2 weeks ago

Selected Answer: BC

Technically both BC and BD would work. But option with D customer has to manage the keys, but there is a requirement for LEAST operational overhead, which leaves option C, keys are provided/managed by amazon SSE-S3 encryption.

upvoted 5 times

awsgeek75 2 months, 3 weeks ago

I agree, BC and BD will work but C has lesser overhead.

upvoted 1 times

awsgeek75 2 months, 3 weeks ago

Only scenario for BD would be ensure that keys are automatically rotated "only" once a year as SSE-S3 keys are rotated regularly and maybe rotated more than once a year.

upvoted 1 times

Question #190

Topic 1

A company has a web application that is based on Java and PHP. The company plans to move the application from on premises to AWS. The company needs the ability to test new site features frequently. The company also needs a highly available and managed solution that requires minimum operational overhead.

Which solution will meet these requirements?

- A. Create an Amazon S3 bucket. Enable static web hosting on the S3 bucket. Upload the static content to the S3 bucket. Use AWS Lambda to process all dynamic content.
- B. Deploy the web application to an AWS Elastic Beanstalk environment. Use URL swapping to switch between multiple Elastic Beanstalk environments for feature testing.
- C. Deploy the web application to Amazon EC2 instances that are configured with Java and PHP. Use Auto Scaling groups and an Application Load Balancer to manage the website's availability.
- D. Containerize the web application. Deploy the web application to Amazon EC2 instances. Use the AWS Load Balancer Controller to dynamically route traffic between containers that contain the new site features for testing.

Correct Answer: D*Community vote distribution*

Shasha1 Highly Voted 1 year, 3 months ago

B

Elastic Beanstalk is a fully managed service that makes it easy to deploy and run applications in the AWS; To enable frequent testing of new site features, you can use URL swapping to switch between multiple Elastic Beanstalk environments.

upvoted 10 times

oguzbeliren 7 months, 3 weeks ago

The correct answer is D.

AWS Elastic Beanstalk is a service that makes it easy to deploy and manage web applications in the AWS cloud. However, it is not a good solution for testing new site features frequently, as it can be difficult to switch between multiple Elastic Beanstalk environments.

upvoted 3 times

cookieMr Highly Voted 9 months ago

Selected Answer: B

B. Provides a highly available and managed solution with minimum operational overhead. By deploying the web application to EBS, the infrastructure and platform management are abstracted, allowing easy deployment and scalability. With URL swapping, different environments can be created for testing new site features, and traffic can be routed between these environments without any downtime.

A. Suggests using S3 for static content hosting and Lambda for dynamic content. While it offers simplicity for static content, it does not provide the necessary flexibility and dynamic functionality required by a Java and PHP-based web application.

C. Involves manual management of EC2, ASG, and ELB, which requires more operational overhead and may not provide the desired level of availability and ease of testing.

D. Introduces containerization, which adds complexity and operational overhead for managing containers and infrastructure, making it less suitable for a requirement of minimum operational overhead.

upvoted 9 times

reviewmine Most Recent 1 month ago

Selected Answer: B

Elastic Beanstalk can test Blue/Green deployment. Switching Dev to prod/ prod to dev easily.

upvoted 1 times

awsgeek75 2 months, 3 weeks ago

Selected Answer: B

A and C are not allowing for feature testing.

B and D allow feature testing. D requires overhead of containerisation as well as the LB controller to selectively chose containers for features (assuming on how this might be implemented). EBS allows switching between environment like A/B testing but on whole site. Expensive but cost is not a concern for this question.

upvoted 1 times

master9 3 months ago

Selected Answer: D

WS Elastic Beanstalk supports multiple environments, but each environment can only run one platform at a time. A platform is a combination of an operating system, runtime, and web server, and in this case, Java and PHP would be considered different platforms.

So, if you want to use both Java and PHP, you would need to create two separate environments, one for each. You can then link these environments together using AWS services like Route 53 for routing traffic, or use an Application Load Balancer to distribute incoming traffic between the two environments.

upvoted 1 times

 ale_brd_ 3 months, 1 week ago

Selected Answer: B

Option B (AWS Elastic Beanstalk): Elastic Beanstalk is a fully managed service that makes it easy to deploy and run applications in multiple languages (including Java and PHP) with MINIMAL OPERATION OVERHEAD. It abstracts the infrastructure management, allowing you to focus on your application. URL swapping in Elastic Beanstalk allows you to easily switch between different environments, making it convenient for testing new features.

upvoted 1 times

 Po_chih 5 months, 3 weeks ago

Selected Answer: B

B

Elastic Beanstalk is a fully managed service that makes it easy to deploy and run applications in the AWS; To enable frequent testing of new site features, you can use URL swapping to switch between multiple Elastic Beanstalk environments.

https://docs.aws.amazon.com/zh_tw/whitepapers/latest/blue-green-deployments/swap-the-environment-of-an-elastic-beanstalk-application.html

upvoted 2 times

 Po_chih 5 months, 3 weeks ago

Selected Answer: B

B

Elastic Beanstalk is a fully managed service that makes it easy to deploy and run applications in the AWS; To enable frequent testing of new site features, you can use URL swapping to switch between multiple Elastic Beanstalk environments.

https://docs.aws.amazon.com/zh_tw/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html

upvoted 1 times

 TariqKipkemei 6 months, 2 weeks ago

Selected Answer: B

AWS Elastic Beanstalk URL swapping is the main ask of this question.

upvoted 2 times

 Guru4Cloud 7 months, 1 week ago

Selected Answer: B

B is the correct answer.

Using AWS Elastic Beanstalk provides a fully managed platform to deploy the web application. Elastic Beanstalk will handle provisioning EC2 instances, load balancing, auto scaling, and application health monitoring.

Elastic Beanstalk's ability to support multiple environments and swap URLs allows easy testing of new features before swapping into production. This requires minimal overhead compared to managing infrastructure directly.

upvoted 3 times

 oguzbeliren 7 months, 3 weeks ago

The correct answer is D.

AWS Elastic Beanstalk is a service that makes it easy to deploy and manage web applications in the AWS cloud. However, it is not a good solution for testing new site features frequently, as it can be difficult to switch between multiple Elastic Beanstalk environments.

upvoted 1 times

 Abrar2022 9 months, 4 weeks ago

S3 is for hosting static websites not dynamic websites or applications

Beanstalk will take care of this.

upvoted 1 times

 kruasan 11 months ago

Selected Answer: B

Frequent feature testing -

- Multiple Elastic Beanstalk environments can be created easily for development, testing and production use cases.
- Traffic can be routed between environments for A/B testing and feature iteration using simple URL swapping techniques. No complex routing rules or infrastructure changes required.

upvoted 1 times

 ashu089 11 months, 3 weeks ago

who needs discussion in the era the of chatGPT

upvoted 3 times

 baku98 3 months, 1 week ago

In the era of ChatGPT, individuals across education, business, content creation, healthcare, programming, language learning, innovation, and mental health benefit from discussions. Students, professionals, writers, developers, language learners, innovators, and those seeking support

find ChatGPT valuable for learning, problem-solving, creative endeavors, and companionship. It serves as a versatile tool for information, collaboration, and engagement across diverse domains, enhancing communication in an accessible and interactive manner.

upvoted 1 times

 **aadityaravi8** 8 months, 3 weeks ago

chatGPT always change its answer. just say wrong answer, he will come up with new answer each time with justification. chatGPT is not trusted at all.

upvoted 3 times

 **kerin** 1 year, 1 month ago

Option B as it has the minimum operational overhead

upvoted 1 times

 **maciekmaciek** 1 year, 1 month ago

Selected Answer: B

Blue/Green deployments <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 2 times

 **nixer82** 1 year, 1 month ago

Selected Answer: B

is correct

upvoted 1 times

Question #191

Topic 1

A company has an ordering application that stores customer information in Amazon RDS for MySQL. During regular business hours, employees run one-time queries for reporting purposes. Timeouts are occurring during order processing because the reporting queries are taking a long time to run. The company needs to eliminate the timeouts without preventing employees from performing queries.

What should a solutions architect do to meet these requirements?

- A. Create a read replica. Move reporting queries to the read replica.
- B. Create a read replica. Distribute the ordering application to the primary DB instance and the read replica.
- C. Migrate the ordering application to Amazon DynamoDB with on-demand capacity.
- D. Schedule the reporting queries for non-peak hours.

Correct Answer: B

Community vote distribution

A (100%)

✉  **BENICE**  1 year, 3 months ago

A is correct answer. This was in my exam
upvoted 21 times

✉  **Grace83** 1 year ago

Did these questions help with your exam?
upvoted 3 times

✉  **lostmagnet001**  1 month, 3 weeks ago

Selected Answer: A

create the replica and all the report queries get data from that read replica.
upvoted 1 times

✉  **truongtx8** 2 months, 1 week ago

Selected Answer: A

B incorrect because ordering application needs to write data to the DB.
upvoted 2 times

✉  **Ruffyit** 4 months, 2 weeks ago

A. By moving the reporting queries to the read replica, the primary DB instance used for order processing is not affected by the long-running reporting queries. This helps eliminate timeouts during order processing while allowing employees to perform their queries without impacting the application's performance.

B. While this can provide some level of load distribution, it does not specifically address the issue of timeouts caused by reporting queries during order processing.

C. While DynamoDB offers scalability and performance benefits, it may require significant changes to the application's data model and querying approach.

D. While this approach can help alleviate the impact on order processing, it does not address the requirement of eliminating timeouts without preventing employees from performing queries.

upvoted 2 times

✉  **David_Ang** 5 months ago

Selected Answer: A

"A" is correct because it does not cause problems in the primary DB
upvoted 1 times

✉  **TariqKipkemei** 6 months, 1 week ago

Selected Answer: A

reports = read replica
upvoted 2 times

✉  **Guru4Cloud** 7 months, 1 week ago

Selected Answer: A

A is the correct answer.

Creating an RDS MySQL read replica will allow the reporting queries to be isolated and run without affecting performance of the primary ordering application.

Read replicas allow read-only workloads to be scaled out while eliminating contention with the primary write workload.
upvoted 2 times

✉ **james2033** 8 months, 1 week ago

Selected Answer: A

Question keyword "regular business hours" made D is incorrect.

C migrate to Amazon DynamoDB (No-SQL) is meaningless, remove C.

Answer B, create a "read replica", it is ok, but "ordering application pointed to read replica" is incorrect.

A is correct answer. Easy question.

upvoted 3 times

✉ **sickcow** 8 months, 3 weeks ago

Selected Answer: A

A sounds right

upvoted 1 times

✉ **rauldevilla** 9 months ago

Selected Answer: A

Using the primary instance continues with the problem

upvoted 1 times

✉ **cookieMr** 9 months ago

Selected Answer: A

A. By moving the reporting queries to the read replica, the primary DB instance used for order processing is not affected by the long-running reporting queries. This helps eliminate timeouts during order processing while allowing employees to perform their queries without impacting the application's performance.

B. While this can provide some level of load distribution, it does not specifically address the issue of timeouts caused by reporting queries during order processing.

C. While DynamoDB offers scalability and performance benefits, it may require significant changes to the application's data model and querying approach.

D. While this approach can help alleviate the impact on order processing, it does not address the requirement of eliminating timeouts without preventing employees from performing queries.

upvoted 3 times

✉ **steev** 9 months, 2 weeks ago

Selected Answer: A

correct

upvoted 1 times

✉ **cheese929** 10 months, 3 weeks ago

Selected Answer: A

A is correct.

upvoted 1 times

✉ **kruasan** 11 months ago

Selected Answer: A

Creating a read replica allows the company to offload the reporting queries to a separate database instance, reducing the load on the primary database used for order processing. By moving the reporting queries to the read replica, the ordering application running on the primary DB instance can continue to process orders without timeouts due to the long-running reporting queries.

Option B is not a good solution because distributing the ordering application to the primary DB instance and the read replica does not address the issue of long-running reporting queries causing timeouts during order processing.

upvoted 1 times

✉ **jjlin526** 11 months, 1 week ago

Please DM contributor access: yi.liiiii520@gmail.com

upvoted 2 times

✉ **ammyboy** 11 months ago

bro i need contibutor access please

upvoted 1 times

✉ **Hung23** 11 months, 1 week ago

Selected Answer: A

Answer: A

upvoted 1 times

✉ **k33** 1 year ago

Selected Answer: A

Answer : A

upvoted 1 times

Question #192

Topic 1

A hospital wants to create digital copies for its large collection of historical written records. The hospital will continue to add hundreds of new documents each day. The hospital's data team will scan the documents and will upload the documents to the AWS Cloud.

A solutions architect must implement a solution to analyze the documents, extract the medical information, and store the documents so that an application can run SQL queries on the data. The solution must maximize scalability and operational efficiency.

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

- A. Write the document information to an Amazon EC2 instance that runs a MySQL database.
- B. Write the document information to an Amazon S3 bucket. Use Amazon Athena to query the data.
- C. Create an Auto Scaling group of Amazon EC2 instances to run a custom application that processes the scanned files and extracts the medical information.
- D. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Rekognition to convert the documents to raw text. Use Amazon Transcribe Medical to detect and extract relevant medical information from the text.
- E. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Textract to convert the documents to raw text. Use Amazon Comprehend Medical to detect and extract relevant medical information from the text.

Correct Answer: CD

Community vote distribution

BE (100%)

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

B and E are correct. Textract to extract text from files. Rekognition can also be used for text detection but after Rekognition - it's mentioned that Transcribe is used. Transcribe is used for Speech to Text. So that option D may not be valid.

upvoted 11 times

 **LoXoL** Most Recent  2 months, 1 week ago

Selected Answer: BE

no brainer: B,E

upvoted 2 times

 **awsgeek75** 2 months, 3 weeks ago

Selected Answer: BE

E: Amazon Textract & Amazon Comprehend Medical obviously do the job with least operational overhead. D can do this but it will be extra work and overhead.

B for running SQL queries on S3 bucket directly without extra overhead.

upvoted 3 times

 **Ruffyit** 4 months, 2 weeks ago

Write the document information to an Amazon S3 bucket. Use Amazon Athena to query the data.

Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Textract to convert the documents to raw text. Use Amazon Comprehend Medical to detect and extract relevant medical information from the text.

upvoted 1 times

 **David_Ang** 5 months ago

Selected Answer: BE

another mistake from the admin, should correct this one, because we all agree

upvoted 2 times

 **vijaykamal** 5 months, 4 weeks ago

Answer - BE

Option D mentions using Amazon Rekognition and Amazon Transcribe Medical, which are primarily designed for image and audio analysis, respectively. While they can be part of a document processing pipeline, Amazon Textract and Amazon Comprehend Medical are more suitable for extracting structured information from documents, making option E a better choice.

upvoted 2 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: BE

Write the document information to an Amazon S3 bucket. Use Amazon Athena to query the data.

Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Textract to convert the documents to raw text. Use Amazon Comprehend Medical to detect and extract relevant medical information from the text.

upvoted 1 times

✉ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: BE

B and E are the correct answers.

B is correct because storing the scanned documents in Amazon S3 provides highly scalable and durable storage. Amazon Athena allows running SQL queries directly against the data in S3 without needing to load the data into a database.

E is correct because using Lambda functions triggered by uploads provides a serverless approach to automatically process each document. Amazon Textract and Comprehend Medical can extract text and medical information without needing to manage server

upvoted 4 times

✉ **james2033** 8 months, 1 week ago

Selected Answer: BE

Amazon Comprehend Medical for image reading
<https://aws.amazon.com/comprehend/medical/>.

Amazon Transcribe Medical for speech audio. Remove D. Keep E.

A is meaningless, remove A (EC2).

B use Amazon S3, Athena for querying, keep B.

Conclusion combination B and E are correct answers.

upvoted 2 times

✉ **MNotABot** 8 months, 2 weeks ago

AC wrong as involve EC2. Either one of DE are correct so that makes B correct. Now E is obvious answer if we have read AWS FAQs

upvoted 1 times

✉ **animefan1** 8 months, 3 weeks ago

Selected Answer: BE

Textract to extract the content and Athena to run sql queries on S3 data

upvoted 1 times

✉ **sickcow** 8 months, 3 weeks ago

Selected Answer: BE

From a DE/ML perspective Lambda + Textract + S3 + Athena is the best way to go

upvoted 1 times

✉ **rauldevilla** 9 months ago

Selected Answer: BE

Transcribe is used. Transcribe is used for Speech to Text

upvoted 1 times

✉ **cookieMr** 9 months ago

Selected Answer: BE

B is correct because it suggests writing the document information to an Amazon S3 bucket, which provides scalable and durable object storage. Using Amazon Athena, the data can be queried using SQL, enabling efficient analysis.

E is correct because it involves creating an AWS Lambda function triggered by new document uploads. Amazon Textract is used to convert the documents to raw text, and Amazon Comprehend Medical extracts relevant medical information from the text.

A is incorrect because writing the document information to an Amazon EC2 instance with a MySQL database is not a scalable or efficient solution for analysis.

C is incorrect because creating an Auto Scaling group of Amazon EC2 instances for processing scanned files and extracting information would introduce unnecessary complexity and management overhead.

D is incorrect because using an EC2 instance with a MySQL database for storing document information is not the optimal solution for scalability and efficient analysis.

upvoted 3 times

✉ **AlankarJ** 9 months, 3 weeks ago

It states in the question that the written documents are scanned. They are converted into images after being scanned. Rekognition would be best to analyse images.

upvoted 1 times

✉ **Bmarodi** 10 months ago

Selected Answer: BE

Options B & E are correct answers.

upvoted 1 times

✉ **antropaws** 10 months, 1 week ago

Selected Answer: BE

Why CD are marked as correct??

upvoted 1 times

Question #193

Topic 1

A company is running a batch application on Amazon EC2 instances. The application consists of a backend with multiple Amazon RDS databases. The application is causing a high number of reads on the databases. A solutions architect must reduce the number of database reads while ensuring high availability.

What should the solutions architect do to meet this requirement?

- A. Add Amazon RDS read replicas.
- B. Use Amazon ElastiCache for Redis.
- C. Use Amazon Route 53 DNS caching
- D. Use Amazon ElastiCache for Memcached.

Correct Answer: A

Community vote distribution

✉ **leonnnn** 1 year, 3 months ago

Selected Answer: B

Use ElastiCache to reduce reading and choose redis to ensure high availability.

upvoted 38 times

✉ **Lalo** 1 year, 1 month ago

Where is the high availability when the database fails and the cache time runs out?

The answer is a.

upvoted 20 times

✉ **LoXoL** 2 months, 1 week ago

Right here: Redis has Multi AZ with Auto-Failover (in addition it got Read Replicas for HA)

upvoted 1 times

✉ **Mia2009687** 9 months ago

They run multiple databases

upvoted 1 times

✉ **mandragon** 10 months ago

ElastiCache for Redis ensures high availability by using read replicas and Multi AZ with failover. It is also faster since it uses cache.

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

upvoted 3 times

✉ **JoeGuan** 7 months, 1 week ago

Caching Frequently Accessed Data: ElastiCache allows you to store frequently accessed or computationally expensive data in-memory within the cache nodes. This means that when an application requests data, ElastiCache can provide the data directly from the cache without having to query the RDS database. This reduces the number of reads on the RDS database because the data is retrieved from the faster in-memory cache.

upvoted 4 times

✉ **channn** 11 months, 2 weeks ago

Selected Answer: A

A vs B:

A: reduce the number of database reads on main + high availability provide

B: only reduce the number of DB reads

so A wins

upvoted 21 times

✉ **pentium75** 2 months, 2 weeks ago

Why "only reduce the number of DB reads"? This is exactly what is asked.

ElastiCache for Redis can be HA (contrary to ElastiCache for Memcached).

upvoted 4 times

✉ **LoXoL** 2 months, 1 week ago

pentium75 is right.

upvoted 1 times

✉ **Kanagarajd** 2 weeks, 2 days ago

Selected Answer: B

B is right answer
upvoted 1 times

 **duyvn98** 3 weeks, 5 days ago

Selected Answer: A

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html
"A read replica is a read-only copy of a DB instance. You can reduce the load on your primary DB instance by routing queries from your applications to the read replica."

upvoted 1 times

 **SVDK** 1 month, 1 week ago

Selected Answer: B

A cannot be write as more read replicas doesn't reduce the number of database queries. A is correct as cached data reduces the number of database queries as content is served from cache instead.

upvoted 1 times

 **NayeraB** 1 month, 1 week ago

Selected Answer: A

B is incorrect because you have to explicitly enable and configure read replicas for Amazon ElastiCache for Redis. It's not enabled by default, and the choice says nothing about enabling read replicas for ElastiCache for Redis. So B serves only the purpose of off-loading reads but not the HA one, while A will reduce the read requests for the main DB AND you can promote the read replica in case the main one fails, aka achieving high availability.

upvoted 1 times

 **bujuman** 1 month, 3 weeks ago

Selected Answer: A

Benefits of Amazon RDS Read Replicas:

Enhanced performance
Increased availability
Designed for security

upvoted 1 times

 **chasingsummer** 1 month, 4 weeks ago

Selected Answer: A

Adding read replicas to an Amazon RDS database allows you to offload read traffic from the primary database to one or more read replicas. This not only reduces the load on the primary database but also improves overall performance. Read replicas provide scalability and can enhance the availability of read operations, as they can be used to distribute the read traffic.

On the other hand, Amazon ElastiCache for Redis is a caching service and might not be the best fit for reducing database reads unless your application can benefit from caching data in-memory. For the given scenario, where the goal is to specifically reduce the number of reads on the databases, adding read replicas to the Amazon RDS setup is the more appropriate solution.

upvoted 3 times

 **app12** 2 months ago

<https://aws.amazon.com/elasticache/redis-vs-memcached/>
The difference between redis and memcached is the HA.
So redis wins.

upvoted 1 times

 **farnamjam** 2 months ago

Selected Answer: A

Why other options aren't as suitable:

- B. ElastiCache for Redis: While it can cache frequently accessed data, it's primarily used for in-memory data storage and retrieval, not as a direct replacement for database reads.
- C. Route 53 DNS caching: This caches DNS records for faster domain resolution, not database queries.
- D. ElastiCache for Memcached: Similar to Redis, it's an in-memory caching service, not optimized for reducing database reads.

upvoted 2 times

 **Priyapani** 2 months, 2 weeks ago

Selected Answer: B

Answer Will be B.
Redis support high availability, failover, data is persistent
Also reduce number of database reads

upvoted 1 times

 **upliftinghut** 2 months, 3 weeks ago

Selected Answer: A

Reduce read while ensuring HA: read replicas instead of pure cache
upvoted 1 times

 **pentium75** 2 months, 2 weeks ago

A reduces the impact of reads, but not the number of reads.

upvoted 3 times

 **Pocaho** 2 months, 4 weeks ago

Selected Answer: B

Redis has high availability and the cache will reduce reads as intended

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Selected Answer: B

The question is a bit unclear, "reduce the number of database reads", as seen from the application or from the database?

A would "reduce the number of database reads" from the primary database, but not "the number of database reads" in general. We would still perform the exactly same number of "database reads" as before, just from a replica.

B - requires changes to the application but would "reduce the number of database reads while ensuring high availability" so Y

C - Nonsense

D - Like B but not HA

I'd be undecided between A and B, but as they are giving us two different ElastiCache flavors they obviously want us to know that Redis provides HA while Memcached does not. Thus B.

upvoted 6 times

 **Kanagarajd** 2 weeks, 2 days ago

good explanation!

upvoted 1 times

 **LoXoL** 2 months, 1 week ago

love pentium75

upvoted 2 times

 **djgodzilla** 3 months ago

Selected Answer: B

Memcached doesn't support the below Redis features

- Advanced data structures: supports lists, sets, sorted sets, hashes, bit arrays, and hyperloglogs. ideal for game leadrboards
- Snapshots : keep your data on disk with a point in time snapshot which can be used for archiving or recovery.
- Replication: Redis lets you create multiple replicas of a Redis primary. This allows you to scale database reads and to have highly available clusters.
- Transactions : Redis supports transactions which let you execute a group of commands as an isolated and atomic operation.
- Pub/Sub : Pub/Sub messaging with pattern matching which you can use for high performance chat rooms, real-time comment streams, social media feeds.
- Lua scripting
- Geospatial support

upvoted 1 times

 **ale_brd_** 3 months, 1 week ago

Selected Answer: A

Option A (Amazon RDS read replicas): Adding read replicas to the Amazon RDS databases allows for offloading read queries from the primary database to the read replicas. This can significantly reduce the load on the primary database, distribute read traffic, and improve overall performance. Read replicas provide high availability and can be used to scale out the read capacity horizontally.

Option B (Amazon ElastiCache for Redis) and Option D (Amazon ElastiCache for Memcached): These options involve caching solutions, which can be effective for reducing database reads by serving frequently accessed data from an in-memory cache. However, they may not directly address the high availability requirement, and the effectiveness depends on the nature of the application and data access patterns.

upvoted 3 times

 **BhavyaMPatel** 3 months, 2 weeks ago

Selected Answer: B

<https://aws.amazon.com/getting-started/hands-on/boosting-mysql-database-performance-with-amazon-elasticsearch-for-redis/> for more detail

upvoted 1 times

Question #194

Topic 1

A company needs to run a critical application on AWS. The company needs to use Amazon EC2 for the application's database. The database must be highly available and must fail over automatically if a disruptive event occurs.

Which solution will meet these requirements?

- A. Launch two EC2 instances, each in a different Availability Zone in the same AWS Region. Install the database on both EC2 instances. Configure the EC2 instances as a cluster. Set up database replication.
- B. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use AWS CloudFormation to automate provisioning of the EC2 instance if a disruptive event occurs.
- C. Launch two EC2 instances, each in a different AWS Region. Install the database on both EC2 instances. Set up database replication. Fail over the database to a second Region.
- D. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use EC2 automatic recovery to recover the instance if a disruptive event occurs.

Correct Answer: C

Community vote distribution



✉ **Gil80** Highly Voted 1 year, 3 months ago

Selected Answer: A

Changing my vote to A. After reviewing a Udemy course of SAA-C03, it seems that A (multi-AZ and Clusters) is sufficient for HA.
upvoted 31 times

✉ **berks** 1 year, 3 months ago

what number of class ?

upvoted 5 times

✉ **AAAWrekng** 4 months, 4 weeks ago

Here AWS defines HA, and uses the word cluster - AWS has several methods for achieving HA through both approaches, such as through a scalable, load balanced cluster or assuming an active–standby pair. - <https://docs.aws.amazon.com/whitepapers/latest/real-time-communication-on-aws/high-availability-and-scalability-on-aws.html>

upvoted 1 times

✉ **Gil80** Highly Voted 1 year, 3 months ago

Selected Answer: C

The question states that it is a critical app and it has to be HA. A could be the answer, but it's in the same AZ, so if the entire region fails, it doesn't cater for the HA requirement.

However, the likelihood of a failure in two different regions at the same time is 0. Therefore, to me it seems that C is the better option to cater for HA requirement.

In addition, C does state like A that the DB app is installed on an EC2 instance.

upvoted 25 times

✉ **Burrito69** 4 days, 16 hours ago

Option C proposes launching two EC2 instances in different AWS Regions and setting up database replication, with failover to a second Region. While this solution does provide geographic redundancy, it may introduce higher latency due to cross-region communication and data replication. Additionally, failover to a different Region typically involves more complex configurations and longer recovery times compared to failover within the same Region.

While Option C may offer a level of redundancy, it might not provide the same level of responsiveness and automatic failover capabilities as Option A, which leverages Availability Zones within the same Region. In scenarios where low latency and rapid failover are critical, Option A is often preferred. However, if geographic redundancy is a top priority and the potential trade-offs in latency and failover time are acceptable, Option C could still be a viable solution.

upvoted 1 times

✉ **javitech83** 1 year, 3 months ago

but for C you need communication between the two VPC, which increase the complexity. With a should be enough for HA
upvoted 5 times

✉ **Steve_4542636** 1 year ago

The question doesn't ask which option is the most HA. It asks what meets the requirements.

upvoted 6 times

 **aussiehoa** 10 months, 2 weeks ago

Design for region failure? may as well design for AWS failure and put replica in GCP and Azure :v
upvoted 10 times

 **Kp88** 8 months ago

And on-prem in multiple DCs and one in mars too :D
upvoted 8 times

 **cyber_bedouin** 5 months, 3 weeks ago

yep lol, even in the other questions, for HA you can use Multi-AZ
upvoted 2 times

 **jjcode** 3 months, 2 weeks ago

this is reading comprehension exam not a practical exam.
upvoted 2 times

 **derekz** **Most Recent** 4 weeks ago

Selected Answer: A

A is for HA. D is for DR
upvoted 1 times

 **MrPCarrot** 1 month, 3 weeks ago

Perfect Answer is A
upvoted 1 times

 **thewalker** 1 month, 3 weeks ago

Selected Answer: A

A.
High Availability - multiple Zones.
Disaster Recovery - multiple Regions.
upvoted 4 times

 **Mkenya08** 1 month, 4 weeks ago

C "if a disruptive event occurs"
upvoted 2 times

 **andyngkh86** 2 months ago

Answer is C, because question mentioned about disruptive event occurs. when the whole region failed, it can not cover the scenario for HA
upvoted 2 times

 **vip2** 2 months, 1 week ago

Selected Answer: A

A is more correct to support both HA and Failover.
C is only for Failover, not HA during the traffic.
upvoted 1 times

 **Priyapani** 2 months, 2 weeks ago

Selected Answer: C

C will be answer
As it is a critical application
upvoted 1 times

 **upliftinghut** 2 months, 3 weeks ago

Selected Answer: C

Only A & C are possible solutions. However A is not suitable when the region fails while this is critical application => C is the answer
upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

Selected Answer: A

Between A and C, A meets the high availability requirements. C seems an overkill and also requires manual failover as the option does not mention how the failover switch is setup (like using CloudFormation or some events etc)
upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

Selected Answer: A

B and D are using a single instance and involve restoring an old AMI in case of failure, that is anything but HA

A is correct, different AZs meet AWS' definition of HA, and the "cluster" should take care of the automatic failover.

C involves manual failover which does not meet the requirements.
upvoted 5 times

 **Sumith4112** 3 months ago

Selected Answer: C

Practically speaking, A should be the answer. Because, if you do, C, DB replication across two reason is not less expensive. Also, C says, "fail over the DB to a second region". This means, it is manual. So, I believe A is the right answer.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Then why did you select C?

upvoted 2 times

 **ale_brd_** 3 months, 1 week ago

Selected Answer: A

for high availability and load distribution, Option A is the most suitable choice by deploying EC2 instances in different AZs within the same AWS Region and configuring them as a cluster with database replication.

upvoted 1 times

 **Sumith4112** 3 months, 2 weeks ago

Selected Answer: A

C has got more votes as well. However, I think, since C says, "fail over the database to a second region". it seems to be manual. So, going with A.

upvoted 2 times

 **yayaayzo** 3 months, 2 weeks ago

CORRECT ANS IS AAAA

A. Launch two EC2 instances, each in a different Availability Zone in the same AWS Region. Install the database on both EC2 instances. Configure the EC2 instances as a cluster. Set up database replication.

Explanation:

Different Availability Zones: Deploying the EC2 instances in different Availability Zones ensures redundancy and availability in case one Availability Zone experiences issues.

Cluster Configuration and Database Replication: Configuring the EC2 instances as a cluster with database replication allows for automatic failover. If one instance becomes unavailable, the other can take over seamlessly.

upvoted 1 times

 **ansagr** 3 months, 2 weeks ago

Selected Answer: A

Configuring the EC2 instances as a cluster enhances high availability by creating a collaborative and redundant environment for the database. In a clustered setup, both EC2 instances work together, sharing the workload and maintaining synchronized copies of the database. If one instance fails due to a disruptive event, the other instance can seamlessly take over, ensuring continuous availability of the database.

upvoted 1 times

Question #195

Topic 1

A company's order system sends requests from clients to Amazon EC2 instances. The EC2 instances process the orders and then store the orders in a database on Amazon RDS. Users report that they must reprocess orders when the system fails. The company wants a resilient solution that can process orders automatically if a system outage occurs.

What should a solutions architect do to meet these requirements?

- A. Move the EC2 instances into an Auto Scaling group. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to target an Amazon Elastic Container Service (Amazon ECS) task.
- B. Move the EC2 instances into an Auto Scaling group behind an Application Load Balancer (ALB). Update the order system to send messages to the ALB endpoint.
- C. Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create an AWS Lambda function, and subscribe the function to the SNS topic. Configure the order system to send messages to the SNS topic. Send a command to the EC2 instances to process the messages by using AWS Systems Manager Run Command.

Correct Answer: D

Community vote distribution

C (95%) 3%

✉ **Guru4Cloud** Highly Voted 7 months, 1 week ago

Selected Answer: C

The key reasons are:

Using an Auto Scaling group ensures the EC2 instances that process orders are highly available and scalable.

With SQS, the orders are decoupled from the instances that process them via asynchronous queuing.

If instances fail or go down, the orders remain in the queue until new instances can pick them up. This provides automated resilience.

Any failed processing can retry by resending messages back to the queue

upvoted 9 times

✉ **awsgeek75** Most Recent 2 months, 3 weeks ago

Selected Answer: C

A uses ECS tasks for something which makes no sense.

B does not solve the reliable processing of orders

C SQS for sending a message and processing it reliable

D is like reinventing SQS with SNS and Lambda mumbo jumbo

upvoted 3 times

✉ **jjcode** 3 months, 2 weeks ago

How does SNS capture the requests after the application fails? Those messages are ephemeral by nature and will not hold the data like SQS would. In theory one could create a subscription based service using SNS to stream the data to a service that could store the request, but why...

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

That's one of the reasons why D is wrong (not to mention the "Systems Manager Run Command" nonsense).

upvoted 2 times

✉ **awsgeek75** 2 months, 3 weeks ago

I stopped reading option D after SNS and Lambda.... it was sounding nonsense. SQS is default reliability delivery system for me.

upvoted 1 times

✉ **pavospam** 3 months, 4 weeks ago

Selected Answer: C

it's C... 4 answers wrong I have found

upvoted 1 times

✉ **Ruffyit** 4 months, 2 weeks ago

C.

Option D suggests using Amazon SNS and AWS Lambda, which can be part of an event-driven architecture but may not be the best fit for ensuring the automatic processing of orders during system outages. It relies on an additional AWS Systems Manager Run Command step, which adds complexity and may not be as reliable as using SQS for queuing messages.

upvoted 1 times

 **David_Ang** 5 months ago

Selected Answer: C

"C" because they need to store the request and then be process by the system if it fails, SNS does not have that capacity. another mistake from the admin

upvoted 1 times

 **vijaykamal** 5 months, 4 weeks ago

Selected Answer: C

Option D suggests using Amazon SNS and AWS Lambda, which can be part of an event-driven architecture but may not be the best fit for ensuring the automatic processing of orders during system outages. It relies on an additional AWS Systems Manager Run Command step, which adds complexity and may not be as reliable as using SQS for queuing messages.

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: C

Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue.

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: C

C is the correct answer.

Using an Auto Scaling group with EC2 instances behind a load balancer provides high availability and scalability.

Sending the orders to an SQS queue decouples the ordering system from the processing system. The EC2 instances can poll the queue for new orders and process them even during an outage. Any failed orders will go back to the queue for reprocessing.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: C

By moving the EC2 into an ASG and configuring them to consume messages from an SQS, the system can decouple the order processing from the order system itself. This allows the system to handle failures and automatically process orders even if the order system or EC2 experience outages.

A. Using an ASG with an EventBridge rule targeting an ECS task does not provide the necessary decoupling and message queueing for automatic order processing during outages.

B. Moving the EC2 instances into an ASG behind an ALB does not address the need for message queuing and automatic processing during outages.

D. Using SNS and Lambda can provide notifications and orchestration capabilities, but it does not provide the necessary message queueing and consumption for automatic order processing during outages. Additionally, using Systems Manager Run Command to send commands for order processing adds complexity and does not provide the desired level of automation.

upvoted 3 times

 **pisica134** 9 months ago

D is so unnecessary this confuses people

upvoted 1 times

 **cookieMr** 9 months ago

Thx Allmighty for voting system! Answers provided by the site (and not by community) are 20% wrong.

upvoted 4 times

 **markw92** 9 months, 1 week ago

The answer D is so complex and unnecessary. Why moderator is not providing an explanation of answers when there are heavy conflicts. These kind of answers put your knowledge in question which is not good going into the exam.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

The "Correct Answers" for this exam are obviously determined by picking a random letter between A and D.

upvoted 2 times

 **gx2222** 11 months, 3 weeks ago

Selected Answer: C

To meet the company's requirements of having a resilient solution that can process orders automatically in case of a system outage, the solutions architect needs to implement a fault-tolerant architecture. Based on the given scenario, a potential solution is to move the EC2 instances into an Auto Scaling group and configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. The EC2 instances can then consume messages from the queue.

upvoted 2 times

 **k33** 1 year ago

Selected Answer: C

Answer : C

upvoted 1 times

 nickolaj 1 year, 1 month ago

Selected Answer: C

C. Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue.

To meet the requirements of the company, a solutions architect should ensure that the system is resilient and can process orders automatically in the event of a system outage. To achieve this, moving the EC2 instances into an Auto Scaling group is a good first step. This will enable the system to automatically add or remove instances based on demand and availability.

upvoted 2 times

 nickolaj 1 year, 1 month ago

However, it's also necessary to ensure that orders are not lost if a system outage occurs. To achieve this, the order system can be configured to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. SQS is a highly available and durable messaging service that can help ensure that messages are not lost if the system fails.

Finally, the EC2 instances can be configured to consume messages from the queue, process the orders and then store them in the database on Amazon RDS. This approach ensures that orders are not lost and can be processed automatically if a system outage occurs. Therefore, option C is the correct answer.

upvoted 2 times

 nickolaj 1 year, 1 month ago

Option A is incorrect because it suggests creating an Amazon EventBridge rule to target an Amazon Elastic Container Service (ECS) task. While this may be a valid solution in some cases, it is not necessary in this scenario.

Option B is incorrect because it suggests moving the EC2 instances into an Auto Scaling group behind an Application Load Balancer (ALB) and updating the order system to send messages to the ALB endpoint. While this approach can provide resilience and scalability, it does not address the issue of order processing and the need to ensure that orders are not lost if a system outage occurs.

Option D is incorrect because it suggests using Amazon Simple Notification Service (SNS) to send messages to an AWS Lambda function, which will then send a command to the EC2 instances to process the messages by using AWS Systems Manager Run Command. While this approach may work, it is more complex than necessary and does not take advantage of the durability and availability of SQS.

upvoted 2 times

 LuckyAro 1 year, 2 months ago

Selected Answer: C

My question is; can orders be sent directly into an SQS queue ? How about the protocol for management of the messages from the queue ? can EC2 instances be programmed to process them like Lambda ?

upvoted 1 times

 berks 1 year, 3 months ago

Selected Answer: D

I choose D

upvoted 1 times

 pentium75 2 months, 4 weeks ago

and manually send commands through Systems Manager whenever a new order appears?

upvoted 1 times

Question #196

Topic 1

A company runs an application on a large fleet of Amazon EC2 instances. The application reads and writes entries into an Amazon DynamoDB table. The size of the DynamoDB table continuously grows, but the application needs only data from the last 30 days. The company needs a solution that minimizes cost and development effort.

Which solution meets these requirements?

- A. Use an AWS CloudFormation template to deploy the complete solution. Redeploy the CloudFormation stack every 30 days, and delete the original stack.
- B. Use an EC2 instance that runs a monitoring application from AWS Marketplace. Configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table. Use a script that runs on the EC2 instance to delete items that have a timestamp that is older than 30 days.
- C. Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table. Configure the Lambda function to delete items in the table that are older than 30 days.
- D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. Configure DynamoDB to use the attribute as the TTL attribute.

Correct Answer: D

Community vote distribution



✉ **Gil80** 1 year, 3 months ago

Selected Answer: D

changing my answer to D after researching a bit.

The DynamoDB TTL feature allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput.

upvoted 33 times

✉ **scar0909** 2 weeks, 1 day ago

Selected Answer: D

use ttl

upvoted 1 times

✉ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: D

A and B don't solve anything.

Between C and D, C requires more cost due to Lambda executions. D uses the TTL built-in feature so it won't cost extra. Also, D does not require extra development and is a matter of configuration. In old-school developer speak, don't write code if your DBA can do some work!

upvoted 2 times

✉ **awsgeek75** 2 months, 1 week ago

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

upvoted 1 times

✉ **TariqKipkemei** 6 months, 1 week ago

Selected Answer: D

DynamoDB Time to Live was designed to handle this kind of requirement where an item is no longer needed. TTL is provided at no extra cost as a means to reduce stored data volumes by retaining only the items that remain current for your workload's needs

upvoted 2 times

✉ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. Configure DynamoDB to use the attribute as the TTL attribute.

The main reasons are:

Using DynamoDB's built-in TTL functionality is the most direct way to handle data expiration.

It avoids the complexity of triggers, streams, and lambda functions in option C.

Modifying the application code to add the TTL attribute is relatively simple and minimizes operational overhead

upvoted 2 times

 **cookieMr** 9 months ago

Selected Answer: D

By adding a TTL attribute to the DynamoDB table and setting it to the current timestamp plus 30 days, DynamoDB will automatically delete the items that are older than 30 days. This solution eliminates the need for manual deletion or additional infrastructure components.

A. Redeploying the CloudFormation stack every 30 days and deleting the original stack introduces unnecessary complexity and operational overhead.

B. Using an EC2 instance with a monitoring application and a script to delete items older than 30 days adds additional infrastructure and maintenance efforts.

C. Configuring DynamoDB Streams to invoke a Lambda function to delete items older than 30 days adds complexity and requires additional development and operational effort compared to using the built-in TTL feature of DynamoDB.

upvoted 2 times

 **pisica134** 9 months ago

D: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

upvoted 1 times

 **Abrar2022** 10 months ago

Amazon DynamoDB Time to Live (TTL) allows you to define a per-item timestamp to determine when an item is no longer needed.

upvoted 3 times

 **studynoplay** 10 months, 2 weeks ago

Selected Answer: D

C is incorrect because it can take more than 15 minutes to delete the old data. Lambda won't work

upvoted 1 times

 **Konb** 10 months, 3 weeks ago

Selected Answer: D

Clear case for TTL - every object gets deleted after a certain period of time

upvoted 1 times

 **rushi0611** 10 months, 3 weeks ago

Selected Answer: D

Use DynamoDB TTL feature to achieve this..

upvoted 1 times

 **jdr75** 11 months, 2 weeks ago

Selected Answer: D

C is absurd. DynamoDB usually is a RDS with high iops (read/write operations on tables), executing a Lambda function each time you insert a item will not be cost-effective. It's much better create such a field the question propose, and manage the delete with a SQL delete sentence:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.DeleteData.html>

upvoted 1 times

 **LuckyAro** 1 year, 2 months ago

Selected Answer: D

Amazon DynamoDB Time to Live (TTL) allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput. TTL is provided at no extra cost as a means to reduce stored data volumes by retaining only the items that remain current for your workload's needs.

TTL is useful if you store items that lose relevance after a specific time.

upvoted 1 times

 **DavidNamy** 1 year, 2 months ago

Selected Answer: D

D: This solution is more efficient and cost-effective than alternatives that would require additional resources and maintenance.

upvoted 1 times

 **anonymouscloudguy** 1 year, 2 months ago

Selected Answer: D

D DyanmoDB TTL will expire the items

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: D

To minimize cost and development effort, a solution that requires minimal changes to the existing application and infrastructure would be the most appropriate. Option D meets these requirements by using DynamoDB's Time-To-Live (TTL) feature, which allows you to specify an attribute on each item in a table that has a timestamp indicating when the item should expire.

In this solution, the application is extended to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. DynamoDB is then configured to use this attribute as the TTL attribute, which causes items to be automatically deleted from

the table when their TTL value is reached. This solution requires minimal changes to the existing application and infrastructure and does not require any additional resources or a complex setup.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option A involves using AWS CloudFormation to redeploy the solution every 30 days, but this would require significant development effort and could cause downtime for the application.

Option B involves using an EC2 instance and a monitoring application to delete items that are older than 30 days, but this requires additional infrastructure and maintenance effort.

Option C involves using DynamoDB Streams and a Lambda function to delete items that are older than 30 days, but this requires additional infrastructure and maintenance effort.

upvoted 1 times

 **techhb** 1 year, 3 months ago

Selected Answer: D

TTL does the trick

upvoted 1 times

Question #197

Topic 1

A company has a Microsoft .NET application that runs on an on-premises Windows Server. The application stores data by using an Oracle Database Standard Edition server. The company is planning a migration to AWS and wants to minimize development changes while moving the application. The AWS application environment should be highly available.

Which combination of actions should the company take to meet these requirements? (Choose two.)

- A. Refactor the application as serverless with AWS Lambda functions running .NET Core.
- B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
- C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI).
- D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment.
- E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

Correct Answer: BD

Community vote distribution

BE (98%)

✉️ **DavidNamy** Highly Voted 1 year, 2 months ago

Selected Answer: BE

- B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
- E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

Rehosting the application in Elastic Beanstalk with the .NET platform can minimize development changes. Multi-AZ deployment of Elastic Beanstalk will increase the availability of application, so it meets the requirement of high availability.

Using AWS Database Migration Service (DMS) to migrate the database to Amazon RDS Oracle will ensure compatibility, so the application can continue to use the same database technology, and the development team can use their existing skills. It also migrates to a managed service, which will handle the availability, so the team do not have to worry about it. Multi-AZ deployment will increase the availability of the database.

upvoted 11 times

✉️ **vijaykamal** Highly Voted 5 months, 4 weeks ago

Selected Answer: BE

DynamoDB is NoSQL - E is out
Replatform requires considerable overhead - C is out
Lambda function is for running code for short duration - A is out
Answer - BE

upvoted 5 times

✉️ **awsgeek75** Most Recent 2 months, 3 weeks ago

Selected Answer: BE

E for minimizing development changes by using same Oracle engine but in highly available deployment.
C and D require platform change so it won't work as it increases development.
A is also development work of converting .Net to .Net core Lambda functions. May not even be possible.
B is simple lift and shift
BE is correct

upvoted 2 times

✉️ **TariqKipkemei** 6 months, 1 week ago

Selected Answer: BE

Minimize development changes + High availability = AWS Elastic Beanstalk and Oracle on Amazon RDS in a Multi-AZ deployment

upvoted 1 times

✉️ **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

- B) Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
- E) Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

The reasons are:

- Rehosting in Elastic Beanstalk allows lifting and shifting the .NET application with minimal code changes. Multi-AZ deployment provides high availability.
- Using DMS to migrate the Oracle data to RDS Oracle in Multi-AZ deployment minimizes changes for the database while achieving high availability.
- Together this "lift and shift" approach minimizes refactoring needs while providing HA on AWS.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: BE

B. This allows the company to migrate the application to AWS without significant code changes while leveraging the scalability and high availability provided by EBS's Multi-AZ deployment.

E. This enables the company to migrate the Oracle database to RDS while maintaining compatibility with the existing application and leveraging the Multi-AZ deployment for high availability.

A. would require significant development changes and may not provide the same level of compatibility as rehosting or replatforming options.

C. would still require changes to the application and the underlying infrastructure, whereas rehosting with EBS minimizes the need for modification.

D. would likely require significant changes to the application code, as DynamoDB is a NoSQL database with a different data model compared to Oracle.

upvoted 3 times

 **markw92** 9 months, 1 week ago

Answer is BE. No idea why D was chosen. That requires development work and question clearly states minimize development changes, changing db from Oracle to DynamoDB is LOT of development.

upvoted 2 times

 **Bmarodi** 10 months ago

Selected Answer: BE

B + E are the answers that fulfil the requirements.

upvoted 1 times

 **cheese929** 10 months, 3 weeks ago

Selected Answer: BE

B and E

upvoted 1 times

 **Nikhilcy** 10 months, 3 weeks ago

why not C?

upvoted 2 times

 **AlankarJ** 9 months, 3 weeks ago

It runs on a windows server, shifting the whole this to Linux based EC2 would be extra work and of no sense

upvoted 1 times

 **k33** 1 year ago

Selected Answer: BE

Answer : BE

upvoted 1 times

 **waiyiu9981** 1 year, 2 months ago

Why A is wrong?

upvoted 1 times

 **gustavtd** 1 year, 2 months ago

Because that needs some development,

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: BE

B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.

E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

To minimize development changes while moving the application to AWS and to ensure a high level of availability, the company can rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment. This will allow the application to run in a highly available environment without requiring any changes to the application code.

The company can also use AWS Database Migration Service (AWS DMS) to migrate the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment. This will allow the company to maintain the existing database platform while still achieving a high level of availability.

upvoted 4 times

 **techhb** 1 year, 3 months ago

Selected Answer: BE

B&E Option ,because D is for No-Sql

upvoted 1 times

 **JayBee65** 1 year, 2 months ago

And requires additional development effort

upvoted 1 times

 **career360guru** 1 year, 3 months ago

B&E Option

upvoted 1 times

 **dcyberguy** 1 year, 3 months ago

B- According to the AWS documentation, the simplest way to migrate .NET applications to AWS is to republish the applications using either AWS Elastic Beanstalk or Amazon EC2.

E - RDS with Oracle is a no-brainer

upvoted 3 times

 **[Removed]** 1 year, 3 months ago

Selected Answer: BE

same as everyone else

upvoted 3 times

Question #198

Topic 1

A company runs a containerized application on a Kubernetes cluster in an on-premises data center. The company is using a MongoDB database for data storage. The company wants to migrate some of these environments to AWS, but no code changes or deployment method changes are possible at this time. The company needs a solution that minimizes operational overhead.

Which solution meets these requirements?

- A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes for compute and MongoDB on EC2 for data storage.
- B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB for data storage
- C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes for compute and Amazon DynamoDB for data storage.
- D. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.

Correct Answer: D

Community vote distribution

D (100%)

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

Selected Answer: D

If you see MongoDB, just go ahead and look for the answer that says DocumentDB.
upvoted 26 times

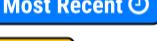
✉  **Guru4Cloud**  7 months, 1 week ago

Selected Answer: D

Option D is the correct solution that meets all the requirements:

- Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.
- The key reasons are:
 - EKS allows running the Kubernetes environment on AWS without changes.
 - Using Fargate removes the need to provision and manage EC2 instances.
 - DocumentDB provides MongoDB compatibility so the data layer is unchanged.

upvoted 5 times

✉  **LoXoL**  2 months, 1 week ago

Selected Answer: D

no brainer says D
upvoted 1 times

✉  **james2033** 8 months, 1 week ago

Selected Answer: D

Question keyword "containerized application", "Kubernetes cluster", "no changes or deployment method changes". Choose C, not D.
But "minimizes operational overhead", choose D.

upvoted 1 times

✉  **cookieMr** 9 months ago

Selected Answer: D

This solution allows the company to leverage EKS to manage the K8s cluster and Fargate to handle the compute resources without requiring manual management of EC2 worker nodes. The use of DocumentDB provides a fully managed MongoDB-compatible database service in AWS.

- A. would require managing and scaling the EC2 instances manually, which increases operational overhead.
- B. would require significant changes to the application code as DynamoDB is a NoSQL database with a different data model compared to MongoDB.
- C. would also require code changes to adapt to DynamoDB's different data model, and managing EC2 worker nodes increases operational overhead.

upvoted 3 times

✉  **Bmarodi** 10 months ago

Selected Answer: D

The solution meets these requirements is option D.

upvoted 1 times

 **studynoplay** 10 months, 2 weeks ago

Selected Answer: D

minimizes operational overhead = Serverless (Fargate)

MongoDB = DocumentDB

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: D

To minimize operational overhead and avoid making any code or deployment method changes, the company can use Amazon Elastic Kubernetes Service (EKS) with AWS Fargate for computing and Amazon DocumentDB (with MongoDB compatibility) for data storage. This solution allows the company to run the containerized application on EKS without having to manage the underlying infrastructure or make any changes to the application code.

AWS Fargate is a fully-managed container execution environment that allows you to run containerized applications without the need to manage the underlying EC2 instances.

Amazon DocumentDB is a fully-managed document database service that supports MongoDB workloads, allowing the company to use the same database platform as in their on-premises environment without having to make any code changes.

upvoted 4 times

 **techhb** 1 year, 3 months ago

Selected Answer: D

Reason A &B Eliminated as its Kubernetes

why D read here <https://containersonaws.com/introduction/ec2-or-aws-fargate/>

upvoted 2 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D

upvoted 2 times

 **dcyberguy** 1 year, 3 months ago

DDDDDDDD

upvoted 1 times

 **Gabs90** 1 year, 3 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/67897-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **leonnnn** 1 year, 3 months ago

Selected Answer: D

D meets the requirements

upvoted 1 times

 **Nigma** 1 year, 3 months ago

Selected Answer: D

D

EKS because of Kubernetes so A and B are eliminated

not C because of MongoDB and Fargate is more expensive

upvoted 1 times

Question #199

Topic 1

A telemarketing company is designing its customer call center functionality on AWS. The company needs a solution that provides multiple speaker recognition and generates transcript files. The company wants to query the transcript files to analyze the business patterns. The transcript files must be stored for 7 years for auditing purposes.

Which solution will meet these requirements?

- A. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use machine learning models for transcript file analysis.
- B. Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis.
- C. Use Amazon Translate for multiple speaker recognition. Store the transcript files in Amazon Redshift. Use SQL queries for transcript file analysis.
- D. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use Amazon Textract for transcript file analysis.

Correct Answer: C

Community vote distribution



Buruguduystunstugudunstuy 1 year, 3 months ago

Selected Answer: B

The correct answer is B: Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis.

Amazon Transcribe is a service that automatically transcribes spoken language into written text. It can handle multiple speakers and can generate transcript files in real-time or asynchronously. These transcript files can be stored in Amazon S3 for long-term storage.

Amazon Athena is a query service that allows you to analyze data stored in Amazon S3 using SQL. You can use it to analyze the transcript files and identify patterns in the data.

Option A is incorrect because Amazon Rekognition is a service for analyzing images and videos, not transcribing spoken language.

Option C is incorrect because Amazon Translate is a service for translating text from one language to another, not transcribing spoken language.

Option D is incorrect because Amazon Textract is a service for extracting text and data from documents and images, not transcribing spoken language.

upvoted 19 times

enzomv 1 year, 2 months ago

The correct answer is C.

<https://docs.aws.amazon.com/transcribe/latest/dg/what-is.html>

You can transcribe streaming media in real time or you can upload and transcribe media files. To see which languages are supported for each type of transcription, refer to the Supported languages and language-specific features table.

upvoted 2 times

enzomv 1 year, 1 month ago

Disregard. I meant B

upvoted 1 times

enzomv 1 year, 1 month ago

<https://aws.amazon.com/about-aws/whats-new/2022/06/amazon-transcribe-supports-automatic-language-identification-multi-lingual-audio/>

Amazon Translate is a service for multi-language identification, which identifies all languages spoken in the audio file and creates transcript using each identified language.

upvoted 1 times

enzomv 1 year, 1 month ago

Disregard. I meant Amazon Transcribe

upvoted 1 times

TheAbsoluteTruth 11 months, 3 weeks ago

What bothers me is the 7 years of storage.

upvoted 6 times

awsgeek75 2 months, 3 weeks ago

Selected Answer: B

This is a poorly worded question with poorly worded options. Rekognition and Translate cannot convert speech to text so those options A, C & D are gone. B is the closest option but it does not mention S3 or retention policy of 7 years. Just a best guess on massive assumptions.

upvoted 2 times

 **SinghJagdeep** 2 months, 3 weeks ago

Selected Answer: B

check out this blog here: <https://aws.amazon.com/de/blogs/machine-learning/automating-the-analysis-of-multi-speaker-audio-files-using-amazon-transcribe-and-amazon-athena/>

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Selected Answer: B

Perfectly explained here: <https://aws.amazon.com/de/blogs/machine-learning/automating-the-analysis-of-multi-speaker-audio-files-using-amazon-transcribe-and-amazon-athena/>

upvoted 2 times

 **youdelin** 5 months, 2 weeks ago

really hope I could have this kind of question during the exam, 4 different techs in the first 5 words of the answer! Just go with the correct one and ignore the rest of the text XDDD

upvoted 2 times

 **paniya93** 5 months, 3 weeks ago

Selected Answer: B

<https://aws.amazon.com/blogs/machine-learning/automating-the-analysis-of-multi-speaker-audio-files-using-amazon-transcribe-and-amazon-athena/>

upvoted 1 times

 **vijaykamal** 5 months, 4 weeks ago

Selected Answer: B

Amazon Rekognition is primarily designed for image and video analysis, not for transcribing audio or recognizing multiple speakers. -> Option A and D are ruled out

Amazon Translate is used for language translation -> Option C is ruled out

upvoted 2 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: B

Provide multiple speaker recognition and generate transcript files = Amazon Transcribe

Query the transcript files = Amazon Athena

upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: B

The correct answer is B: Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis.

upvoted 2 times

 **Thornessen** 8 months, 1 week ago

Selected Answer: B

Tricky or incomplete question..

B is the answer because Transcribe is the right service for processing voice calls.

But 7 years of storage is not covered (should add S3 storage)

And Athena querying is just SQL querying, it cannot help you much to recognize business patterns, for that I would think some text analysis service like Comprehend would be needed.

Unless... We use Transcribe not only to transcribe, but also to recognize some key words, and then create a DB/S3 record with multiple fields, e.g. if it is a telemarketing questionnaire, record answer for each question. Then SQL querying might be useful.

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

"The company wants to query the transcript files" is the requirement. How they will be using the query results "to analyze the business patterns" is not our issue.

The "7 years" are not mentioned in any of the options, but Transcribe stores results in S3.

upvoted 1 times

 **sickcow** 8 months, 3 weeks ago

Selected Answer: C

Transcribe and (S3) + Athena is the way to go here.

Redshift sounds like an overkill

upvoted 2 times

 **cookieMr** 9 months ago

Amazon Transcribe provides accurate transcription of audio recordings with multiple speakers, generating transcript files. These files can be stored in Amazon S3. To analyze the transcripts and extract insights, Amazon Athena allows SQL-based querying of the stored files.

A. Amazon Rekognition is for image and video analysis, not audio transcription.

C. Amazon Translate is for language translation, not speaker recognition or transcript analysis. Amazon Redshift may not be the best choice for storing and querying transcript files.

D. Amazon Rekognition is for image and video analysis, and Amazon Textract is for document extraction, not suitable for audio transcription or analysis. Storing the transcript files in S3 is appropriate, but the analysis requires a different service like Amazon Athena.

upvoted 1 times

 **Bmarodi** 10 months ago

Selected Answer: B

the solution that meets these requirements is option B.

upvoted 1 times

 **cheese929** 10 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

 **Rahulbit34** 10 months, 3 weeks ago

Amazon Transcribe is a service that convert speech into text, so B is the answer

upvoted 1 times

 **k33** 1 year ago

Selected Answer: B

Answer : B

upvoted 2 times

 **enzomv** 1 year, 2 months ago

Selected Answer: C

<https://docs.aws.amazon.com/transcribe/latest/dg/what-is.html>

upvoted 1 times

Question #200

Topic 1

A company hosts its application on AWS. The company uses Amazon Cognito to manage users. When users log in to the application, the application fetches required data from Amazon DynamoDB by using a REST API that is hosted in Amazon API Gateway. The company wants an AWS managed solution that will control access to the REST API to reduce development efforts.

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

- A. Configure an AWS Lambda function to be an authorizer in API Gateway to validate which user made the request.
- B. For each user, create and assign an API key that must be sent with each request. Validate the key by using an AWS Lambda function.
- C. Send the user's email address in the header with every request. Invoke an AWS Lambda function to validate that the user with that email address has proper access.
- D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request.

Correct Answer: A*Community vote distribution*

D (97%)

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

Selected Answer: D

KEYWORD: LEAST operational overhead

To control access to the REST API and reduce development efforts, the company can use an Amazon Cognito user pool authorizer in API Gateway. This will allow Amazon Cognito to validate each request and ensure that only authenticated users can access the API. This solution has the LEAST operational overhead, as it does not require the company to develop and maintain any additional infrastructure or code.

Therefore, Option D is the correct answer.

Option D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request.
upvoted 11 times

 **awsgeek75** Most Recent 2 months, 3 weeks ago

Selected Answer: D

A is possible if the authorisation logic makes sense and does not require operational overhead.

B is too much overhead for each new user.

C is lol

D Company already has Cognito for it's users so just integrate it with the API gateway

This question and options are poorly worded an A could be a reasonable choice if more information is provided. Just keep that in mind for the exam!

upvoted 2 times

 **osmk** 3 months, 1 week ago

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

upvoted 2 times

 **Tom123456ac** 5 months, 3 weeks ago

The description of this question is really bad. Company is using Cognito to manage users already, but still verifying user info from dynamodb, very wired situation. But just select Cognito when you see Api gateway + cognito + authentication + least efforts

upvoted 3 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: D

use Amazon Cognito to authorize user requests.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request

upvoted 2 times

 **Guru4Cloud** 7 months, 1 week ago

Selected Answer: D

Option D is the best solution with the least operational overhead:

Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request.

The key reasons are:

- Cognito user pool authorizers allow seamless integration between Cognito and API Gateway for access control.
- API Gateway handles validating the access tokens from Cognito automatically without any custom code.
- This is a fully managed solution with minimal ops overhead.

upvoted 2 times

 **cookieMr** 9 months ago

By configuring an Amazon Cognito user pool authorizer in API Gateway, you can leverage the built-in functionality of Amazon Cognito to authenticate and authorize users. This eliminates the need for custom development or managing access keys. Amazon Cognito handles user authentication, securely manages user identities, and provides seamless integration with API Gateway for controlling access to the REST API.

A. Configuring an AWS Lambda function as an authorizer in API Gateway would require custom implementation and management of the authorization logic.

B. Creating and assigning an API key for each user would require additional management and validation logic in an AWS Lambda function.

C. Sending the user's email address in the header and validating it with an AWS Lambda function would also require custom implementation and management of the authorization logic.

Option D, using an Amazon Cognito user pool authorizer, provides a streamlined and managed solution for controlling access to the REST API with minimal operational overhead.

upvoted 2 times

 **Bmarodi** 10 months ago

Selected Answer: D

solution will meet these requirements with the LEAST operational overhead is option D.

upvoted 1 times

 **studynoplay** 10 months, 2 weeks ago

Selected Answer: D

LEAST operational overhead = Serverless = Cognito user pool

upvoted 1 times

 **cheese929** 10 months, 3 weeks ago

Selected Answer: D

D is correct.

upvoted 1 times

 **k33** 1 year ago

Selected Answer: D

Answer : D

upvoted 1 times

 **Hello4me** 1 year ago

D is correct

upvoted 1 times

 **Mahadeva** 1 year, 2 months ago

Selected Answer: A

There is a difference between "Grant Access" (Authentication done by Cognito user pool), and "Control Access" to APIs (Authorization using IAM policy, custom Authorizer, Federated Identity Pool). The question very specifically asks about *Control access to REST APIs* which is a clear case of Authorization and not Authentication. So custom Authorizer using Lambda in API Gateway is the solution.

Pls refer to this blog: <https://aws.amazon.com/blogs/security/building-fine-grained-authorization-using-amazon-cognito-api-gateway-and-iam/>
upvoted 1 times

 **Mahadeva** 1 year, 2 months ago

Option D: there is nothing called Cognito user pool authorizer. We only have custom Authorizer function through Lambda.

upvoted 1 times

 **JayBee65** 1 year, 2 months ago

Oh yes there is :)

upvoted 3 times

 **TungPham** 1 year ago

Control access to a REST API using Amazon Cognito user pools as authorizer

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

upvoted 3 times

 **JayBee65** 1 year, 2 months ago

This answer looks to be entirely wrong

This article explains how to do what you claim cannot be done: <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html>

[integrate-with-cognito.html](#)

It starts "As an alternative to using IAM roles and policies or Lambda authorizers (formerly known as custom authorizers), you can use an Amazon Cognito user pool to control who can access your API in Amazon API Gateway."

This suggests that Amazon Cognito user pools CAN be used for Authorization, which you say above cannot be done.

Further, it explains how to do this...

"To use an Amazon Cognito user pool with your API, you must first create an authorizer of the COGNITO_USER_POOLS type and then configure an API method to use that authorizer"

So whilst A is a valid approach, it looks like D achieves the same with "the LEAST operational overhead".

upvoted 7 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: D

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

upvoted 4 times

 **MutiverseAgent** 8 months ago

up this

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D - As company already has all the users authentication information in Cognito

upvoted 1 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: D

D is correct

upvoted 2 times

Question #201

Topic 1

A company is developing a marketing communications service that targets mobile app users. The company needs to send confirmation messages with Short Message Service (SMS) to its users. The users must be able to reply to the SMS messages. The company must store the responses for a year for analysis.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon Connect contact flow to send the SMS messages. Use AWS Lambda to process the responses.
- B. Build an Amazon Pinpoint journey. Configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving.
- C. Use Amazon Simple Queue Service (Amazon SQS) to distribute the SMS messages. Use AWS Lambda to process the responses.
- D. Create an Amazon Simple Notification Service (Amazon SNS) FIFO topic. Subscribe an Amazon Kinesis data stream to the SNS topic for analysis and archiving.

Correct Answer: A

Community vote distribution



TariqKipkemei Highly Voted 6 months, 1 week ago

Selected Answer: B

Marketing communications = Amazon Pinpoint
upvoted 9 times

cookieMr Highly Voted 9 months ago

Selected Answer: B

By using Pinpoint, the company can effectively send SMS messages to its mobile app users. Additionally, Pinpoint allows the configuration of journeys, which enable the tracking and management of user interactions. The events generated during the journey, including user responses to SMS, can be captured and sent to an Kinesis data stream. This data stream can then be used for analysis and archiving purposes.

- A. Creating an Amazon Connect contact flow is primarily focused on customer support and engagement, and it lacks the capability to store and process SMS responses for analysis.
- C. Using SQS is a message queuing service and is not specifically designed for handling SMS responses or capturing them for analysis.
- D. Creating an SNS FIFO topic and subscribing a Kinesis data stream is not the most appropriate solution for capturing and storing SMS responses, as SNS is primarily used for message publishing and distribution.

In summary, option B is the best choice as it leverages Pinpoint to send SMS messages and captures user responses for analysis and archiving using an Kinesis data stream.

upvoted 5 times

scar0909 Most Recent 2 weeks, 1 day ago

Selected Answer: A

<https://docs.aws.amazon.com/connect/latest/adminguide/setup-sms-messaging.html>
upvoted 1 times

MoshiurGCP 1 month ago

Why not A. Amazon connect has this option.
upvoted 1 times

awsgeek75 2 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/pinpoint/latest/userguide/welcome.html>
Amazon Pinpoint is the easiest solution.
Amazon Connect is Contact Centre as a Service so this option is not relevant to the requirement.
SQS and SNS options are overengineered or under engineered for the requirements so natural choice is "B"
upvoted 1 times

whoob 5 months, 4 weeks ago

base function of AWS Pinpoint
upvoted 1 times

Guru4Cloud 6 months, 2 weeks ago

Selected Answer: B

B. AWS Pinpoint is for Marketing communications.

upvoted 3 times

✉ **Bmarodi** 9 months, 2 weeks ago

Selected Answer: B

Option B is correct answer: link: <https://aws.amazon.com/pinpoint/>, and video under the link.

upvoted 2 times

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

Selected Answer: B

Two-Way Messaging

Receive SMS messages from your customers and reply back to them in a chat-like interactive experience. With Amazon Pinpoint, you can create automatic responses when customers send you messages that contain certain keywords.

upvoted 1 times

✉ **CLOUDUMASTER** 10 months, 4 weeks ago

Based on my research Kinesis stream is real time data ingestion, and also stores only event data and not the actual people responses, furthermore there is no requirement to have real time data streaming. That is probably why I am hesitating agree here with everyone on B and rather choose A.

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

"A Kinesis data stream stores records for 24 hours by default, up to 365 days (8,760 hours)."

<https://aws.amazon.com/de/blogs/big-data/retaining-data-streams-up-to-one-year-with-amazon-kinesis-data-streams/#:~:text=A%20Kinesis%20data%20stream%20stores,parallel%20and%20at%20low%2Dlatency>.

upvoted 1 times

✉ **jayce5** 11 months ago

Selected Answer: B

The answer is B. AWS Pinpoint is for Marketing communications.

AWS Connect is for Contact center.

upvoted 2 times

✉ **jaswantn** 11 months ago

Selected Answer: A

According to the following link I would choose Option A.

<https://docs.aws.amazon.com/connect/latest/adminguide/web-and-mobile-chat.html>

upvoted 1 times

✉ **smartegnine** 9 months, 3 weeks ago

no no, there is no SMS, note the question stated all activities through SMS, also Amazon connect flow most likely working on web application UI, but if you see question clearly, this is receiving and sending SMS not through application UI (Web/Mobile App). So for those reason we choose B

upvoted 2 times

✉ **ProfXsamson** 1 year, 1 month ago

Selected Answer: B

Amazon Pinpoint is a flexible, scalable and fully managed push notification and SMS service for mobile apps.

upvoted 3 times

✉ **Foucault** 1 year, 2 months ago

It's B, see following link <https://docs.aws.amazon.com/pinpoint/latest/developerguide/event-streams.html>

upvoted 2 times

✉ **LuckyAro** 1 year, 2 months ago

Selected Answer: B

<https://aws.amazon.com/pinpoint/product-details/sms/>

Two-Way Messaging:

Receive SMS messages from your customers and reply back to them in a chat-like interactive experience. With Amazon Pinpoint, you can create automatic responses when customers send you messages that contain certain keywords. You can even use Amazon Lex to create conversational bots.

A majority of mobile phone users read incoming SMS messages almost immediately after receiving them. If you need to be able to provide your customers with urgent or important information, SMS messaging may be the right solution for you.

You can use Amazon Pinpoint to create targeted groups of customers, and then send them campaign-based messages. You can also use Amazon Pinpoint to send direct messages, such as appointment confirmations, order updates, and one-time passwords.

upvoted 2 times

✉ **DavidNamy** 1 year, 2 months ago

Selected Answer: D

D:

Amazon Simple Notification Service (SNS) is a fully managed messaging service that enables you to send and receive SMS messages in a cost-effective and highly scalable way. By creating an SNS FIFO topic, you can ensure that the SMS messages are delivered to your users in the order they were sent and that the SMS responses are processed and stored in the same order. You can also configure your SNS FIFO topic to publish SMS responses to an Amazon Kinesis data stream, which will allow you to store and analyze the responses for a year.

Amazon Pinpoint ?¿¿? NO!

is not correct solution because while Amazon Pinpoint allows you to send SMS and Email campaigns, as well as handle push notifications to a user base, it doesn't provide SMS sending feature by itself. Furthermore, it's a service mainly focused on sending and tracking marketing campaigns, not for managing two-way SMS communication and the reception of reply.

upvoted 3 times

✉️👤 Omok 1 year, 1 month ago

What do think about <https://docs.aws.amazon.com/pinpoint/latest/userguide/channels-sms-two-way.html>?

upvoted 1 times

✉️👤 Buruguduystunstugudunstuy 1 year, 3 months ago

Selected Answer: B

To send SMS messages and store the responses for a year for analysis, the company can use Amazon Pinpoint. Amazon Pinpoint is a fully-managed service that allows you to send targeted and personalized SMS messages to your users and track the results.

To meet the requirements of the company, a solutions architect can build an Amazon Pinpoint journey and configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving. The Kinesis data stream can be configured to store the data for a year, allowing the company to analyze the responses over time.

So, Option B is the correct answer.

Option B. Build an Amazon Pinpoint journey. Configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving.

upvoted 3 times

Question #202

Topic 1

A company is planning to move its data to an Amazon S3 bucket. The data must be encrypted when it is stored in the S3 bucket. Additionally, the encryption key must be automatically rotated every year.

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

- A. Move the data to the S3 bucket. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.
- B. Create an AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket.
- C. Create an AWS Key Management Service (AWS KMS) customer managed key. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket. Manually rotate the KMS key every year.
- D. Encrypt the data with customer key material before moving the data to the S3 bucket. Create an AWS Key Management Service (AWS KMS) key without key material. Import the customer key material into the KMS key. Enable automatic key rotation.

Correct Answer: B

Community vote distribution

B (57%)

A (42%)

 **Buruguduystunstugudunstuy**  1 year, 3 months ago

Selected Answer: A

KEYWORD: LEAST operational overhead

To encrypt the data when it is stored in the S3 bucket and automatically rotate the encryption key every year with the least operational overhead, the company can use server-side encryption with Amazon S3-managed encryption keys (SSE-S3). SSE-S3 uses keys that are managed by Amazon S3, and the built-in key rotation behavior of SSE-S3 encryption keys automatically rotates the keys every year.

To meet the requirements of the company, the solutions architect can move the data to the S3 bucket and enable server-side encryption with SSE-S3. This solution requires no additional configuration or maintenance and has the least operational overhead.

Hence, the correct answer is;

Option A. Move the data to the S3 bucket. Use server-side encryption with Amazon S3-managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.

upvoted 31 times

 **bicrasse** 4 months, 1 week ago

The good answer was B before May 2022, because the rotation schedule for AWS managed keys was 3 years (SSE-S3 is based on it)...

From May 2022 the schedule rotation is 1 year, then A is now the best answer because there is NO operational task to do: S3 is by default encrypted at rest with SSE-S3 (rotation every year)... So it depends if the question has been updated since 2022

upvoted 5 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option B involves using a customer-managed AWS KMS key and enabling automatic key rotation, but this requires the company to manage the KMS key and monitor the key rotation process.

Option C involves using a customer-managed AWS KMS key, but this requires the company to manually rotate the key every year, which introduces additional operational overhead.

Option D involves encrypting the data with customer key material and creating a KMS key without key material, but this requires the company to manage the customer key material and import it into the KMS key, which introduces additional operational overhead.

upvoted 2 times

 **JayBee65** 1 year, 2 months ago

But...

For A there is no reference to how often these keys are rotated, and to rotate to a new key, you need to upload it, which is operational overhead. So not only does it not necessarily meet the 'rotate keys every year' requirement, but every year it requires operational overhead.

More importantly, the question states move the objects first, and then configure encryption, but ... "There is no change to the encryption of the objects that existed in the bucket before default encryption was enabled." from <https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>

So A is clearly wrong.

For B, whilst you have to set up KMS once, you then don't have to anything else, which i would say is LEAST operational overhead.
upvoted 17 times

 **ocbn3wby** 1 year, 2 months ago

God bless you, man! The most articulated answers, easy to understand. Good job!
upvoted 4 times

 **JayBee65** 1 year, 2 months ago

But wrong :)
upvoted 4 times

 **ocbn3wby** 1 year, 1 month ago

Reviewed it the second time. Some of them are wrong, indeed.
upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

The order of these events is being ignored here in my opinion. The encryption checkbox needs to be checked before data is moved into the S3 bucket or it will not be encrypted otherwise, you'll have to encrypt manually and reload into S3 bucket. If the box was checked before moving data into S3 then you are good to go !

upvoted 8 times

 **LuckyAro** 1 year, 1 month ago

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>
upvoted 1 times

 **Wang87** 2 months, 3 weeks ago

SSE DOES not rotate encryption keys, it changes master key used to lock encryption keys which creates new ciphered key and stores it.
upvoted 1 times

 **Smart** 7 months, 3 weeks ago

Ignoring the new changes that the default encryption is already enabled. I agree that the encryption should be configured before moving the data into the bucket. Otherwise, the existing objects will remain unencrypted.

Correct Answer is B.

Additionally, where is the reference that SSE-S3 will rotate keys every year (which is the question's requirement).

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

SSE-S3 rotates the keys when AWS wants it, not "every year" like required here.
upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

No, I stand corrected.

All AWS managed keys are automatically rotated every year. You cannot change this rotation schedule.

upvoted 3 times

 **awsgEEK75** 2 months, 3 weeks ago

I want to find a source for this yearly rotation because SSE-S3 just rotates periodically and doesn't say it follows the same policy as other managed key. I think you may be right but just need a doc link
upvoted 2 times

 **Maru86** 3 weeks, 5 days ago

https://repost.aws/questions/QUES_1VN01TU-eRSO3LXergA/s3-managed-key-sse-s3-rotation-period
upvoted 1 times

 **tohegajaf** 2 months, 3 weeks ago

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys
upvoted 1 times

 **techhb**  1 year, 3 months ago

Selected Answer: B

SSE-S3 - is free and uses AWS owned CMKs (CMK = Customer Master Key). The encryption key is owned and managed by AWS, and is shared among many accounts. Its rotation is automatic with time that varies as shown in the table here. The time is not explicitly defined.

SSE-KMS - has two flavors:

AWS managed CMK. This is free CMK generated only for your account. You can only view its policies and audit usage, but not manage it. Rotation is automatic - once per 1095 days (3 years),

Customer managed CMK. This uses your own key that you create and can manage. Rotation is not enabled by default. But if you enable it, it will be automatically rotated every 1 year. This variant can also use an imported key material by you. If you create such key with an imported material, there is no automated rotation. Only manual rotation.

SSE-C - customer provided key. The encryption key is fully managed by you outside of AWS. AWS will not rotate it.

upvoted 28 times

 **ruqui** 10 months ago

AWS managed CMK rotates every 365 days (not 1095 days). Reference:
<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#key-mgmt>
 upvoted 2 times

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

It's A. Because it's said that they need with LEAST operation overhead and S3 Managed Keys can rotate automatically every year without needing the user intervention. For the Customer Managed Keys, you need to do some configuration for that.
 upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

Selected Answer: A

Both A and B are viable answers but A with SSE-S3 is least operational overhead. B will require customer to manage the key.
 HOWEVER note that SSE-S3 managed keys are rotated periodically so there is no user control on limiting the rotation to "once a year". For exam, probably read the question with full context and hope there is more detail in the actual exam!
 upvoted 1 times

 **SinghJagdeep** 2 months, 3 weeks ago

Selected Answer: B

Please see JayBee response below. Make sense.
 upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Selected Answer: A

Now "all AWS managed keys are automatically rotated every year. You cannot change this rotation schedule". However, if you insist that option A also specifies the order of steps then it would be wrong, you'd need to enable encryption BEFORE moving the data to the bucket. But per my understanding of English, the order is not specified, it's just a combination of things you do.

Otherwise B would be the correct answer, but it has more operational overhead than A, at least now. Probably the question is old.
 upvoted 1 times

 **ale_brd_** 3 months, 1 week ago

Selected Answer: B

nowhere in this documentation states how often the keys are rotated, and only the key that encrypts the S3 encryption key actually gets to rotate.
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingServerSideEncryption.html>
 upvoted 1 times

 **xdkonorek2** 4 months, 2 weeks ago

Selected Answer: B

I'm voting B
 Each object in s3 using SSE-S3 uses separate key, this key is encrypted using another master key that is regularly rotated but AWS doesn't share how often it happens.

With SSE-KMS you have option to tick: "Automatically rotate this KMS key every year.".
 upvoted 1 times

 **bogobob** 4 months, 2 weeks ago

In 2023 the answer would be A. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingServerSideEncryption.html> states that S3 automatically uses SSE, and rotates the keys "regularly" which as far as I've understood is yearly
 upvoted 1 times

 **theonlyhero** 3 months, 4 weeks ago

but based on this reference:

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

it mentions varies, so i would stick with B

upvoted 1 times

 **rlamberti** 5 months ago

Selected Answer: A

SSE-S3 are rotated automatically every year. Default behaviour.
 upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: A

LEAST operational overhead = Amazon S3 managed encryption keys
 upvoted 3 times

 **XCheng** 6 months, 1 week ago

Selected Answer: —

https://docs.aws.amazon.com/zh_cn/AmazonS3/latest/userguide/default-bucket-encryption.html
 upvoted 1 times

 **roggerrubens** 6 months, 1 week ago

Resposta A , todo objeto que é colocado no S3 , e automaticamente criptografado por padrão SSE-S3 , não ???
upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: B

B. Create an AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket.

upvoted 3 times

 **Jeyaluxshan** 6 months, 2 weeks ago

Answer is B.
SSE-S3 encryption will not apply to existing objects in S3 bucket.
Question is when it is stored in S3, data must be encrypted.
If you already stored and later enable SSE-S3, will not be a solution.
So A is not the correct answer.
upvoted 2 times

 **omar_bahrain** 6 months, 3 weeks ago

Selected Answer: A

Once you enable SSE-S3 encryption for your S3 bucket, Amazon automatically rotates the data encryption keys for your objects every 365 days. This means that your data encryption keys are automatically replaced with new ones every year. You can also manually rotate the encryption keys for your objects at any time.

<https://saturncloud.io/blog/how-does-amazon-sse-s3-key-rotation-work/#:~:text=Once%20you%20enable%20SSE%2DS3,your%20objects%20at%20any%20time.>

upvoted 1 times

 **Sutariya** 6 months, 3 weeks ago

B is right Answer : If you need more control over your keys, such as managing key rotation and access policy grants, you can choose to use server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS), or dual-layer server-side encryption with AWS KMS keys (DSSE-KMS). For more information about editing KMS keys
upvoted 1 times

Question #203

Topic 1

The customers of a finance company request appointments with financial advisors by sending text messages. A web application that runs on Amazon EC2 instances accepts the appointment requests. The text messages are published to an Amazon Simple Queue Service (Amazon SQS) queue through the web application. Another application that runs on EC2 instances then sends meeting invitations and meeting confirmation email messages to the customers. After successful scheduling, this application stores the meeting information in an Amazon DynamoDB database.

As the company expands, customers report that their meeting invitations are taking longer to arrive.

What should a solutions architect recommend to resolve this issue?

- A. Add a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database.
- B. Add an Amazon API Gateway API in front of the web application that accepts the appointment requests.
- C. Add an Amazon CloudFront distribution. Set the origin as the web application that accepts the appointment requests.
- D. Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

Correct Answer: D

Community vote distribution

D (100%)

 **Buruguduystunstugudunstuy**  1 year, 3 months ago

Selected Answer: D

Option D. Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

To resolve the issue of longer delivery times for meeting invitations, the solutions architect can recommend adding an Auto Scaling group for the application that sends meeting invitations and configuring the Auto Scaling group to scale based on the depth of the SQS queue. This will allow the application to scale up as the number of appointment requests increases, improving the performance and delivery times of the meeting invitations.

upvoted 9 times

 **cookieMr**  9 months ago

Selected Answer: D

By adding an ASG for the application that sends meeting invitations and configuring it to scale based on the depth of the SQS, the system can automatically adjust its capacity based on the number of pending messages in the queue. This ensures that the application can handle increased message load and process the meeting invitations more efficiently, reducing the delay experienced by customers.

- A. Adding a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database would improve read performance for DynamoDB, but it does not directly address the issue of delayed meeting invitations.
- B. Adding an API Gateway API in front of the web application that accepts the appointment requests may help with request handling and management, but it does not directly address the issue of delayed meeting invitations.
- C. Adding an CloudFront distribution with the web application as the origin would improve content delivery and caching, but it does not directly address the issue of delayed meeting invitations.

upvoted 7 times

 **67a3f49**  1 month ago

First question with consistent answer :)

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: D

Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

upvoted 1 times

✉️  **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D is the right Answer,
upvoted 2 times

✉️  **k1kavi1** 1 year, 3 months ago

Selected Answer: D

Agreed
upvoted 1 times

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

Selected Answer: D

ANswer d
upvoted 1 times

✉️  **leonnnn** 1 year, 3 months ago

Selected Answer: D

D meets the requirements
upvoted 1 times

✉️  **Nigma** 1 year, 3 months ago

Selected Answer: D

Answer : D
upvoted 1 times

Question #204

Topic 1

An online retail company has more than 50 million active customers and receives more than 25,000 orders each day. The company collects purchase data for customers and stores this data in Amazon S3. Additional customer data is stored in Amazon RDS.

The company wants to make all the data available to various teams so that the teams can perform analytics. The solution must provide the ability to manage fine-grained permissions for the data and must minimize operational overhead.

Which solution will meet these requirements?

- A. Migrate the purchase data to write directly to Amazon RDS. Use RDS access controls to limit access.
- B. Schedule an AWS Lambda function to periodically copy data from Amazon RDS to Amazon S3. Create an AWS Glue crawler. Use Amazon Athena to query the data. Use S3 policies to limit access.
- C. Create a data lake by using AWS Lake Formation. Create an AWS Glue JDBC connection to Amazon RDS. Register the S3 bucket in Lake Formation. Use Lake Formation access controls to limit access.
- D. Create an Amazon Redshift cluster. Schedule an AWS Lambda function to periodically copy data from Amazon S3 and Amazon RDS to Amazon Redshift. Use Amazon Redshift access controls to limit access.

Correct Answer: D

Community vote distribution

C (100%)

✉️  **anhike**  1 year, 3 months ago

Answer : C keyword "manage-fine-grained"
<https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/>
 upvoted 20 times

✉️  **markw92** 9 months, 1 week ago

You can manage fine grained using redshift as well - <https://aws.amazon.com/blogs/big-data/achieve-fine-grained-data-security-with-row-level-access-control-in-amazon-redshift/>
 But, I believe the keyword to look for is "minimize operational overhead", which lakeformation does without duplicating much of the data. Redshift is operational overhead and duplication of data. not sure why the answer is D. i vote C as well.
 upvoted 7 times

✉️  **Olaunfazed** 8 months, 4 weeks ago

yeah, most of examtopics answers are wrong
 upvoted 7 times

✉️  **LoXoL**  2 months, 1 week ago

Selected Answer: C
 C represents the easiest way to ingest data from S3 and control accesses.
 upvoted 1 times

✉️  **karloscetina007** 5 months, 4 weeks ago

Selected Answer: C
 a fine grained permissions is one of the conditions to accomplish with the requirement.
 With the use of AWS Glue you can get accomplish with this requirement.
 My answer is: C
 upvoted 3 times

✉️  **TariqKipkemei** 6 months, 1 week ago

Selected Answer: C
 With Lake formation you can scale permissions more easily with fine-grained security capabilities, including row- and cell-level permissions and tag-based access control.
 upvoted 4 times

✉️  **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: C
 Lake Formation enables the creation of a secure and scalable data lake on AWS, allowing centralized access controls for both S3 and RDS data. By using Lake Formation, the company can manage permissions effectively and integrate RDS data through the AWS Glue JDBC connection. Registering the S3 in Lake Formation ensures unified access control. This solution reduces operational overhead while providing fine-grained permissions management.
 upvoted 3 times

 **cookieMr** 9 months ago

Selected Answer: C

Lake Formation enables the creation of a secure and scalable data lake on AWS, allowing centralized access controls for both S3 and RDS data. By using Lake Formation, the company can manage permissions effectively and integrate RDS data through the AWS Glue JDBC connection. Registering the S3 in Lake Formation ensures unified access control. This solution reduces operational overhead while providing fine-grained permissions management.

A. Directly writing purchase data to Amazon RDS with RDS access controls lacks comprehensive permissions management for both S3 and RDS data.

B. Periodically copying data from RDS to S3 using Lambda and using AWS Glue and Athena for querying does not offer fine-grained permissions management and introduces data synchronization complexities.

D. Creating an Redshift cluster and copying data from S3 and RDS to Redshift adds complexity and operational overhead without the flexibility of Lake Formation's permissions management capabilities.

upvoted 3 times

 **pisica134** 9 months ago

Answer is C AWS Lake Formation provides a comprehensive solution for building and managing a data lake. It simplifies data ingestion, organization, and access control. By creating a data lake using AWS Lake Formation, you can centralize and govern access to your data across multiple sources.

upvoted 1 times

 **Bmarodi** 9 months, 2 weeks ago

Selected Answer: C

Option C is right answer: <https://docs.aws.amazon.com/lake-formation/latest/dg/what-is-lake-formation.html>

upvoted 1 times

 **Abrar2022** 9 months, 4 weeks ago

Lake Formation helps you manage fine-grained access for internal and external customers from a centralized location and in a scalable way.

upvoted 1 times

 **doorahmie** 1 year, 1 month ago

<https://docs.aws.amazon.com/lake-formation/latest/dg/access-control-overview.html>

upvoted 2 times

 **LuckyAro** 1 year, 2 months ago

Selected Answer: C

To me, the give-away was: "The company wants to make all the data available to various teams" - Data-Lake - All data in one place.

upvoted 4 times

 **master1004** 1 year, 2 months ago

The correct answer is D.

The company uses all the data from various teams so that the teams can do their analysis.

Therefore, it is the best way to separately configure redshift for data warehousing and for all employees to connect to the redshift DB and perform analysis tasks without burdening the operating DB (must minimize operational overhead).

upvoted 3 times

 **ruqui** 9 months, 3 weeks ago

I don't think that "periodically copy data from Amazon S3 and RDS to Redshift" minimize the operational overhead. The correct answer for me is C

upvoted 2 times

 **aba2s** 1 year, 2 months ago

Selected Answer: C

Manage fine-grained access control using AWS Lake Formation

<https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/>

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: C

Option C. Create a data lake by using AWS Lake Formation. Create an AWS Glue JDBC connection to Amazon RDS. Register the S3 bucket in Lake Formation. Use Lake Formation access controls to limit access.

To make all the data available to various teams and minimize operational overhead, the company can create a data lake by using AWS Lake Formation. This will allow the company to centralize all the data in one place and use fine-grained access controls to manage access to the data.

To meet the requirements of the company, the solutions architect can create a data lake by using AWS Lake Formation, create an AWS Glue JDBC connection to Amazon RDS, and register the S3 bucket in Lake Formation. The solutions architect can then use Lake Formation access controls to limit access to the data. This solution will provide the ability to manage fine-grained permissions for the data and minimize operational overhead.

upvoted 3 times

 **majdango** 10 months, 1 week ago

.....

upvoted 1 times

 **kvenikoduru** 1 year, 3 months ago

Selected Answer: C

a combination of the following 2 URLs I believe it is C

<https://aws.amazon.com/lake-formation/>

<https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/>

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Option C is the right answer. Fine-grained access-control from different types of data sources is a Lakeformation usecase.

upvoted 2 times

 **gloritown** 1 year, 3 months ago

Selected Answer: C

CCCCCCCCCC

upvoted 2 times

Question #205

Topic 1

A company hosts a marketing website in an on-premises data center. The website consists of static documents and runs on a single server. An administrator updates the website content infrequently and uses an SFTP client to upload new documents.

The company decides to host its website on AWS and to use Amazon CloudFront. The company's solutions architect creates a CloudFront distribution. The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin.

Which solution will meet these requirements?

- A. Create a virtual server by using Amazon Lightsail. Configure the web server in the Lightsail instance. Upload website content by using an SFTP client.
- B. Create an AWS Auto Scaling group for Amazon EC2 instances. Use an Application Load Balancer. Upload website content by using an SFTP client.
- C. Create a private Amazon S3 bucket. Use an S3 bucket policy to allow access from a CloudFront origin access identity (OAI). Upload website content by using the AWS CLI.
- D. Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP. Configure the S3 bucket for website hosting. Upload website content by using the SFTP client.

Correct Answer: C*Community vote distribution*

C (74%)

D (26%)

 **bjexamprep**  7 months, 3 weeks ago

Selected Answer: C

The question here is whether the solution architect can change the requirement. The requirement says very clear about SFTP which cannot be addressed by option C. But the question also gives very clear hint about OAI which cannot be addressed by option D. Option D also doesn't mention anything about CloudFront which is part of the requirement of the question.

So, if the requirement cannot be changed, D is the answer; if the requirement can be changed, C is the answer. But if the requirement can be changed, what's the limitation? That will be a Chaos.

I'm voting C, and curse the question designer.

upvoted 11 times

 **Iconique** 6 months ago

"The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin." The solution architect is looking for a solution that can fit with CloudFront as origin! So it doesn't matter that option D does not mention CF, CF is part of the solution!

Having a marketing website on-premise clearly indicates having S3 as static content.

AWS Transfer Family is the way to upload files via FTP to S3!

So the answer is D.

Why not C?

User is already uploading content via FTP, option C is eliminating this option for him and forces using the CLI. The solution from C does not meet the requirements of having FTP.

upvoted 5 times

 **cookieMr**  9 months ago

Selected Answer: C

Hosting the website in a private S3 provides cost-effective and highly available storage for the static website content. By configuring a bucket policy to allow access from a CloudFront OAI, the S3 can be securely accessed only through CloudFront. This ensures that the website content is served through CloudFront while keeping the S3 private. Uploading website content using the AWS CLI allows for easy and efficient content management.

A. Hosting the website on an Lightsail virtual server would introduce additional management overhead and costs compared to using S3 directly for static content hosting.

B. Using an AWS ASG with EC2 instances and an ALB is not necessary for serving static website content. It would add unnecessary complexity and cost.

D. While using AWS Transfer for SFTP allows for SFTP uploads, it introduces additional costs and complexity compared to directly uploading content to an S3 using the AWS CLI. Additionally, hosting the website content in a public S3 may not be desirable from a security standpoint.

upvoted 5 times

 **djgodzilla**  3 months ago

Selected Answer: D

you can see in this figure that transfer family framework allows for the data to be available for a broad variety of use cases including content distribution (CF) <https://d1.awsstatic.com/HIW%20SFTP%20Connectors%20v3.920176622d281d0bd087518827314169b496a055.png>

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

Two main problems with D:

It's public S3 behind CloudFront which is not well-architected

Infrequent site updates using SFTP so with S3 it will be cli changes. They don't need fancy transfer for this. Right?

upvoted 1 times

 **MiniYang** 3 months, 3 weeks ago

Selected Answer: C

I think the this is a big misleading " SFTP" (doesn't usually upload) , and it said clearly need Cloudfront and want a cheep solution. So I chose "C"

upvoted 1 times

 **rlamberti** 5 months ago

Selected Answer: C

Transferring via AWS CLI is cheaper than via Transfer Family.

It is not the best option, but will do the job of uploading the data to S3.

upvoted 1 times

 **juanrasus2** 5 months, 1 week ago

I'd go with D. In C there is no mention to S3 bucket being configured for web hosting. Simply adding the Cloudfront distribution and pointing that to the S3 won't work out of the box.

upvoted 2 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

D - SFTP client to upload new documents.

upvoted 1 times

 **baku98** 3 months, 1 week ago

D is the only one possible.

C cannot be because: In Amazon CloudFront: For Restricting access to an Amazon S3 origin: If your origin is an Amazon S3 bucket configured as a website endpoint, you must set it up with CloudFront as a custom origin. That means you can't use OAC (or OAI).

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

I changed C. is better then D

upvoted 2 times

 **eugene_stalker** 10 months ago

Selected Answer: D

D - SFTP client to upload new documents.

upvoted 1 times

 **bdp123** 1 year, 1 month ago

Selected Answer: C

AWS transfer is a cost and doesn't mention using CloudFront

<https://aws.amazon.com/aws-transfer-family/pricing/>

upvoted 4 times

 **Yelizaveta** 1 year, 1 month ago

Selected Answer: C

If you don't want to disable block public access settings for your bucket but you still want your website to be public, you can create a Amazon CloudFront distribution to serve your static website. For more information, see Use an Amazon CloudFront distribution to serve a static website in the Amazon Route 53 Developer Guide.

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

upvoted 1 times

 **PDR** 1 year, 1 month ago

Selected Answer: C

I at first thought D but it is in fact C because

"D: Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP. Configure the S3 bucket for website hosting. Upload website content by using the SFTP client." questions says that the company has decided to use Amazon Cloudfront and this answer does not reference using CF and setting S3 as the Origin

"C. Create a private Amazon S3 bucket. Use an S3 bucket policy to allow access from a CloudFront origin access identity (OAI). Upload website content by using the AWS CLI." - mentions CF and the origin and the AWS CLI does infact support transfer by SFTP (which was the part I originally doubted but this link evidences that it does:

<https://docs.aws.amazon.com/cli/latest/reference/transfer/describe-server.html>

upvoted 3 times

✉ **bullrem** 1 year, 2 months ago

Selected Answer: D

Option C, creating a private Amazon S3 bucket and using an S3 bucket policy to allow access from a CloudFront origin access identity (OAI), would not be the most cost-effective solution. While it would allow the company to use Amazon S3 for storage, it would also require additional setup and maintenance of the OAI, which would add additional cost. Additionally, this solution would not allow the use of SFTP client for uploading content which is the current method used by the company.

upvoted 1 times

✉ **verguy** 1 year, 2 months ago

The Answer is C

<https://medium.com/aws-poc-and-learning/how-to-access-s3-hosted-website-via-cloudfront-using-oai-origin-access-identity-720ad7c57f15>

upvoted 2 times

✉ **Mahadeva** 1 year, 2 months ago

Selected Answer: C

Option C is a better choice than D for following reasons:

- (1) Cost effective: data transfer is cheaper for Cloudfront than directly from S3 bucket
- (2) Resilient: recovery from failures. Having a Cloudfront distribution and making S3 bucket policy only for Cloudfront. ie. private bucket (with OAI for access) hardens and betters resiliency.

upvoted 3 times

✉ **gustavtd** 1 year, 2 months ago

Selected Answer: C

If you don't do extra setup in AWS, you can not use SFTP connecting to it, so D is not the case

upvoted 1 times

✉ **vtbk** 1 year, 2 months ago

Selected Answer: C

s3 + Cloudfront. In this case, S3 does not need to be public.

upvoted 1 times

✉ **Zerotn3** 1 year, 2 months ago

Selected Answer: D

The most cost-effective and resilient solution for hosting a website on AWS with CloudFront is to create a public Amazon S3 bucket, configure AWS Transfer for SFTP, configure the S3 bucket for website hosting, and then upload website content using the SFTP client.

Option A involves using Amazon Lightsail to create a virtual server, which may not be the most cost-effective solution compared to using S3. Option B involves using an Auto Scaling group with EC2 instances and an Application Load Balancer, which may be more expensive and complex than using S3. Option C involves creating a private S3 bucket, which may not allow CloudFront to access the website content.

upvoted 2 times

Question #206

Topic 1

A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.

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

- A. Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a CreateImage API call is detected.
- B. Configure AWS CloudTrail with an Amazon Simple Notification Service (Amazon SNS) notification that occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on CreateImage when an API call is detected.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected.
- D. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a CreateImage API call is detected.

Correct Answer: D

Community vote distribution



✉️ [User] [Removed] Highly Voted 1 year, 3 months ago

Selected Answer: C

I'm team C.

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html#:~:text=For%20example%2C%20you%20can%20create%20an%20EventBridge%20rule%20that%20detects%20when%20the%20AMI%20creation%20process%20has%20completed%20and%20then%20invokes%20an%20Amazon%20SNS%20topic%20to%20send%20an%20email%20notification%20to%20you>.

upvoted 18 times

✉️ [User] MutiverseAgent 8 months ago

C is correct > <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitor-ami-events.html>

upvoted 1 times

✉️ [User] JayBee65 1 year, 2 months ago

That link contains the exact use case and explains how C can be used.

Option B requires you to send logs to S3 and use Athena, 2 additional services that are not required, so this does not meet the "LEAST operational overhead?" requirement, since these are extra services requiring management.

upvoted 4 times

✉️ [User] Wajif Highly Voted 1 year, 3 months ago

Selected Answer: A

Why not A? API calls are already logged in Cloudtrail.

upvoted 15 times

✉️ [User] pentium75 2 months, 4 weeks ago

"Least operational overhead" is when the event triggers an action, not when you run a scheduled task that searches logs for the event.

upvoted 3 times

✉️ [User] Mahmouddd 3 days, 23 hours ago

Just took the exam today, most of the questions were from here wish I saw them all to be honest before entering the exam. Anyways, this question was at the exam, I picked option A because as the question stated it wanted two things not one thing only an application that CAPTURES API calls and SEND ALERTS WHENEVER Createimage API call is made, OPTION C CLEARLY STATES THAT IN THIS CASE IT WILL ONLY LOOK FOR CREATEIMAGE API CALL it will not capture other API calls like the lambda in option A would! Am I the only one that thinks that or what? TBH I am not sure about anything in this question but that is why I did not pick option C during the exam.

upvoted 1 times

✉️ [User] bujuman 1 month, 3 weeks ago

Selected Answer: D

On of the requirements is LEAST operational overhead

CloudTrail sends a notification when log files are written to the Amazon S3 bucket. An active account can generate a large number of notifications. If you subscribe with email or SMS, you can receive a large volume of messages. We recommend that you subscribe using Amazon Simple Queue Service (Amazon SQS), which lets you handle notifications programmatically. For more information, see Subscribing a Queue to an Amazon SNS Topic in the Amazon Simple Queue Service Developer Guide.

upvoted 1 times

 **Wang87** 2 months, 3 weeks ago

Selected Answer: C

Answer is c.

upvoted 1 times

 **farnamjam** 2 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

 **master9** 3 months ago

Selected Answer: D

AWS CloudTrail primarily focuses on auditing and recording API calls made in your AWS account. It logs all API requests made via the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This includes the identity of the caller, the time of the API call, the source IP address of the caller, the request parameters, and the response elements returned by the AWS service. This information is useful for security analysis, resource change tracking, and troubleshooting.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

But this is not about "auditing and recording", you don't want to create reports who created images during the last year, you want an instant alert when someone creates an image. Thus CloudWatch Events.

upvoted 1 times

 **Sadish** 3 months ago

Cloud Watch = AWS Monitoring service for any AWS resources

Cloud Trail = AWS API monitoring service with respect to application event that are hosted on AWS.

Answer would be "C"

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html>
service

upvoted 2 times

 **rlamberti** 5 months ago

Selected Answer: C

"LEAST operational overhead"

Option A envolves coding a Lambda. Not good!

Option C seems to be the correct.

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: C

Event bridge was built specifically to handle this kind of scenario:

CreateImage API call (Event Source) -> Event bus -> Rules -> Amazon SNS (Event target)

upvoted 4 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: C

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected

upvoted 3 times

 **Nava702** 6 months, 3 weeks ago

Selected Answer: A

A look like the least overhead option to capture an API call.

upvoted 2 times

 **Mia2009687** 8 months, 3 weeks ago

Selected Answer: B

The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.

With option C, it won't "The company needs to design an application that captures AWS API calls". it only sends the "CreateImage API" event. We need to store the AWS API calls as well.

upvoted 1 times

 **cookieMr** 9 months ago

EventBridge (formerly CloudWatch Events) is a fully managed event bus service that allows you to monitor and respond to events within your AWS environment. By creating an EventBridge rule specifically for the CreateImage API call, you can easily detect and capture this event. Configuring the target as an SNS topic allows you to send an alert whenever a CreateImage API call occurs. This solution requires minimal operational overhead as EventBridge and SNS are fully managed services.

A. While using an Lambda to query CloudTrail logs and send an alert can achieve the desired outcome, it introduces additional operational overhead compared to using EventBridge and SNS directly.

B. Configuring CloudTrail with an SNS notification and using Athena to query on CreateImage API calls would require more setup and maintenance compared to using EventBridge and SNS.

D. Configuring an SQS FIFO queue as a target for CloudTrail logs and using a function to send an alert to an SNS topic adds unnecessary complexity to the solution and increases operational overhead. Using EventBridge and SNS directly is a simpler and more efficient approach.
upvoted 4 times

 **pisica134** 9 months ago

D makes no sense, FIFO is not required, SQS is not used for sending notifications...C all the way

upvoted 1 times

 **edric1998** 9 months, 1 week ago

Selected Answer: D

As the link shared by who chose C, it said EventBridge can catch event (available/failed/deregistered). In this doc, CreateImage not distinct with CopyImage/RegisterImage/CreateRestoreImageTask.

So It not C.

It not B because it very overhead.

And the question say "whenever", means quick as possible, so It not A.

The right answer is D

upvoted 1 times

 **TheAbsoluteTruth** 11 months, 3 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html#:~:text=For%20example%2C%20you%20can%20create%20an%20EventBridge%20regla%20que%20detecta%20cuando%20el%20creación%20AMI%20proceso%20ha%20completado%20y%20entonces%20invoca%20un%20Amazon%20SNS%20tema%20para%20enviar%20un%20correoelectrónico%20notificación%20para%20usted>

upvoted 1 times

Question #207

Topic 1

A company owns an asynchronous API that is used to ingest user requests and, based on the request type, dispatch requests to the appropriate microservice for processing. The company is using Amazon API Gateway to deploy the API front end, and an AWS Lambda function that invokes Amazon DynamoDB to store user requests before dispatching them to the processing microservices.

The company provisioned as much DynamoDB throughput as its budget allows, but the company is still experiencing availability issues and is losing user requests.

What should a solutions architect do to address this issue without impacting existing users?

- A. Add throttling on the API Gateway with server-side throttling limits.
- B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.
- C. Create a secondary index in DynamoDB for the table with the user requests.
- D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Correct Answer: D

Community vote distribution

D (98%)

👤 **pentium75** Highly Voted 2 months, 4 weeks ago

Selected Answer: D

A does not meet the "without impacting existing users" requirement
 B does not help with writing (DAX caches reads)
 C does not help with writing (index could increase read performance only)
 D decouples writing from front-end, which is acceptable because it is "an asynchronous API" anyway
 upvoted 8 times

👤 **nder** Highly Voted 1 year ago

Selected Answer: D

The key here is "Losing user requests" sqs messages will stay in the queue until it has been processed
 upvoted 7 times

👤 **Guru4Cloud** Most Recent 6 months, 2 weeks ago

Selected Answer: D

This solution can handle bursts of incoming requests more effectively and reduce the chances of losing requests due to DynamoDB capacity limitations. The Lambda can be configured to retrieve messages from the SQS and write them to DynamoDB at a controlled rate, allowing DynamoDB to handle the requests within its provisioned capacity. This approach provides resilience to spikes in traffic and ensures that requests are not lost during periods of high demand.
 upvoted 3 times

👤 **cookieMr** 9 months ago

Selected Answer: D

This solution can handle bursts of incoming requests more effectively and reduce the chances of losing requests due to DynamoDB capacity limitations. The Lambda can be configured to retrieve messages from the SQS and write them to DynamoDB at a controlled rate, allowing DynamoDB to handle the requests within its provisioned capacity. This approach provides resilience to spikes in traffic and ensures that requests are not lost during periods of high demand.

- A. It limits can help control the request rate, but it may lead to an increase in errors and affect the user experience. Throttling alone may not be sufficient to address the availability issues and prevent the loss of requests.
- B. It can improve read performance but does not directly address the availability issues and loss of requests. It focuses on optimizing read operations rather than buffering writes.
- C. It may help with querying the user requests efficiently, but it does not directly solve the availability issues or prevent the loss of requests. It is more focused on data retrieval rather than buffering writes.
 upvoted 3 times

👤 **studynoplay** 10 months, 2 weeks ago

Selected Answer: D

DAX is for reads
 upvoted 3 times

👤 **smartegnine** 9 months, 3 weeks ago

DAX is not ideal for the following types of applications:

Applications that require strongly consistent reads (or that cannot tolerate eventually consistent reads).

Applications that do not require microsecond response times for reads, or that do not need to offload repeated read activity from underlying tables.

Applications that are write-intensive, or that do not perform much read activity.

Applications that are already using a different caching solution with DynamoDB, and are using their own client-side logic for working with that caching solution.

upvoted 2 times

 **dark_firzen** 1 year, 1 month ago

Selected Answer: D

D because SQS is the cheapest way. First 1,000,000 requests are free each month.

Question states: "The company provisioned as much DynamoDB throughput as its budget allows"

upvoted 3 times

 **Wajif** 1 year, 3 months ago

Selected Answer: D

D is more likely to fix this problem as SQS queue has the ability to wait (buffer) for consumer to notify that the request or message has been processed.

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Selected Answer: D

To address the issue of lost user requests and improve the availability of the API, the solutions architect should use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB. Option D (correct answer)

By using an SQS queue and Lambda, the solutions architect can decouple the API front end from the processing microservices and improve the overall scalability and availability of the system. The SQS queue acts as a buffer, allowing the API front end to continue accepting user requests even if the processing microservices are experiencing high workloads or are temporarily unavailable. The Lambda function can then retrieve requests from the SQS queue and write them to DynamoDB, ensuring that all user requests are stored and processed. This approach allows the company to scale the processing microservices independently from the API front end, ensuring that the API remains available to users even during periods of high demand.

upvoted 4 times

 **alect096** 1 year, 3 months ago

Selected Answer: B

I would go to B : <https://aws.amazon.com/es/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>

upvoted 1 times

 **ruqui** 8 months, 3 weeks ago

That's wrong. The document you mentioned explained it very clearly:

"Whereas both read-through and write-through caches address read-heavy workloads, a write-back (or write-behind) cache is designed to address write-heavy workloads. Note that DAX is not a write-back cache currently"

upvoted 2 times

 **BENICE** 1 year, 3 months ago

D is correct answer

upvoted 1 times

 **NikacZ** 1 year, 3 months ago

Selected Answer: D

D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

upvoted 1 times

 **career360guru** 1 year, 3 months ago

Selected Answer: D

Option D is right answer

upvoted 1 times

 **alexfk** 1 year, 3 months ago

Why not B? DAX.

"When you're developing against DAX, instead of pointing your application at the DynamoDB endpoint, you point it at the DAX endpoint, and DAX handles the rest. As a read-through/write-through cache, DAX seamlessly intercepts the API calls that an application normally makes to DynamoDB so that both read and write activity are reflected in the DAX cache."

<https://aws.amazon.com/es/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>

upvoted 1 times

 **ruqui** 8 months, 3 weeks ago

B is wrong because of this:

"Whereas both read-through and write-through caches address read-heavy workloads, a write-back (or write-behind) cache is designed to address write-heavy workloads. Note that DAX is not a write-back cache currently"

upvoted 1 times

 **AgboolaKun** 11 months, 2 weeks ago

It is not DAX because of the company's budget restriction associated with the DynamoDB. This is a requirement in the question. DynamoDB charges for DAX capacity by the hour and your DAX instances run with no long-term commitments. Please refer to:
https://aws.amazon.com/dynamodb/pricing/provisioned/#.E2.80.A2_DynamoDB_Accelerator_.28DAX.29

upvoted 2 times

 **akosigengen** 1 year, 3 months ago

yeah I though the answer is also DAX.

upvoted 1 times

 **leonnnn** 1 year, 3 months ago

Selected Answer: D

Using SQS should be the answer.

upvoted 3 times

 **nVizzz** 1 year, 3 months ago

Why not DAX? Could somebody explain?

upvoted 1 times

 **Rameez1** 1 year, 3 months ago

DAX helps in reducing the read loads from DynamoDB, here we need a solution to handle write requests, which is well handled by SQS and Lamda to buffer writes on DynamoDB.

upvoted 4 times

 **bmofo** 1 year, 3 months ago

key noted issue is "losing user requests" which is resolved with SQS

upvoted 5 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Using DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB, may improve the write performance of the system, but it does not provide the same level of scalability and availability as using an SQS queue and Lambda.

Hence, Option B is incorrect.

upvoted 1 times

 **jambajuice** 1 year, 3 months ago

Selected Answer: D

Answer d

upvoted 2 times

 **Nigma** 1 year, 3 months ago

Answer : D

upvoted 1 times

Question #208

Topic 1

A company needs to move data from an Amazon EC2 instance to an Amazon S3 bucket. The company must ensure that no API calls and no data are routed through public internet routes. Only the EC2 instance can have access to upload data to the S3 bucket.

Which solution will meet these requirements?

- A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
- B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2 instance is located. Attach appropriate security groups to the endpoint. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
- C. Run the nslookup tool from inside the EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
- D. Use the AWS provided, publicly available ip-ranges.json file to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

Correct Answer: B

Community vote distribution



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

Selected Answer: A

I think answer should be A and not B.
as we cannot "Attach a security groups to a gateway endpoint."
upvoted 27 times

✉️ **A_New_Guy** 1 year, 3 months ago

It's possible:

<https://aws.amazon.com/premiumsupport/knowledge-center/connect-s3-vpc-endpoint/>
upvoted 4 times

✉️ **kruasan** 11 months ago

No, it's not

upvoted 3 times

✉️ **smartegnine** 9 months, 3 weeks ago

Create a security group that allows the resources in your VPC to communicate with the endpoint network interfaces for the VPC endpoint. To ensure that tools such as the AWS CLI can make requests over HTTPS from resources in the VPC to the AWS service, the security group must allow inbound HTTPS traffic.

For Security groups, select the security groups to associate with the endpoint network interfaces for the VPC endpoint. By default, we associate the default security group for the VPC.

upvoted 1 times

✉️ **slackbot** 7 months ago

this is valid for interface endpoint, not for gateway endpoint, which option B mentioned
upvoted 2 times

✉️ **markw92** 9 months, 1 week ago

Gateway endpoint must be used as a target in a route table does not use security groups.
upvoted 5 times

✉️ **Iconique** 6 months ago

Go to console and test it yourself! With Interface Endpoint you can add security groups.
upvoted 2 times

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

Selected Answer: B

The correct solution to meet the requirements is Option B. A gateway VPC endpoint for Amazon S3 should be created in the Availability Zone where the EC2 instance is located. This will allow the EC2 instance to access the S3 bucket directly, without routing through the public internet. The

endpoint should also be configured with appropriate security groups to allow access to the S3 bucket. Additionally, a resource policy should be attached to the S3 bucket to only allow the EC2 instance's IAM role for access.

upvoted 27 times

 **Buruguduystunstugudunstuy** 1 year, 3 months ago

Option A is incorrect because an interface VPC endpoint for Amazon S3 would not provide a direct connection between the EC2 instance and the S3 bucket.

Option C is incorrect because using the nslookup tool to obtain the private IP address of the S3 bucket's service API endpoint would not provide a secure connection between the EC2 instance and the S3 bucket.

Option D is incorrect because using the ip-ranges.json file to obtain the private IP address of the S3 bucket's service API endpoint is not a secure method to connect the EC2 instance to the S3 bucket.

upvoted 3 times

 **ChrisG1454** 1 year, 1 month ago

There are two types VPC Endpoint:

Gateway endpoint
Interface endpoint

A Gateway endpoint:

- 1) Helps you to securely connect to Amazon S3 and DynamoDB
- 2) Endpoint serves as a target in your route table for traffic
- 3) Provide access to endpoint (endpoint, identity and resource policies)

An Interface endpoint:

- 1) Help you to securely connect to AWS services EXCEPT FOR Amazon S3 and DynamoDB
- 2) Powered by PrivateLink (keeps network traffic within AWS network)
- 3) Needs a elastic network interface (ENI) (entry point for traffic)

upvoted 28 times

 **slackbot** 7 months ago

interface endpoint exists for S3 as well

upvoted 4 times

 **mhmt4438** 1 year, 2 months ago

An interface VPC endpoint does provide a direct connection between the EC2 instance and the S3 bucket. It enables private communication between instances in your VPC and resources in other services without requiring an internet gateway, a NAT device, or a VPN connection.

Option A , which recommends creating an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located and attaching a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access, is the correct solution for the given scenario. It meets the requirement to ensure that no API calls and no data are routed through public internet routes and that only the EC2 instance can have access to upload data to the S3 bucket.

upvoted 5 times

 **Omok** 1 year, 1 month ago

In support, see <https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>

upvoted 6 times

 **scar0909** Most Recent 2 weeks, 1 day ago

Selected Answer: B

vpc gateway endpoint

upvoted 1 times

 **TheFivePips** 4 weeks ago

Selected Answer: A

I used to think that gatway endpoints were only for s3 and dynamodb, but I guess thats not the whole story. S3 can use interface endpoints, and they are privately routed.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>

upvoted 1 times

 **frmrkc** 1 month, 3 weeks ago

Selected Answer: A

Option B is wrong:

- you cannot attach security groups to gateway VPC endpoint
- you cannot create gateway VPC endpoint in the Availability Zone

upvoted 2 times

 **thewalker** 1 month, 3 weeks ago

Selected Answer: B

The main difference between an interface VPC endpoint and a gateway VPC endpoint is how traffic is routed to AWS services outside the VPC:

Interface VPC Endpoint:

Uses an Elastic Network Interface (ENI) within your VPC subnets to allow communication between your VPC and AWS services.

When you create an interface endpoint, a private IP address is assigned to the ENI that acts as the entry point for traffic destined to the AWS service.

DNS queries for the service are routed to the private IP address of the ENI, avoiding the public internet.

upvoted 1 times

 **thewalker** 1 month, 3 weeks ago

Gateway VPC Endpoint:

Adds an entry in your VPC route table that defines the service as a valid destination and routes traffic to it.

Traffic destined for the service leaves your VPC and travels across the AWS global network to the service.

Gateway endpoints currently only support S3 and DynamoDB. Interface endpoints support many more AWS services.

Some key points to consider when choosing an endpoint type include availability of the service, need for cross-region access, and whether traffic needs to flow from on-premises.

upvoted 2 times

 **Charumathi** 1 month, 3 weeks ago

Selected Answer: A

Interface Endpoints are used for accessing AWS services within the same region over the AWS PrivateLink network, while Gateway Endpoints are used for providing private connectivity to specific AWS services outside your VPC. Each serves a distinct purpose based on the type of service and the desired network architecture.

upvoted 1 times

 **prudhvi08** 1 month, 4 weeks ago

Answer should be B

<https://k21academy.com/amazon-web-services/aws-solutions-architect/aws-gateway-endpoints/>

upvoted 1 times

 **ThongHM** 2 months, 2 weeks ago

Selected Answer: A

I choose A because this phrase "no API calls and no data are routed through PUBLIC INTERNET routes"

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.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/private-link-interface-endpoints.html>

upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

Selected Answer: A

Both A and B are close. I prefer A but B also seems to work as both have configurable security and limit traffic to within AWS network. I don't have a test account now but for Gateway end-point, I suspect that the security group will force you to allow traffic on public IP.

<https://docs.aws.amazon.com/vpc/latest/private-link/gateway-endpoints.html#gateway-endpoint-security>

<https://docs.aws.amazon.com/vpc/latest/private-link/gateway-endpoints.html#gateway-endpoint-security>

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Selected Answer: A

B is wrong because question does NOT ask that no data is "transferred over public Internet", it asks that no data is "routed through public internet routes (!)". Gateway VPC Endpoint uses public IP, thus from VPC perspective the traffic would hit a "public internet route", even if AWS would route the traffic internally.

Besides, you don't create a Gateway VPC endpoint 'in an Availability Zone'.

upvoted 1 times

 **jAtlas7** 3 months ago

Selected Answer: B

Voting B (use gateway endpoint) on the basis that, to enable private connection between VPC and S3, one may either:

option 1: interface VPC endpoint -> AWS PrivateLink -> S3

option 2: gateway VPC endpoint -> S3

i.e. Answer A (interface endpoint) would have been ok if it mentions the use of PrivateLink - unfortunately answer A doesn't mention PrivateLink.

Answer B (interface endpoint) is basically option 1 - and therefore Answer B appears to be best answer.

Ref: <https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/>

upvoted 1 times

 **ale_brd_** 3 months, 1 week ago

Selected Answer: A

Answer is A, Option B is wrong as with Gateway Endpoint you need to set up also the Route Table to use to reach the endpoint resource (S3 or DynamoDB) and not the security groups.

upvoted 1 times

 **osmk** 3 months, 1 week ago

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html#gateway-endpoint-considerations-s3>

The rules for the security groups for your instances that access Amazon S3 through a gateway endpoint must allow traffic to and from Amazon S3. You can reference the ID of the prefix list for Amazon S3 in security group rules.

upvoted 1 times

 **v_rainbow** 3 months, 2 weeks ago

Selected Answer: A

While gateway endpoints also provide private connectivity, they are designed to be used by multiple resources within the VPC. This adds complexity and is not necessary for this scenario where only one EC2 instance needs access.

upvoted 3 times

 **ansagr** 3 months, 2 weeks ago

Selected Answer: A

You cannot attach security groups to VPC gateway endpoints. For VPC gateway endpoints (like S3 or DynamoDB), you typically rely on route tables and IAM policies for access control.

upvoted 1 times

 **MiniYang** 3 months, 3 weeks ago

Selected Answer: A

When you need to ensure that only specific Amazon EC2 instances can access your Amazon S3 bucket, but do not allow data to be routed over the public internet, you can consider the following two key concepts:

VPC Endpoint: VPC endpoints are a way for EC2 instances to privately communicate with AWS services within your virtual private cloud (VPC). For Amazon S3, you can create an interface VPC endpoint, which allows EC2 instances to access S3 directly through a network connection within the VPC instead of going through the public Internet.

IAM roles and S3 access control: You can use AWS Identity and Access Management (IAM) to control EC2 instance access to S3 buckets. You can grant EC2 instances access to S3 by assigning them specific IAM roles. At the same time, you can set a resource policy (Resource Policy) on the S3 bucket to only allow specific IAM roles or specific EC2 instances to access.

upvoted 1 times

Question #209

Topic 1

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.

What should the solutions architect do to ensure that the architecture supports distributed session data management?

- A. Use Amazon ElastiCache to manage and store session data.
- B. Use session affinity (sticky sessions) of the ALB to manage session data.
- C. Use Session Manager from AWS Systems Manager to manage the session.
- D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session.

Correct Answer: A

Community vote distribution

A (100%)

 **Buruguduystunstugudunstuy**  1 year, 3 months ago

Selected Answer: A

The correct answer is A. Use Amazon ElastiCache to manage and store session data.

In order to support distributed session data management in this scenario, it is necessary to use a distributed data store such as Amazon ElastiCache. This will allow the session data to be stored and accessed by multiple EC2 instances across multiple Availability Zones, which is necessary for a scalable and highly available architecture.

Option B, using session affinity (sticky sessions) of the ALB, would not be sufficient because this would only allow the session data to be stored on a single EC2 instance, which would not be able to scale across multiple Availability Zones.

Options C and D, using Session Manager and the GetSessionToken API operation in AWS STS, are not related to session data management and would not be appropriate solutions for this scenario.

upvoted 19 times

 **awsgEEK75**  2 months, 3 weeks ago

Selected Answer: A

A is in scope of question as company is willing to make code changes.

B would have been correct if no code changes were allowed and scaling could be compromised.

C is wrong technology (cloud management)

D is also wrong technology (AWS IAM or account management).

upvoted 1 times

 **Michael_Li** 3 months, 2 weeks ago

A is correct

B is not correct as session affinity allows web users to stick to a specific EC2 instance for a period of time, so if that instance goes down, the session data will be lost.

C is wrong as Session Manager is for admins to manage EC2 CLI access, not for web end users.

D is wrong as GetSessionToken API is for use cases such as granting user access to a S3 bucket with customized code.

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: A

Yap agree with you guys, this is one of the use cases for Amazon ElastiCache.

It was designed to store ephemeral session data to quickly personalize gaming, e-commerce, social media, and online applications with microsecond response times.

<https://aws.amazon.com/elasticsearch/#:~:text=Store,-,ephemeral,-session%20data%20to>

upvoted 1 times

 **Cloud_A** 2 months, 1 week ago

<https://aws.amazon.com/elasticsearch/#:~:text=Store%20ephemeral%20session%20data%20to%20quickly%20personalize%20gaming%2C%20e%2Dcommerce%2C%20social%20media%20and%20online%20applications%20with%20microsecond%20response%20times>

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

The correct answer is A. Use Amazon ElastiCache to manage and store session data.

upvoted 1 times

 **cookieMr** 8 months, 3 weeks ago

Selected Answer: A

ElastiCache is a managed in-memory data store service that is well-suited for managing session data in a distributed architecture. It provides high-performance, scalable, and durable storage for session data, allowing multiple EC2 instances to access and share session data seamlessly. By using ElastiCache, the application can offload the session management workload from the EC2 instances and leverage the distributed caching capabilities of ElastiCache for improved scalability and performance.

Option B, using session affinity (sticky sessions) of the ALB, is not the best choice for distributed session data management because it ties each session to a specific EC2 instance. As the instances scale up and down frequently, it can lead to uneven load distribution and may not provide optimal scalability.

Options C and D are not applicable for managing session data. AWS Systems Manager's Session Manager is primarily used for secure remote shell access to EC2 instances, and the AWS STS GetSessionToken API operation is used for temporary security credentials and not session data management.

upvoted 1 times

 **cookieMr** 9 months ago

ElastiCache is a managed in-memory data store service that is well-suited for managing session data in a distributed architecture. It provides high-performance, scalable, and durable storage for session data, allowing multiple EC2 instances to access and share session data seamlessly. By using ElastiCache, the application can offload the session management workload from the EC2 instances and leverage the distributed caching capabilities of ElastiCache for improved scalability and performance.

Option B, using session affinity (sticky sessions) of the ALB, is not the best choice for distributed session data management because it ties each session to a specific EC2 instance. As the instances scale up and down frequently, it can lead to uneven load distribution and may not provide optimal scalability.

Options C and D are not applicable for managing session data. AWS Systems Manager's Session Manager is primarily used for secure remote shell access to EC2 instances, and the AWS STS GetSessionToken API operation is used for temporary security credentials and not session data management.

upvoted 2 times

 **Abrar2022** 9 months, 1 week ago

Selected Answer: A

A. Use Amazon ElastiCache to manage and store session data.

- Correct. - Session data is managed at the application-layer, and a distributed cache should be used

B. Use session affinity (sticky sessions) of the ALB to manage session data.

- Wrong. This tightly couples the individual EC2 instances to the session data, and requires additional logic in the ALB. When scale-in happens, the session data stored on individual EC2 instances is destroyed

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: A

correct answer is A as instance are getting up and down.

upvoted 1 times

 **inseong** 1 year, 3 months ago

야 근데 210문제는 어딨나 ..?

upvoted 1 times

 **noche** 1 year ago

<https://www.examtopics.com/discussions/amazon/view/94992-exam-aws-certified-solutions-architect-associate-saa-c03/>
여기 임마

upvoted 1 times

 **NikaCZ** 1 year, 3 months ago

Selected Answer: A

Amazon ElastiCache to manage and store session data.

upvoted 1 times

 **k1kavi1** 1 year, 3 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/46412-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **Shasha1** 1 year, 3 months ago

A

Amazon ElastiCache to manage and store session data. This solution will allow the application to automatically scale across multiple Availability Zones without losing session data, as the session data will be stored in a cache that is accessible from any EC2 instance. Additionally, using Amazon ElastiCache will enable the company to easily manage and scale the cache as needed, without requiring any changes to the application code.

Option C is not correct because, Session Manager from AWS Systems Manager will not provide the necessary support for distributed session data management. Session Manager is a tool for managing and tracking sessions on EC2 instances, but it does not provide a mechanism for storing and managing session data in a distributed environment.

upvoted 3 times

 **TelaO** 1 year, 3 months ago

better justification found here...

<https://www.examtopics.com/discussions/amazon/view/46412-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

✉ **kmaneith** 1 year, 3 months ago

why not C?

upvoted 1 times

✉ **leonnnn** 1 year, 3 months ago

Selected Answer: A

ALB sticky session can keep request accessing to the same backend application. But it says "distributed session management" and company "will to change code", so I think A is better

upvoted 3 times

✉ **Nigma** 1 year, 3 months ago

Selected Answer: A

Answer : A

upvoted 1 times

Question #210

Topic 1

A company offers a food delivery service that is growing rapidly. Because of the growth, the company's order processing system is experiencing scaling problems during peak traffic hours. The current architecture includes the following:

- A group of Amazon EC2 instances that run in an Amazon EC2 Auto Scaling group to collect orders from the application
- Another group of EC2 instances that run in an Amazon EC2 Auto Scaling group to fulfill orders

The order collection process occurs quickly, but the order fulfillment process can take longer. Data must not be lost because of a scaling event.

A solutions architect must ensure that the order collection process and the order fulfillment process can both scale properly during peak traffic hours. The solution must optimize utilization of the company's AWS resources.

Which solution meets these requirements?

- Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure each Auto Scaling group's minimum capacity according to peak workload values.
- Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure a CloudWatch alarm to invoke an Amazon Simple Notification Service (Amazon SNS) topic that creates additional Auto Scaling groups on demand.
- Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Scale the Auto Scaling groups based on notifications that the queues send.
- Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Create a metric based on a backlog per instance calculation. Scale the Auto Scaling groups based on this metric.

Correct Answer: C

Community vote distribution



✉️ **TungPham** 1 year ago

Selected Answer: D

When the backlog per instance reaches the target value, a scale-out event will happen. Because the backlog per instance is already 150 messages (1500 messages / 10 instances), your group scales out, and it scales out by five instances to maintain proportion to the target value.

Backlog per instance: To calculate your backlog per instance, start with the ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling group is the number of instances in the InService state, to get the backlog per instance.

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

upvoted 10 times

✉️ **n43u435b543ht2b** 7 months, 2 weeks ago

Selected Answer: D

C is incorrect as scaling based on the number of "notifications" doesn't make logical sense. This means that both the order collection and fulfillment instances would scale in parallel, but they have clearly said that the collection is processing quickly while the fulfillment is struggling. Therefore, we should scale the pool when there is a backlog building in a respective queue - not just based on the number of incoming requests.

upvoted 6 times

✉️ **bujuman** 1 month, 2 weeks ago

Selected Answer: D

D is the most appropriate response base on <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

upvoted 1 times

✉️ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

D. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Create a metric based on a backlog per instance calculation. Scale the Auto Scaling groups based on this metric.

upvoted 4 times

✉️ **argl1995** 9 months ago

SQS auto-scales by default so I don't think we need to mention it explicitly. Option D should be correct.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: D

- A. This approach focuses solely on CPU utilization, which may not accurately reflect the scaling needs of the order collection and fulfillment processes. It does not address the need for decoupling and reliable message processing.
- B. While this approach incorporates alarms to trigger additional Auto Scaling groups, it lacks the decoupling and reliable message processing provided by using SQS queues. It may lead to inefficient scaling and potential data loss.
- C. Although using SQS queues is a step in the right direction, scaling solely based on queue notifications may not provide optimal resource utilization. It does not consider the backlog per instance and does not allow for fine-grained control over scaling.

Overall, option D, which involves using SQS queues for order collection and fulfillment, creating a metric based on backlog per instance calculation, and scaling the Auto Scaling groups accordingly, is the most suitable solution to address the scaling problems while optimizing resource utilization and ensuring reliable message processing.

upvoted 4 times

 **studynoplay** 10 months, 2 weeks ago

Selected Answer: D

C is incorrect. "based on notifications that the queues send" SQS does not send notification

upvoted 3 times

 **mandragon** 10 months, 3 weeks ago

Selected Answer: C

D is not correct because it requires more operational overhead and complexity than option C which is simpler and more cost-effective. It uses the existing queue metrics that are provided by Amazon SQS and does not require creating or publishing any custom metrics. You can use target tracking scaling policies to automatically maintain a desired backlog per instance ratio without having to calculate or monitor it yourself.

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

"You can use target tracking scaling policies" but you don't with option C. What is "scaling based on notifications that the queues send"? Where do they send these notifications to?

upvoted 1 times

 **JayBee65** 1 year, 2 months ago

Selected Answer: D

Scale based on queue length

upvoted 2 times

 **Rudraman** 1 year, 2 months ago

answer is D.

read question again

upvoted 2 times

 **LuckyAro** 1 year, 2 months ago

Selected Answer: D

The number of instances in your Auto Scaling group can be driven by how long it takes to process a message and the acceptable amount of latency (queue delay).

The solution is to use a backlog per instance metric with the target value being the acceptable backlog per instance to maintain.

upvoted 1 times

 **Aseem8888** 1 year, 2 months ago

Selected Answer: D

D is correct

upvoted 1 times

 **Rudraman** 1 year, 2 months ago

C

Need to Auto-

Scale Queue of SQS

upvoted 1 times

 **JayBee65** 1 year, 2 months ago

Why would you scale based on " Scale the Auto Scaling groups based on notifications that the queues send."? Would it not make 1000 times more sense to scale base don queue length "Create a metric based on a backlog per instance calculation"?

upvoted 3 times

 **techhb** 1 year, 2 months ago

Selected Answer: D

I think its D as here we are creating new metric to calculate load on each EC2 instance.

upvoted 2 times

 **techhb** 1 year, 2 months ago

I think its D as here we are creating new metric to calculate load on each EC2 instance.

upvoted 2 times

 **wmp7039** 1 year, 2 months ago

Selected Answer: D

C is incorrect as SQS doesn't send notifications and needs to be polled by the consumers
upvoted 3 times

 **KM01** 1 year, 2 months ago

I think, D
upvoted 1 times

Question #211

Topic 1

A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of “application” and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.

Which solution meets these requirements?

- A. Use AWS CloudTrail to generate a list of resources with the application tag.
- B. Use the AWS CLI to query each service across all Regions to report the tagged components.
- C. Run a query in Amazon CloudWatch Logs Insights to report on the components with the application tag.
- D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag.

Correct Answer: D

Community vote distribution

D (100%)

 **cookieMr**  9 months ago

Selected Answer: D

A is not the quickest solution because CloudTrail primarily focuses on capturing and logging API activity. While it can provide information about resource changes, it may not provide a comprehensive and quick way to identify all the tagged components across multiple services and Regions.

B involves manually querying each service using the AWS CLI, which can be time-consuming and cumbersome, especially when dealing with multiple services and Regions. It is not the most efficient solution for quickly identifying tagged components.

C is focused on analyzing logs rather than directly identifying the tagged components. While CloudWatch Logs Insights can help extract information from logs, it may not provide a straightforward and quick way to gather a consolidated list of all tagged components across different services and Regions.

D is the quickest solution as it leverages the Resource Groups Tag Editor, which is specifically designed for managing and organizing resources based on tags. It offers a centralized and efficient approach to generate a report of tagged components across multiple services and Regions.

upvoted 12 times

 **TariqKipkemei**  6 months, 1 week ago

Selected Answer: D

Tags are key and value pairs that act as metadata for organizing your AWS resources

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag

upvoted 3 times

 **Bmarodi** 10 months ago

Selected Answer: D

A solutions architect can provide the quickest solution for identifying all of the tagged components by running a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag, hence the option D is right answer.

upvoted 2 times

 **Dondozzy** 1 year ago

Selected Answer: D

The answer is D

upvoted 2 times

 **sh0811** 1 year, 1 month ago

Selected Answer: D

D가 맞습니다.

upvoted 2 times

 **Training4aBetterLife** 1 year, 1 month ago

Selected Answer: D

<https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html>

upvoted 3 times

 **Rudraman** 1 year, 2 months ago

Answer is D.

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: D

validated

<https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html>

upvoted 1 times

 **kbaruu** 1 year, 2 months ago

Selected Answer: D

D is correct

upvoted 1 times

 **waiyiu9981** 1 year, 2 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/51352-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Question #212

Topic 1

A company needs to export its database once a day to Amazon S3 for other teams to access. The exported object size varies between 2 GB and 5 GB. The S3 access pattern for the data is variable and changes rapidly. The data must be immediately available and must remain accessible for up to 3 months. The company needs the most cost-effective solution that will not increase retrieval time.

Which S3 storage class should the company use to meet these requirements?

- A. S3 Intelligent-Tiering
- B. S3 Glacier Instant Retrieval
- C. S3 Standard
- D. S3 Standard-Infrequent Access (S3 Standard-IA)

Correct Answer: A*Community vote distribution*

techhb 1 year, 2 months ago

Selected Answer: A

S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the Infrequent Access tier and after 90 days of no access to the Archive Instant Access tier.

upvoted 16 times

Devsin2000 10 months, 3 weeks ago

<https://aws.amazon.com/getting-started/hands-on/getting-started-using-amazon-s3-intelligent-tiering/>

upvoted 5 times

pentium75 2 months, 4 weeks ago

Selected Answer: A

I think it cannot be clearly answered because we know that the 'access pattern is variable and changes rapidly', but ultimately it depends on the total number and volume of accesses. All four options meet the "not increase retrieval time" requirement (even Glacier Instant Retrieval has "the same latency and access time as S3 Standard"). If data would be rarely accessed, B would be cheapest. If it would be constantly accessed, C would be cheapest (we'd pay the Intelligent Tiering fee but it would never move anything to a cheaper tier). Inbetween it would be D.

But I guess the key is Amazon's clear recommendation to use Intelligent Tiering (A) for "unknown or changing access" patterns, which matches the statement in the question.

upvoted 5 times

escalibran 1 week, 6 days ago

Feels like half the scenario or answers are missing. Where's the "remove objects after 90 days"? Intelligent Tiering has an upcharge for the provided convenience - does it even make sense, when objects won't remain long enough to be archived?

Other classes trade storage cost for request costs. Dependent on how often objects are queried, IA might make sense. Even Glacier Instant Retrieval could come out ahead, given minimal access (and it has 90 days minimum storage duration, exact fit for the description).

With no further details provided, this is just throwing darts blindly.

upvoted 1 times

escalibran 1 week, 6 days ago

Given just the uncertain access patterns AND limited storage time, I would argue in favor of simple S3 Standard.

If the question mentioned that the pattern of access varies across objects, but is relatively consistent for the individual objects, intelligent tiering may be worth it. Otherwise you just pay more to have objects monitored for Infrequent Access, and then suddenly become popular after being moved.

upvoted 1 times

MrPCarrot 1 month, 1 week ago

A is the perfect answer - The S3 access pattern for the data is variable and changes rapidly.

upvoted 1 times

bujuman 1 month, 2 weeks ago

Selected Answer: A

With regard to "The S3 access pattern for the data is variable and changes rapidly"

Even though Answer B could fulfill some requirements, Answer A is for long-lived data that have unpredictable access patterns.

upvoted 1 times

theochan 2 months, 1 week ago

Selected Answer: B

"immediately available" =>

D is not immediately, and for cost B < A/C

upvoted 1 times

 **Vladan0** 4 months, 2 weeks ago

Selected Answer: B

<https://aws.amazon.com/s3/storage-classes/glacier/instant-retrieval/>

"Amazon S3 Glacier Instant Retrieval is an archive storage class that delivers the lowest-cost storage for long-lived data that is rarely accessed and requires retrieval in milliseconds"

upvoted 2 times

 **ivan_riqueros12** 5 months, 1 week ago

Selected Answer: A

A. El patrón de acceso a los datos es variable y cambia rápidamente = S3 Intelligent-Tiering

upvoted 1 times

 **Abdou1604** 5 months, 2 weeks ago

very important note , S3 Intelligent-Tiering got no retrival charges

upvoted 3 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: A

access pattern for the data is variable and changes rapidly = S3 Intelligent-Tiering

upvoted 3 times

 **Sultanoid** 6 months, 3 weeks ago

Selected Answer: C

There are 2 viable options A and C.

The Intelligent tearing(A) might put your data in the archive or Infrequent Acces if it is not used for 80 days and then used as crazy for the last 10 days of the period which will cause delays in retrieval or the costs associated with traffic.

Option C can be optimised with the Time To Live policy of 90 days and will be the most efficient and reliable solution to satisfy the needs.

upvoted 4 times

 **pentium75** 2 months, 4 weeks ago

Lifecycle policies apply to all tiers, you can have data deleted or archived after 3 months regardless whether it is in Standard or Intelligent-Tiering.

upvoted 1 times

 **mtnmayer** 7 months, 3 weeks ago

Has to be C. S3 Intelligent-Tiering is for data with varying or unknown access needs. Not the case here. We know data must be highly available for 30 days.

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

Isn't "varying or unknown access needs" the same as "the access pattern is variable and changes rapidly"?

upvoted 2 times

 **maheshudara** 8 months, 3 weeks ago

Selected Answer: A

key - "Changing access patterns"

upvoted 1 times

 **maheshudara** 8 months, 3 weeks ago

"The S3 access pattern for the data is variable and changes rapidly"

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: A

Option A is designed for objects with changing access patterns, but it may not be the most cost-effective solution for long-term storage of the data, especially if the access pattern is variable and changes rapidly.

Option B is optimized for long-term archival storage and may not provide the immediate accessibility required by the company. Retrieving data from Glacier storage typically incurs a longer retrieval time compared to other storage classes.

Option C is the appropriate choice for immediate availability and quick access to the data. It offers high durability, availability, and low latency access, making it suitable for the company's needs. However, it is not the most cost-effective option for long-term storage.

Option D is a more cost-effective storage class compared to S3 Standard, especially for data that is accessed less frequently. However, since the access pattern for the data is variable and changes rapidly, S3 Standard-IA may not be the most cost-effective solution, as it incurs additional retrieval fees for frequent access.

upvoted 3 times

 **markw92** 9 months, 1 week ago

Answer A: S3 Intelligent-Tiering is the recommended storage class for data with unknown, changing, or unpredictable access patterns, independent of object size or retention period, such as data lakes, data analytics, and new applications.

upvoted 1 times

 **AlankarJ** 9 months, 3 weeks ago

The questions specifically says, data should me immediately available. So D can't be true as S3 Infrequent access is for data which is not accessed frequently. Don't forget upto 3 months.

upvoted 2 times

 **ruqui** 10 months ago

Selected Answer: A

Amazon S3 Intelligent-Tiering is the only cloud storage class that delivers automatic storage cost savings when data access patterns change, without performance impact or operational overhead

upvoted 1 times

Question #213

Topic 1

A company is developing a new mobile app. The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection. The company has minimal infrastructure and operational staff. The company needs to reduce its share of the responsibility in managing, updating, and securing servers for its AWS environment.

What should a solutions architect recommend to meet these requirements?

- A. Configure AWS WAF rules and associate them with the ALB.
- B. Deploy the application using Amazon S3 with public hosting enabled.
- C. Deploy AWS Shield Advanced and add the ALB as a protected resource.
- D. Create a new ALB that directs traffic to an Amazon EC2 instance running a third-party firewall, which then passes the traffic to the current ALB.

Correct Answer: A*Community vote distribution*

ShinobiGrappler Highly Voted 1 year, 2 months ago

Selected Answer: C

C --- Read and understand the question. *The company needs to reduce its share of responsibility in managing, updating, and securing servers for its AWS environment* Go with AWS Shield advanced --This is a managed service that includes AWS WAF, custom mitigations, and DDoS insight.
upvoted 18 times

arjundevops 11 months, 1 week ago

Brother answer is A, Read the question once again or ask CHATGPT for more in-depth analysis

upvoted 2 times

rokeus 5 months ago

I agree, both A and C answer the first demand ,where A is answer to the technical request., but for reducing responsibility you will need shield advance - meaning C.

upvoted 2 times

pentium75 2 months, 4 weeks ago

No because this is about application-level attacks which requires WAF aka answer A.

upvoted 2 times

Steve_4542636 1 year ago

You stated, "This is a managed service that includes AWS WAF, custom mitigations, and DDoS insight." and you are correct. However, the service you would actually have to setup to prevent SQL injection attacks is WAF.

upvoted 9 times

darn 11 months, 1 week ago

exactly, that's like saying let's implement Network Firewall Manager to manage WAF, absurd!

upvoted 4 times

Guru4Cloud 6 months, 2 weeks ago

I don't know how this comment gets 11x upvotes.

A. To filter traffic and protect against application attacks like cross-site scripting and SQL injection, the company can use AWS Web Application Firewall with managed rules on the Application Load Balancer. This provides security with minimal infrastructure and operations overhead.

upvoted 12 times

cookieMr Highly Voted 9 months ago

Selected Answer: A

By configuring AWS WAF rules and associating them with the ALB, the company can filter and block malicious traffic before it reaches the application. AWS WAF offers pre-configured rule sets and allows custom rule creation to protect against common vulnerabilities like XSS and SQL injection.

Option B does not provide the necessary security and traffic filtering capabilities to protect against application-level attacks. It is more suitable for hosting static content rather than implementing security measures.

Option C is focused on DDoS protection rather than application-level attacks like XSS or SQL injection. While AWS Shield Advanced does not address the specific requirements mentioned in the scenario.

Option D involves maintaining and securing additional infrastructure, which goes against the requirement of reducing responsibility and relying on minimal operational staff.

upvoted 6 times

✉ bujuman **Most Recent** 1 month, 2 weeks ago

Selected Answer: A

This is confusing "The company needs to reduce its share of the responsibility in managing, updating, and securing servers for its AWS environment." But could be achieved when using WAF and AWS managed Rules.

upvoted 1 times

✉ thewalker 1 month, 3 weeks ago

Selected Answer: A

A is the answer.

upvoted 1 times

✉ farnamjam 2 months ago

Selected Answer: A

AWS Shield Advanced does not directly protect against XSS (cross-site scripting) or SQL injection attacks. It focuses on defending against Distributed Denial of Service (DDoS) attacks, which aim to overwhelm resources and disrupt availability.

upvoted 1 times

✉ awsgeek75 2 months, 3 weeks ago

Selected Answer: A

S makes more sense as Shield Advanced (which actually contains WAF) doesn't provide any additional benefits apart from networks protection. WAF will still have to be configured. So just use WAF to fulfil the requirements.

upvoted 2 times

✉ pentium75 2 months, 4 weeks ago

Selected Answer: A

You need to "configure AWS WAF rules and associate them with the ALB" which is A. AWS Shield Advance INTEGRATES with WAF, so you can manage WAF through Shield Advanced, but still you would need to set it up and configure rules, which C does not mention.

upvoted 4 times

✉ Sadish 3 months, 2 weeks ago

AWS Shield is not only DDoS and it handles Layer 3 and layer 4 including AWS WAF so C should match.

upvoted 1 times

✉ pentium75 2 months, 4 weeks ago

"Shield Advanced provides ... integration (!) with AWS WAF", but you still need WAF. And you need WAF rules, wherever you configure them.

upvoted 1 times

✉ TariqKipkemei 6 months, 1 week ago

Selected Answer: A

AWS WAF helps you protect against common web exploits and bots that can affect availability, compromise security, or consume excessive resources. Protect against vulnerabilities and exploits such as SQL injection or Cross site scripting attacks.

upvoted 5 times

✉ Guru4Cloud 6 months, 2 weeks ago

Selected Answer: A

To filter traffic and protect against application attacks like cross-site scripting and SQL injection, the company can use AWS Web Application Firewall with managed rules on the Application Load Balancer. This provides security with minimal infrastructure and operations overhead.

upvoted 3 times

✉ Undisputed 8 months ago

Selected Answer: A

To achieve proper traffic filtering and protect the Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting (XSS) or SQL injection, while minimizing infrastructure and operational overhead, the company can consider using AWS Web Application Firewall (WAF) with AWS Managed Rules.

upvoted 2 times

✉ vini15 8 months, 1 week ago

A-- Keywords(cross-site scripting or SQL injection)

upvoted 3 times

✉ animefan1 8 months, 3 weeks ago

Selected Answer: A

WAF benefits are rules, SQL injection & XSS protection

upvoted 1 times

✉ sbnpj 8 months, 4 weeks ago

Selected Answer: A

Not C because- AWS Shield Advanced provides DDoS protection, it does not specifically address application-level attacks such as XSS or SQL injection

upvoted 4 times

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

Selected Answer: C

With Shield advanced you get centralized protection management; this allows you to use AWS firewall manager (included in AWS Shield) with policies automatically apply WAF to appliances. Massive sales pitch, see the link: <https://aws.amazon.com/shield/features/>
upvoted 1 times

✉️ **Terry_123** 10 months, 1 week ago

Selected Answer: A

Shield is not aimed to handle SQL injection.

upvoted 1 times

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

Selected Answer: A

WAF = cross-site scripting or SQL injection
Shield/Shield Advanced = DDoS

upvoted 3 times

Question #214

Topic 1

A company's reporting system delivers hundreds of .csv files to an Amazon S3 bucket each day. The company must convert these files to Apache Parquet format and must store the files in a transformed data bucket.

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

- A. Create an Amazon EMR cluster with Apache Spark installed. Write a Spark application to transform the data. Use EMR File System (EMRFS) to write files to the transformed data bucket.
- B. Create an AWS Glue crawler to discover the data. Create an AWS Glue extract, transform, and load (ETL) job to transform the data. Specify the transformed data bucket in the output step.
- C. Use AWS Batch to create a job definition with Bash syntax to transform the data and output the data to the transformed data bucket. Use the job definition to submit a job. Specify an array job as the job type.
- D. Create an AWS Lambda function to transform the data and output the data to the transformed data bucket. Configure an event notification for the S3 bucket. Specify the Lambda function as the destination for the event notification.

Correct Answer: D

Community vote distribution

B (100%)

✉️  Babba  1 year, 2 months ago

Selected Answer: B

It looks like AWS Glue allows fully managed CSV to Parquet conversion jobs: <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>

upvoted 15 times

✉️  awsgeek75 2 months, 3 weeks ago

A text book use case: <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html#three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet-epics>

B is the correct answer.

upvoted 1 times

✉️  cookieMr  9 months ago

Selected Answer: B

AWS Glue is a fully managed ETL service that simplifies the process of preparing and transforming data for analytics. Using AWS Glue requires minimal development effort compared to the other options.

Option A requires more development effort as it involves writing a Spark application to transform the data. It also introduces additional infrastructure management with the EMR cluster.

Option C requires writing and managing custom Bash scripts for data transformation. It requires more manual effort and does not provide the built-in capabilities of AWS Glue for data transformation.

Option D requires developing and managing a custom Lambda for data transformation. While Lambda can handle the transformation, it requires more effort compared to AWS Glue, which is specifically designed for ETL operations.

Therefore, option B provides the easiest and least development effort by leveraging AWS Glue's capabilities for data discovery, transformation, and output to the transformed data bucket.

upvoted 5 times

✉️  Rido4good  2 months, 1 week ago

D

I think people are forgetting the question says "Low Overhead".

upvoted 1 times

✉️  awsgeek75 2 months, 1 week ago

Pray tell, how is a Lambda less overhead than B or even A?

upvoted 2 times

✉️  nileeka97 6 months ago

Selected Answer: B

Parquet format =====> Amazon Glue

upvoted 2 times

✉ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: B

B. Create an AWS Glue crawler to discover the data. Create an AWS Glue extract, transform, and load (ETL) job to transform the data. Specify the transformed data bucket in the output step.

upvoted 2 times

✉ **markw92** 9 months, 1 week ago

Least development effort means lambda. Glue also works but more overhead and cost. A simple lambda like this <https://github.com/ayshaysha/aws-csv-to-parquet-converter/blob/main/csv-parquet-converter.py> can be used to convert as soon as you see files in s3 bucket.

upvoted 3 times

✉ **achevez85** 1 year ago

Selected Answer: B

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-job-types-for-converting-data-to-apache-parquet.html>

upvoted 2 times

✉ **Training4aBetterLife** 1 year, 2 months ago

Selected Answer: B

S3 provides a single control to automatically encrypt all new objects in a bucket with SSE-S3 or SSE-KMS. Unfortunately, these controls only affect new objects. If your bucket already contains millions of unencrypted objects, then turning on automatic encryption does not make your bucket secure as the unencrypted objects remain.

For S3 buckets with a large number of objects (millions to billions), use Amazon S3 Inventory to get a list of the unencrypted objects, and Amazon S3 Batch Operations to encrypt the large number of old, unencrypted files.

upvoted 2 times

✉ **Training4aBetterLife** 1 year, 2 months ago

Please delete this. I was meaning to place this response on a different question.

upvoted 1 times

✉ **Training4aBetterLife** 1 year, 2 months ago

Versioning:

When you overwrite an S3 object, it results in a new object version in the bucket. However, this will not remove the old unencrypted versions of the object. If you do not delete the old version of your newly encrypted objects, you will be charged for the storage of both versions of the objects.

S3 Lifecycle

If you want to remove these unencrypted versions, use S3 Lifecycle to expire previous versions of objects. When you add a Lifecycle configuration to a bucket, the configuration rules apply to both existing objects and objects added later. C is missing this step, which I believe is what makes B the better choice. B includes the functionality of encrypting the old unencrypted objects via Batch Operations, whereas, Versioning does not address the old unencrypted objects.

upvoted 1 times

✉ **Training4aBetterLife** 1 year, 2 months ago

Please delete this. I was meaning to place this response on a different question.

upvoted 2 times

✉ **Rudraman** 1 year, 2 months ago

ETL = Glue

upvoted 3 times

✉ **Aninina** 1 year, 2 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

✉ **techhb** 1 year, 2 months ago

Selected Answer: B

AWS Glue Crawler is for ETL

upvoted 1 times

✉ **kbaruu** 1 year, 2 months ago

Selected Answer: B

The correct answer is B

upvoted 1 times

✉ **Mamioholo** 1 year, 2 months ago

B is the answer

upvoted 2 times

✉ **swolfgang** 1 year, 2 months ago

Selected Answer: B

it should be b
upvoted 1 times

 **marcioicebr** 1 year, 2 months ago

Selected Answer: B

De acordo com a documentação, a resposta certa é B.

https://docs.aws.amazon.com/pt_br/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html

upvoted 1 times

 **AHUI** 1 year, 2 months ago

B is the ans
upvoted 1 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: B

Answer is B
upvoted 1 times

Question #215

Topic 1

A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data need to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migration must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.

What should a solutions architect do to migrate and store the data at the LOWEST cost?

- A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
- B. Deploy a VPN connection between the data center and Amazon VPC. Use the AWS CLI to copy the data from on premises to Amazon S3 Glacier.
- C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
- D. Use AWS DataSync to transfer the data and deploy a DataSync agent on premises. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

Correct Answer: A

Community vote distribution

A (100%)

 **voccer**  8 months, 2 weeks ago

Selected Answer: A

hundreds of Terabytes => always use Snowball
upvoted 7 times

 **TariqKipkemei**  6 months, 1 week ago

Selected Answer: A

Terabytes, low costs, limited time = AWS snowball devices
upvoted 6 times

 **awsgeek75**  2 months, 3 weeks ago

It took me quite some time to do the mental math for realising that the data can't be transferred in 30 days. Also, note the MBps (Megabits) and not Megabytes. 500Mbps is like 60MBps. That's a lame connection to transfer anything!

upvoted 3 times

 **pentium75** 2 months, 4 weeks ago

Selected Answer: A

B and D would use existing 500 mbps Internet connection which cannot transfer more than ca. 160 TB in a month. C would cost a lot, take weeks to deliver, and still not provide more bandwidth. Thus A is the simply the only option, thus also the one with "lowest cost".

upvoted 2 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
upvoted 1 times

 **gosai90786** 8 months, 4 weeks ago

one DataSync agent can use 10GBps and can setup a bandwidth.

So total time = $(700 \times 1000) \text{GB} / 10 \text{GBps} = 70000 \text{ sec} = 19.4 \text{ days}$.

Using Multiple Snowball devices will involve ordering them from AWS, setting them up on your data-center for copy and then incurring the shipping cost for too and fro movement to your AWS cloud.

if time constraint was critical , say 1 week then snowball would have been a viable option. But here we have 30 days, so DataSync will be less costly(takes ~19days)

upvoted 2 times

 **slackbot** 7 months ago

your math is wrong mate, and they have 0.5Gbps connection, not 10GBps

500Mbps = roughly 60MBps

30x24x3600x0.06TB = roughly 155TB

this is way short of 700TB

upvoted 4 times

 **cookieMr** 9 months ago

Selected Answer: A

By ordering Snowball devices, the company can transfer the 700 TB of backup data from its data center to AWS. Once the data is transferred to S3, a lifecycle policy can be applied to automatically transition the files from the S3 Standard storage class to the cost-effective Amazon S3 Glacier Deep Archive storage class.

Option B would require continuous data transfer over the public internet, which could be time-consuming and costly given the large amount of data. It may also require significant bandwidth allocation.

Option C would involve additional costs for provisioning and maintaining the dedicated connection, which may not be necessary for a one-time data migration.

Option D could be a viable option, but it may incur additional costs for deploying and managing the DataSync agent.

Therefore, option A is the recommended choice as it provides a secure and efficient data transfer method using Snowball devices and allows for cost optimization through lifecycle policies by transitioning the data to S3 Glacier Deep Archive for long-term storage.

upvoted 2 times

 **arjundevops** 11 months, 1 week ago

A is the correct answer.

even though they have 500mbps internetspeed, it will take around 130days to transfer the data from on premises to AWS

so they have only 1 option which is Snowball devices

upvoted 2 times

 **Paras043** 11 months, 3 weeks ago

Selected Answer: A

A is the correct one

upvoted 1 times

 **CapJackSparrow** 1 year ago

Q: What is AWS Snowball Edge?

AWS Snowball Edge is an edge computing and data transfer device provided by the AWS Snowball service. It has on-board storage and compute power that provides select AWS services for use in edge locations. Snowball Edge comes in two options, Storage Optimized and Compute Optimized, to support local data processing and collection in disconnected environments such as ships, windmills, and remote factories. Learn more about its features here.

Q: What happened with the original 50 TB and 80 TB AWS Snowball devices?

The original Snowball devices were transitioned out of service and Snowball Edge Storage Optimized are now the primary devices used for data transfer.

Q: Can I still order the original Snowball 50 TB and 80 TB devices?

No. For data transfer needs now, please select the Snowball Edge Storage Optimized devices.

upvoted 1 times

 **vherman** 1 year ago

Selected Answer: A

Snowball

upvoted 1 times

 **KZM** 1 year, 1 month ago

9 Snowball devices are needed to migrate the 700TB of data.

upvoted 2 times

 **KZM** 1 year, 1 month ago

700TB of Data can not be transferred through a 500Mbps link within one month.

Total data that can be transferred in one month = bandwidth x time

= (500 Mbps / 8 bits per byte) x (30 days x 24 hours x 3600 seconds per hour)

= 648,000 GB or 648 TB

This is calculated theoretically with the maximum available situation. Due to a number of factors, the actual total transferred Data may be less than 645 TB.

upvoted 3 times

 **mandragon** 10 months, 3 weeks ago

Good thinking. Agree with the solution. Only the calculation is wrong. It should give 162tb as a result

upvoted 3 times

 **Rudraman** 1 year, 2 months ago

Snow ball Devices the answe is AAAA.

upvoted 2 times

 **wmp7039** 1 year, 2 months ago

A is incorrect as DC is an expensive option. Correct answer should be C as the company already has 500Mbps that can be used for data transfer. By consuming all the available internet bandwidth, data transfer will complete in 3 hours 6 mins - <https://www.omnicalculator.com/other/data-transfer>

upvoted 1 times

✉ **wmp7039** 1 year, 2 months ago

Ignore please, miscalculated time to transfer, it will take 129 days and will breach the 1 month requirement. A is correct.

upvoted 5 times

✉ **kbaruu** 1 year, 2 months ago

Selected Answer: A

A is correct

upvoted 1 times

✉ **swolfgang** 1 year, 2 months ago

a is correct but not less expensive.I think,should be D.

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

Does not work in a month

upvoted 1 times

✉ **Parsons** 1 year, 2 months ago

Selected Answer: A

A is correct.

Cannot copy files directly from on-prem to S3 Glacier with DataSync. It should be S3 standard first, then configuration S3 Lifecycle to transit to Glacier => Exclude D.

upvoted 1 times

✉ **PDR** 1 year, 1 month ago

yes you can - <https://docs.aws.amazon.com/datasync/latest/userguide/create-s3-location.html#using-storage-classes>

upvoted 1 times

Question #216

Topic 1

A company has a serverless website with millions of objects in an Amazon S3 bucket. The company uses the S3 bucket as the origin for an Amazon CloudFront distribution. The company did not set encryption on the S3 bucket before the objects were loaded. A solutions architect needs to enable encryption for all existing objects and for all objects that are added to the S3 bucket in the future.

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

- A. Create a new S3 bucket. Turn on the default encryption settings for the new S3 bucket. Download all existing objects to temporary local storage. Upload the objects to the new S3 bucket.
- B. Turn on the default encryption settings for the S3 bucket. Use the S3 Inventory feature to create a .csv file that lists the unencrypted objects. Run an S3 Batch Operations job that uses the copy command to encrypt those objects.
- C. Create a new encryption key by using AWS Key Management Service (AWS KMS). Change the settings on the S3 bucket to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Turn on versioning for the S3 bucket.
- D. Navigate to Amazon S3 in the AWS Management Console. Browse the S3 bucket's objects. Sort by the encryption field. Select each unencrypted object. Use the Modify button to apply default encryption settings to every unencrypted object in the S3 bucket.

Correct Answer: B

Community vote distribution



✉️ Parsons 1 year, 2 months ago

Selected Answer: B

Step 1: S3 inventory to get object list
Step 2 (If needed): Use S3 Select to filter
Step 3: S3 object operations to encrypt the unencrypted objects.

On the going object use default encryption.

upvoted 12 times

✉️ Parsons 1 year, 2 months ago

Useful ref link: <https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>
upvoted 9 times

✉️ cookieMr 9 months ago

Selected Answer: B

By enabling default encryption settings on the S3, all newly added objects will be automatically encrypted. To encrypt the existing objects, the S3 Inventory feature can be used to generate a list of unencrypted objects. Then, an S3 Batch Operations job can be executed to copy those objects while applying encryption.

A. This solution involves creating a new S3 and manually downloading and uploading all existing objects. It requires significant effort and time to transfer millions of objects, making it a less efficient solution.

C. While enabling SSE with AWS KMS is a valid approach to encrypt objects in an S3, it does not address the requirement of encrypting existing objects. It only applies encryption to new objects added to the bucket.

D. Manually modifying each object in the S3 to apply default encryption settings is a labor-intensive and error-prone process. It would require individually selecting and modifying each unencrypted object, which is impractical for a large number of objects.

upvoted 8 times

✉️ pentium75 2 months, 4 weeks ago

Selected Answer: B

A - Extreme amount of effort
B - Should work
C - SSE-KMS is not "least amount of effort" compared to SSE-S3; Turning versioning is not required to achieve the result but on the contrary, it will cause the non-encrypted files to remain as old versions even if you encrypt them in the future.
D - Even more effort as A

upvoted 1 times

✉️ foha2012 2 months ago

.csv for millions of objects ?? C looks simpler.
upvoted 1 times

✉️ foha2012 2 months ago

B doesnt look like least amount of effort

upvoted 1 times

 **CapJackSparrow** 1 year ago

Selected Answer: B

B...

<https://catalog.us-east-1.prod.workshops.aws/workshops/05f16f1a-0bbf-45a7-a304-4fc7fca3d1f/en-US/s3-track/module-2>

You're welcome

upvoted 3 times

 **bdp123** 1 year, 1 month ago

Selected Answer: B

Amazon S3 now configures default encryption on all existing unencrypted buckets to apply server-side encryption with S3 managed keys (SSE-S3) as the base level of encryption for new objects uploaded to these buckets. Objects that are already in an existing unencrypted bucket won't be automatically encrypted.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-encryption-faq.html>

upvoted 3 times

 **Yelizaveta** 1 year, 1 month ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-copy-example-bucket-key.html>

upvoted 1 times

 **akashkumar1999** 1 year, 1 month ago

Selected Answer: B

B is the correct answer

upvoted 1 times

 **Val182** 1 year, 1 month ago

Selected Answer: B

B 100%

<https://spin.atomicobject.com/2020/09/15/aws-s3-encrypt-existing-objects/>

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: A

Why is no one discussing A ? I think A can also achieve the required results. B is the most appropriate answer though.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Downloading and uploading "millions of objects" is surely not "least amount of effort", thus does not meet the requirements.

upvoted 1 times

 **Training4aBetterLife** 1 year, 2 months ago

Selected Answer: B

S3 provides a single control to automatically encrypt all new objects in a bucket with SSE-S3 or SSE-KMS. Unfortunately, these controls only affect new objects. If your bucket already contains millions of unencrypted objects, then turning on automatic encryption does not make your bucket secure as the unencrypted objects remain.

For S3 buckets with a large number of objects (millions to billions), use Amazon S3 Inventory to get a list of the unencrypted objects, and Amazon S3 Batch Operations to encrypt the large number of old, unencrypted files.

upvoted 3 times

 **Training4aBetterLife** 1 year, 2 months ago

Versioning:

When you overwrite an S3 object, it results in a new object version in the bucket. However, this will not remove the old unencrypted versions of the object. If you do not delete the old version of your newly encrypted objects, you will be charged for the storage of both versions of the objects.

S3 Lifecycle

If you want to remove these unencrypted versions, use S3 Lifecycle to expire previous versions of objects. When you add a Lifecycle configuration to a bucket, the configuration rules apply to both existing objects and objects added later. C is missing this step, which I believe is what makes B the better choice. B includes the functionality of encrypting the old unencrypted objects via Batch Operations, whereas, Versioning does not address the old unencrypted objects.

upvoted 1 times

 **Training4aBetterLife** 1 year, 2 months ago

S3 provides a single control to automatically encrypt all new objects in a bucket with SSE-S3 or SSE-KMS. Unfortunately, these controls only affect new objects. If your bucket already contains millions of unencrypted objects, then turning on automatic encryption does not make your bucket secure as the unencrypted objects remain.

For S3 buckets with a large number of objects (millions to billions), use Amazon S3 Inventory to get a list of the unencrypted objects, and Amazon S3 Batch Operations to encrypt the large number of old, unencrypted files.

upvoted 1 times

 **Training4aBetterLife** 1 year, 2 months ago

Versioning:

When you overwrite an S3 object, it results in a new object version in the bucket. However, this will not remove the old unencrypted versions of the object. If you do not delete the old version of your newly encrypted objects, you will be charged for the storage of both versions of the objects.

S3 Lifecycle

If you want to remove these unencrypted versions, use S3 Lifecycle to expire previous versions of objects. When you add a Lifecycle configuration to a bucket, the configuration rules apply to both existing objects and objects added later. C is missing this step, which I believe is what makes B the better choice. B includes the functionality of encrypting the old unencrypted objects via Batch Operations, whereas, Versioning does not address the old unencrypted objects.

upvoted 1 times

 **Training4aBetterLife** 1 year, 2 months ago

Please remove duplicate response as I was meaning to submit a voting comment.

upvoted 1 times

 **John_Zhuang** 1 year, 2 months ago

Selected Answer: B

C is wrong. Even though you turn on the SSE-KMS with a new key, the existing objects are still yet to be encrypted. They still need to be manually encrypted by AWS batch

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

And as in C you "turn on versioning", the old, unencrypted objects will be kept.

upvoted 1 times

 **LuckyAro** 1 year, 2 months ago

Selected Answer: B

<https://spin.atomicobject.com/2020/09/15/aws-s3-encrypt-existing-objects/>

upvoted 1 times

 **Aninina** 1 year, 2 months ago

Selected Answer: C

C is the answer

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Why? This does not include a step to encrypt existing objects, and by turning on versioning you will keep the unencrypted versions forever.

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: B

Agree with Parsons

upvoted 1 times

 **Lilibell** 1 year, 2 months ago

the answer is C

also, the questions require future encryption of the objects is the S3 bucket = VERSIONING

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Huh? "future encryption of objects = versioning"???????

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Actually it's the opposite. Versioning will keep the unencrypted objects as previous versions, even if you encrypt them.

upvoted 1 times

 **swolfgang** 1 year, 2 months ago

Selected Answer: C

could not open default encrypton for exist bucket,so need to use KMS

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

SSE-KMS is never "least amount of effort"

upvoted 1 times

Question #217

Topic 1

A company runs a global web application on Amazon EC2 instances behind an Application Load Balancer. The application stores data in Amazon Aurora. The company needs to create a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss. The solution does not need to handle the load when the primary infrastructure is healthy.

What should a solutions architect do to meet these requirements?

- A. Deploy the application with the required infrastructure elements in place. Use Amazon Route 53 to configure active-passive failover. Create an Aurora Replica in a second AWS Region.
- B. Host a scaled-down deployment of the application in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora Replica in the second Region.
- C. Replicate the primary infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora database that is restored from the latest snapshot.
- D. Back up data with AWS Backup. Use the backup to create the required infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-passive failover. Create an Aurora second primary instance in the second Region.

Correct Answer: D

Community vote distribution

A (69%)

D (31%)

✉️  Parsons  1 year, 2 months ago

Selected Answer: A

A is correct.

- "The solution does not need to handle the load when the primary infrastructure is healthy." => Should use Route 53 Active-Passive ==> Exclude B, C
- D is incorrect because "Create an Aurora second primary instance in the second Region.", we need to create an Aurora Replica enough. upvoted 24 times

✉️  Parsons 1 year, 2 months ago

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

upvoted 5 times

✉️  diabloexodia  8 months, 1 week ago

Selected Answer: A

Anything that is not instant recovery is active - passive.

In active -passive we have :

1. Aws Backup(least op overhead) - RTO/RPO = hours
2. Pilot Light (Basic Infra is already deployed, but needs to be fully implemented) -RTO/RPO = 10's of minutes.
3. Warm Standby- (Basic infra + runs small loads (might need to add auto scaling) -RTO/RPO= minutes
4. (ACTIVE -ACTIVE) : Multi AZ option : instant

here we can tolerate 30 mins

hence B,D are incorrect. AWS backup is in hours, hence D is incorrect .

therefore A

upvoted 15 times

✉️  pentium75 2 months, 2 weeks ago

A does not create the infrastructure in the DR region though.

upvoted 1 times

✉️  MrPCarrot  1 month, 1 week ago

A is perfect - Active-Passive Failover: Use this failover configuration when you want a primary group of resources to be available the majority of the time and you want a secondary group of resources to be on standby in case all of the primary resources become unavailable.

upvoted 1 times

✉️  MrPCarrot 1 month, 1 week ago

A is perfect

upvoted 1 times

✉️  farnamjam 2 months ago

Selected Answer: A

Here's why the other options aren't as suitable:

- B. Active-active failover: Incur higher costs due to running both infrastructures simultaneously and introduces complexity in managing traffic

distribution.

C. Restoring from snapshot: Could take longer than 30 minutes to recover, exceeding the company's downtime tolerance.

D. AWS Backup: Dependent on backup and restore times, potentially exceeding the 30-minute recovery window.

upvoted 1 times

 **pentium75** 2 months, 2 weeks ago

Selected Answer: D

Not A - does not mention a second region for the infrastructure elements. Also, you cannot really "create an Aurora Replica in a second AWS Region", replicas must be in same region unless using Aurora Global Database (which is not mentioned)

Not B - would send half of the traffic to the DR region

Not C - this could send traffic to the DR instance even when the primary instance is healthy

D - the wording "Aurora second primary instance" is a bit strange, but still a "primary instance" is what we would need in the other region. We would still need to establish replication between the databases (like binlog), or restore a snapshot before failover, but in general this option could meet the 30 minute RTO/RPO requirement.

upvoted 4 times

 **awsgeek75** 2 months, 3 weeks ago

Selected Answer: D

I agreed with D as the requirements of 30 min downtime and potential data loss and no load consideration when primary instance is healthy. It makes D more feasible than A. Aurora-Replica is normally used for active-active failovers. Be frugal!

upvoted 3 times

 **Jeffab** 5 months ago

If this is the quality of the questions in exam, then we are all screwed! I don't think any options are correct. A probably the most correct, but a big flaw. "Deploy the application with the required infrastructure elements in place." Deploy to where? Fair enough if you assume another region/AZ, but it's not stated and only Aurora replica is mentioned, not the Web/app servers etc.

upvoted 9 times

 **awsgeek75** 2 months, 1 week ago

I really hope the language is better in the exams. Option A is like "do what it takes to make the solution work".... well then by default it is right until the second part makes it wrong. smh!

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: A

'Can tolerate up to 30 minutes of downtime and potential data loss' rules out any option with 'active-active'. Leaves D and A. D is convoluted. Leaving A.

upvoted 5 times

 **cookieMr** 9 months ago

Selected Answer: A

A. involves deploying the application and infrastructure elements in the primary Region. An Aurora Replica is created in a second Region to serve as the standby database. Route 53 is configured with active-passive failover, directing traffic to the primary Region by default. In the event of a disaster, Route 53 can automatically redirect traffic to the standby Region, minimizing downtime. Data loss may occur up to the point of the last replication to the standby Region, which can be within the defined tolerance of 30 minutes.

Option B, is not necessary in this case as the solution does not need to handle the load when the primary infrastructure is healthy, and it may involve higher complexity and costs.

Option C, may introduce additional complexity and potential data loss, as the standby database might not be up-to-date with the primary database.

Option D, may be suitable for backup and recovery scenarios but may not provide the required failover and downtime tolerance specified in the requirements.

upvoted 2 times

 **antropaws** 9 months, 3 weeks ago

Selected Answer: D

I vote D, because option A is not highly available. In option A, you can't configure active-passive failover because you haven't created a backup infrastructure.

upvoted 2 times

 **kraken21** 12 months ago

Selected Answer: A

It is a cross region DR strategy. You need a read replica and Application in another region to have a realistic DR option. The read replica will take few minutes to promote/Active and the application is available. Option D lacks clarity on application and Backups can take time to restore.

upvoted 2 times

 **Yelizaveta** 1 year, 1 month ago

Selected Answer: A

Depending on the Regions involved and the amount of data to be copied, a cross-Region snapshot copy can take hours to complete and will be a factor to consider for the RPO requirements. You need to take this into account when you estimate the RPO of this DR strategy.

If you have strict RTO and RPO requirements, you should consider a different DR strategy, such as Amazon Aurora Global Database .
<https://aws.amazon.com/blogs/database/cost-effective-disaster-recovery-for-amazon-aurora-databases-using-aws-backup/>

upvoted 1 times

✉  **JiyuKim** 1 year, 1 month ago

Selected Answer: D

The solution does not need to handle the load when the primary infrastructure is healthy. -> Amazon Route 53 active-passive failover -> A,D
The company can tolerate up to 30 minutes of downtime and potential data loss -> backup -> D
you don't have to use read replicas if you can tolerate downtime and data loss.

upvoted 4 times

✉  **ChrisG1454** 1 year, 1 month ago

Consider Answer B.

It is suggesting a Pilot Light DR strategy.

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

upvoted 2 times

✉  **Bofi** 1 year ago

I will Vote B and i initially thought it Pilot Light however after 2nd read, it seem it more like warm standby. Option D looks more like back up and Restore strategy and it will take more than 30 minutes to get it done. C is wrong, snapshot takes longer time to restore

upvoted 1 times

✉  **ChrisG1454** 1 year ago

The key sentence is

"a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss"

Take a look at the visualization in the URL provided. Pilot light = 30 minutes.

upvoted 2 times

✉  **aakashkumar1999** 1 year, 1 month ago

Selected Answer: D

I am confused within A and D but I think D is the answer because this seems to be a cost related problem, a replica is kind of a standby and you can promote to be the main db anytime without any much downtime, but here it says it can withstand 30 mins of downtime so we can just keep a backup of the instance and then create a DB whenever required from the backup, hence less cost

upvoted 10 times

✉  **Aninina** 1 year, 2 months ago

Selected Answer: A

A is correct

upvoted 1 times

✉  **gunmin** 1 year, 2 months ago

Selected Answer: A

aaaaaaaaaa

upvoted 1 times

Question #218

Topic 1

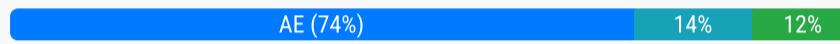
A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address. The default security group is assigned to the EC2 instance. The default network ACL has been modified to block all traffic. A solutions architect needs to make the web server accessible from everywhere on port 443.

Which combination of steps will accomplish this task? (Choose two.)

- A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
- B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.
- C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.
- D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
- E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

Correct Answer: AE

Community vote distribution



✉️ **Parsons** Highly Voted 1 year, 2 months ago

Selected Answer: AE

A, E is perfect the combination. To be more precise, We should add outbound with "outbound TCP port 32768-65535 to destination 0.0.0.0/0." as an ephemeral port due to the stateless of NACL.

upvoted 13 times

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

What is the main reason that you are using the TCP port 32768-65535> In the question, it doesn't ask you any requirement about it.

upvoted 4 times

✉️ **MohammadTofic8787** 6 months, 1 week ago

i Think AD because acl is stateless we must open the port outbound and inbound , in option c we only open 443 on inbound
upvoted 1 times

✉️ **MohammadTofic8787** 6 months, 1 week ago

i Think AD because acl is stateless we must open the port outbound and inbound , in option E we only open 443 on inbound
upvoted 3 times

✉️ **pentium75** Highly Voted 2 months, 4 weeks ago

Selected Answer: E

For me it's grammatically unclear whether "port 443" and "port 32768-65535" in answers D and E are referring to the source or destination ports of the outbound traffic. If source ports then it would be D. If destination ports (which seems more likely) then it's E.

"On Windows, the ephemeral port range is usually from 49152 to 65535.

On Linux, it is often from 32768 to 61000."

Thus 32768-65535 would cover both Windows and Linux.

upvoted 6 times

✉️ **sidharthwader** Most Recent 2 weeks, 3 days ago

AE

Security group is a stateful resource and can understand to allow traffic from source 0.0.0.0/0 with port 443 but ACL is stateless so traffic that is allowed inside the network we must configure the same to go outside the network as well.

upvoted 1 times

✉️ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: AE

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-basics>

"NACLs are stateless, which means that information about previously sent or received traffic is not saved. If, for example, you create a NACL rule to allow specific inbound traffic to a subnet, responses to that traffic are not automatically allowed. This is in contrast to how security groups work. Security groups are stateful, which means that information about previously sent or received traffic is saved. If, for example, a security group allows inbound traffic to an EC2 instance, responses are automatically allowed regardless of outbound security group rules."

A fulfills the security group requirement

E is the only option that explicitly covers outbound traffic and ports.

D covers outbound destination but given that all traffic is blocked (as per the question) this won't work

upvoted 2 times

 [Removed] 4 months, 1 week ago

Selected Answer: AC

For typical web server scenarios, such as serving content over HTTPS (port 443), you generally do not need to explicitly open outbound ports in the network ACL (NACL) for the return traffic.

upvoted 1 times

 pentium75 2 months, 4 weeks ago

But NACLs are stateless."The default network ACL has been modified to block all traffic"; if you don't allow any outbound traffic then the web server won't be able to reply to clients.

upvoted 2 times

 TariqKipkemei 6 months, 1 week ago

Selected Answer: AE

ACL is stateless. you have to define both inbound and outbound rules.

upvoted 2 times

 MohammadTofic8787 6 months, 1 week ago

i Think AD because acl is stateless we must open the port outbound and inbound , in option c we only open 443 on inbound

upvoted 2 times

 MohammadTofic8787 6 months, 1 week ago

i Think AD because acl is stateless we must open the port outbound and inbound , in option D we only open 443 on inbound

upvoted 1 times

 MohammadTofic8787 6 months, 1 week ago

please admin delete this , sorry

upvoted 1 times

 MohammadTofic8787 6 months, 1 week ago

please admin delete this , sorry

upvoted 1 times

 Guru4Cloud 6 months, 2 weeks ago

Selected Answer: AE

A, E is perfect the combination. To be more precise, We should add outbound with "outbound TCP port 32768-65535 to destination 0.0.0.0/0." as an ephemeral port due to the stateless of NACL.

upvoted 3 times

 beginnercloud 7 months ago

Selected Answer: AE

AE is the best answer here, but in reality, E is not good enough. Here, it says that the client chooses the ephemeral port, and it can start from 1024. Only Linux clients have the range starting at 32768 <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports> Unless the destination advertises the ephemeral ports, which I don't think is the case

upvoted 1 times

 pentium75 2 months, 4 weeks ago

"On Windows, the ephemeral port range is usually from 49152 to 65535.

On Linux, it is often from 32768 to 61000."

Combined: 32768 - 65535 ...

upvoted 2 times

 Thornessen 8 months, 1 week ago

Selected Answer: AE

AE is the best answer here, but in reality, E is not good enough.

Here, it says that the client chooses the ephemeral port, and it can start from 1024. Only Linux clients have the range starting at 32768 <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports>

Unless the destination advertises the ephemeral ports, which I don't think is the case

upvoted 2 times

 Abrar2022 9 months, 4 weeks ago

32768-65535 ports Allows outbound IPv4 responses to clients on the internet (for example, serving webpages to people visiting the web servers in the subnet).

upvoted 1 times

 WherecanIstart 1 year ago

Selected Answer: AE

NACL blocks outgoing traffic since it is infact stateless..Option E allows outbound traffic from ephemeral ports going outside of the VPC back to the web.

upvoted 2 times

 Brak 1 year ago

It can't be C, since the current NACL blocks all traffic, including outbound. Need to allow outbound traffic through the NACL.
But E is a bad answer, since ephemeral ports start at 1024, not 32768.

upvoted 2 times

 **neosis91** 1 year, 1 month ago

Selected Answer: AC

A and C not E

Option E states to allow incoming TCP ports on 443 and outgoing on 32768-65535 to all IP addresses (0.0.0.0/0). This option only allows outgoing ports and does not guarantee that incoming connections on 443 will be allowed. It does not meet the requirement of making the web server accessible on port 443 from anywhere. Therefore, option C which states to allow incoming TCP ports on 443 from all IP addresses is the best answer to meet the requirements.

upvoted 4 times

 **Deepak_k** 1 year, 1 month ago

Answer : AE - Incoming traffic on port 443 but sever can use any port to reply back.

upvoted 2 times

 **JoeGuan** 7 months, 1 week ago

It seems there are lots of questions that ask for minimum requirements, and often times adding 'things' to the solution are not correct. I am not sure about this question and I would pick C. E adds ambiguity. What if you only needed to open ports for Lambda? That would be a different set of ports. I think E adds some assumptions into the question. I think opening some ports for some assumptions and keeping ports closed for other assumptions is not correct. The best assumption is to assume they are asking how to open ports for 443

upvoted 1 times

 **slackbot** 7 months ago

E still guarantees something will work. C definitely means - nothing will work, because you are not allowing egress traffic at all

upvoted 2 times

 **slackbot** 7 months ago

seems like either you did not read what you wrote "Option E states to allow incoming TCP ports on 443 and outgoing on 32768-65535 to all IP addresses (0.0.0.0/0)." (because first part of the sentence allows incoming 443) or you do not understand how ACLs work - they are STATELESS, which means, you need to allow both IN and OUT, not just IN like SGs which are stateful. if they were the same - what would be the purpose of the ACLs?

upvoted 1 times

 **Aninina** 1 year, 2 months ago

Selected Answer: AE

AE correct

upvoted 3 times

 **techhb** 1 year, 2 months ago

Selected Answer: AE

A & E , E as NACL is stateless.

upvoted 2 times

 **AHUI** 1 year, 2 months ago

AE:

<https://www.examtopics.com/discussions/amazon/view/29767-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Question #219

Topic 1

A company's application is having performance issues. The application is stateful and needs to complete in-memory tasks on Amazon EC2 instances. The company used AWS CloudFormation to deploy infrastructure and used the M5 EC2 instance family. As traffic increased, the application performance degraded. Users are reporting delays when the users attempt to access the application.

Which solution will resolve these issues in the MOST operationally efficient way?

- A. Replace the EC2 instances with T3 EC2 instances that run in an Auto Scaling group. Make the changes by using the AWS Management Console.
- B. Modify the CloudFormation templates to run the EC2 instances in an Auto Scaling group. Increase the desired capacity and the maximum capacity of the Auto Scaling group manually when an increase is necessary.
- C. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Use Amazon CloudWatch built-in EC2 memory metrics to track the application performance for future capacity planning.
- D. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Deploy the Amazon CloudWatch agent on the EC2 instances to generate custom application latency metrics for future capacity planning.

Correct Answer: D*Community vote distribution*

D (100%)

 Parsons Highly Voted 1 year, 2 months ago

Selected Answer: D

D is the correct answer.

"in-memory tasks" => need the "R" EC2 instance type to archive memory optimization. So we are concerned about C & D. Because EC2 instances don't have built-in memory metrics to CW by default. As a result, we have to install the CW agent to archive the purpose.
upvoted 28 times

 Babba Highly Voted 1 year, 2 months ago

Selected Answer: D

It's D, EC2 do not provide by default memory metrics to CloudWatch and require the CloudWatch Agent to be installed on the monitored instances : <https://aws.amazon.com/premiumsupport/knowledge-center/cloudwatch-memory-metrics-ec2/>
upvoted 10 times

 Guru4Cloud Most Recent 6 months, 2 weeks ago

Selected Answer: D

R5 instances are better optimized for the in-memory workload than M5.
Auto Scaling alone doesn't handle stateful applications well, manual capacity adjustments would still be needed.
Custom latency metrics give better visibility than built-in metrics for capacity planning.
upvoted 4 times

 cookieMr 9 months ago

Selected Answer: D

By replacing the M5 instances with R5 instances, which are optimized for memory-intensive workloads, the application can benefit from increased memory capacity and performance.

In addition, deploying the CloudWatch agent on the EC2 instances allows for the generation of custom application latency metrics, which can provide valuable insights into the application's performance.

This solution addresses the performance issues efficiently by leveraging the appropriate instance types and collecting custom application metrics for better monitoring and future capacity planning.

- A. Replacing with T3 instances may not provide enough memory capacity for in-memory tasks.
- B. Manually increasing the capacity of the ASG does not directly address the performance issues.
- C. Relying solely on built-in EC2 memory metrics may not provide enough granularity for optimizing in-memory tasks.

The most efficient solution is to modify the CloudFormation templates, replace with R5 instances, and deploy the CloudWatch agent for custom metrics.
upvoted 4 times

 Bmarodi 10 months ago

Selected Answer: D

Option D is the correct answer.

upvoted 1 times

 **BABU97** 12 months ago

will go for C

upvoted 1 times

 **Aninina** 1 year, 2 months ago

Selected Answer: D

Would go with D

upvoted 1 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: D

I think D

upvoted 1 times

Question #220

Topic 1

A solutions architect is designing a new API using Amazon API Gateway that will receive requests from users. The volume of requests is highly variable; several hours can pass without receiving a single request. The data processing will take place asynchronously, but should be completed within a few seconds after a request is made.

Which compute service should the solutions architect have the API invoke to deliver the requirements at the lowest cost?

- A. An AWS Glue job
- B. An AWS Lambda function
- C. A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)
- D. A containerized service hosted in Amazon ECS with Amazon EC2

Correct Answer: B*Community vote distribution*

Parsons Highly Voted 1 year, 2 months ago

Selected Answer: B

B is the correct answer.

API Gateway + Lambda is the perfect solution for modern applications with serverless architecture.

upvoted 7 times

TariqKipkemei Most Recent 6 months, 1 week ago

Selected Answer: B

data processing should be completed within a few seconds = An AWS Lambda function

upvoted 1 times

Guru4Cloud 6 months, 2 weeks ago

Selected Answer: B

B. An AWS Lambda function

upvoted 1 times

ukivanlamipi 7 months, 1 week ago

Selected Answer: D

lambda is expensive than running ECS on EC2

upvoted 1 times

pentium75 2 months, 4 weeks ago

"Several hours can pass without receiving a single request", during which Lambda costs 0.00.

upvoted 2 times

Undisputed 8 months ago

Selected Answer: B

Lambda all the way.

upvoted 1 times

cookieMr 9 months ago

Selected Answer: B

Lambda is a serverless compute service that can be triggered by API Gateway to process requests asynchronously. It automatically scales based on the incoming request volume and allows for cost optimization by charging only for the actual compute time used to process the requests.

A. Glue is a fully managed ETL service. It is designed for data processing and transformation tasks rather than serving API requests. It may not be suitable for handling variable request volumes and delivering responses within a few seconds.

C. While EKS provides scalability and flexibility, it may introduce additional complexity and overhead for managing and scaling the infrastructure for handling variable API request volumes.

D. Similar to the previous option, using ECS with EC2 would require additional effort for infrastructure management and scaling, which may not be necessary for handling intermittent and variable API request volumes.

upvoted 3 times

Bmarodi 10 months ago

Selected Answer: B

Option B meets the requirements.

upvoted 1 times

 **Aninina** 1 year, 2 months ago

Selected Answer: B

Lambda !

upvoted 3 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/43780-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Question #221

Topic 1

A company runs an application on a group of Amazon Linux EC2 instances. For compliance reasons, the company must retain all application log files for 7 years. The log files will be analyzed by a reporting tool that must be able to access all the files concurrently.

Which storage solution meets these requirements MOST cost-effectively?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon EC2 instance store
- D. Amazon S3

Correct Answer: D

Community vote distribution

D (100%)

✉  **cookieMr**  9 months ago

Selected Answer: D

- A. EBS provides block-level storage volumes for use with EC2 instances. While it offers durability and persistence, it is not the most cost-effective solution for long-term retention of log files. Additionally, it does not provide concurrent access to the files, which is a requirement in this scenario.
- B. EFS is a scalable file storage service that can be mounted on multiple EC2 instances concurrently. While it provides concurrent access to files, it may not be the most cost-effective option for long-term retention due to its higher pricing compared to S3.
- C. The instance store is a temporary storage option that is physically attached to the EC2 instance. It does not provide the durability and long-term retention required for compliance purposes. Additionally, the instance store is not accessible outside of the specific EC2 instance it is attached to, so concurrent access by the reporting tool would not be possible.

Therefore, considering the requirements for long-term retention, concurrent access, and cost-effectiveness, S3 is the most suitable and cost-effective storage solution.

upvoted 9 times

✉  **Ruffyt**  4 months ago

- A. EBS provides block-level storage volumes for use with EC2 instances. While it offers durability and persistence, it is not the most cost-effective solution for long-term retention of log files. Additionally, it does not provide concurrent access to the files, which is a requirement in this scenario.
- B. EFS is a scalable file storage service that can be mounted on multiple EC2 instances concurrently. While it provides concurrent access to files, it may not be the most cost-effective option for long-term retention due to its higher pricing compared to S3.
- C. The instance store is a temporary storage option that is physically attached to the EC2 instance. It does not provide the durability and long-term retention required for compliance purposes. Additionally, the instance store is not accessible outside of the specific EC2 instance it is attached to, so concurrent access by the reporting tool would not be possible.

upvoted 1 times

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

this sounds like an expensive solution but if necessary then S3 would be the best

upvoted 1 times

✉  **TariqKipkemei** 6 months ago

most cost effective = Amazon S3

upvoted 1 times

✉  **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

D. Amazon S3

upvoted 1 times

✉  **kapit** 9 months, 1 week ago

s3<efs<ebs

upvoted 1 times

Iconique 6 months ago

actually S3 < EBS < EFS, but for EBS you need to pay for the underlying provisioned GB.

If you compare 1 GB then S3 < EBS < EFS but if you have 100GB storage for EBS than EBS is more expensive.

upvoted 1 times

✉  **mattcl** 9 months, 2 weeks ago

"The log files will be analyzed by a reporting tool that must be able to access all the files concurrently", so you need to access concurrently to get the logs. So is EFS. Letter B

upvoted 1 times

 **northyork** 9 months, 2 weeks ago

<https://aws.amazon.com/efs/faq/>

EFS is a file storage service for use with Amazon compute (EC2, containers, serverless) and on-premises servers. EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently accessible storage for up to thousands of EC2 instances.

upvoted 1 times

 **alexandercamachop** 10 months, 2 weeks ago

Selected Answer: D

Whenever we see long time storage and no special requirements that needs EFS or FSx, then S3 is the way.

upvoted 3 times

 **elearningtakai** 12 months ago

Selected Answer: D

To meet the requirements of retaining application log files for 7 years and allowing concurrent access by a reporting tool, while also being cost-effective, the recommended storage solution would be D: Amazon S3.

upvoted 2 times

 **osmk** 12 months ago

ddddddddddddd

upvoted 2 times

 **udo2020** 1 year ago

What about the keyword "concurrently"? Doesn't this mean EFS?

upvoted 3 times

 **Aninina** 1 year, 2 months ago

Selected Answer: D

Cost Effective: S3

upvoted 2 times

 **Parsons** 1 year, 2 months ago

Selected Answer: D

S3 is enough with the lowest cost perspective.

upvoted 1 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/22182-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

Question #222

Topic 1

A company has hired an external vendor to perform work in the company's AWS account. The vendor uses an automated tool that is hosted in an AWS account that the vendor owns. The vendor does not have IAM access to the company's AWS account.

How should a solutions architect grant this access to the vendor?

- A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.
- B. Create an IAM user in the company's account with a password that meets the password complexity requirements. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.
- C. Create an IAM group in the company's account. Add the tool's IAM user from the vendor account to the group. Attach the appropriate IAM policies to the group for the permissions that the vendor requires.
- D. Create a new identity provider by choosing "AWS account" as the provider type in the IAM console. Supply the vendor's AWS account ID and user name. Attach the appropriate IAM policies to the new provider for the permissions that the vendor requires.

Correct Answer: A

Community vote distribution



✉️ mp165 1 year, 2 months ago

Selected Answer: A

A is proper

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html
upvoted 8 times

✉️ cookieMr 9 months ago

By creating an IAM role and delegating access to the vendor's IAM role, you establish a trust relationship between accounts. This allows the vendor's automated tool to assume the role in the company's account and access the necessary resources.

By attaching the appropriate IAM policies to the role, you can define the precise permissions that the vendor requires for their tool to perform its tasks. This ensures that the vendor has the necessary access without granting them direct IAM access to the company's account.

B is incorrect because creating an IAM user with a password would require sharing the credentials with the vendor, which is not recommended for security reasons.

C is incorrect because adding the vendor's IAM user to an IAM group in the company's account would not provide a direct and controlled way to delegate access to the vendor's tool.

D is incorrect because creating a new identity provider for the vendor's AWS account would not provide a straightforward way to delegate access to the vendor's tool. Identity providers are typically used for federated access using external identity systems.

upvoted 6 times

✉️ Ruffyit 4 months ago

Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires

upvoted 1 times

✉️ TariqKipkemei 6 months ago

Selected Answer: A

Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires

upvoted 1 times

✉️ Guru4Cloud 6 months, 2 weeks ago

Selected Answer: A

A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.

upvoted 1 times

✉️ teja54 9 months, 4 weeks ago

Selected Answer: C

.....
upvoted 1 times

✉  **Bmarodi** 10 months ago

Selected Answer: A

Option A fulfill the requirements.

upvoted 1 times

✉  **Aninina** 1 year, 2 months ago

Selected Answer: A

IAM role is the answer

upvoted 1 times

✉  **techhb** 1 year, 2 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

✉  **kbaruu** 1 year, 2 months ago

Selected Answer: A

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

upvoted 2 times

✉  **venice1234** 1 year, 2 months ago

Selected Answer: A

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

upvoted 2 times

✉  **Parsons** 1 year, 2 months ago

Selected Answer: A

A is the correct answer.

upvoted 3 times

✉  **Babba** 1 year, 2 months ago

Selected Answer: D

My guess is D: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

upvoted 2 times

✉  **pentium75** 2 months, 4 weeks ago

But your link describes A, not D.

upvoted 1 times

Question #223

Topic 1

A company has deployed a Java Spring Boot application as a pod that runs on Amazon Elastic Kubernetes Service (Amazon EKS) in private subnets. The application needs to write data to an Amazon DynamoDB table. A solutions architect must ensure that the application can interact with the DynamoDB table without exposing traffic to the internet.

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

- A. Attach an IAM role that has sufficient privileges to the EKS pod.
- B. Attach an IAM user that has sufficient privileges to the EKS pod.
- C. Allow outbound connectivity to the DynamoDB table through the private subnets' network ACLs.
- D. Create a VPC endpoint for DynamoDB.
- E. Embed the access keys in the Java Spring Boot code.

Correct Answer: AD

Community vote distribution

AD (100%)

 **Burrito69** 3 days, 13 hours ago

After seeing D, I didn't even look at option E. its AD correct
upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Selected Answer: AD

B: Wrong, cannot be a user for EKS
C: Not possible as NACL need destination CIDR/ports etc. This is not correct way to connect to DynamoDB
E: Not secure
AD is correct because you need roles for allowing service permissions and accessing DynamoDB with VPC endpoint is the correct way
upvoted 1 times

 **Ruffyit** 4 months ago

The application needs to write data to an Amazon DynamoDB table = Attach an IAM role that has write privileges to the EKS pod
Without exposing traffic to the internet = VPC endpoint for DynamoDB
upvoted 1 times

 **TariqKipkemei** 6 months ago

Selected Answer: AD

The application needs to write data to an Amazon DynamoDB table = Attach an IAM role that has write privileges to the EKS pod
Without exposing traffic to the internet = VPC endpoint for DynamoDB
upvoted 3 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: AD

A. By attaching an IAM role to the EKS pod, you can grant the necessary permissions for the pod to access DynamoDB. The IAM role should have appropriate policies allowing access to the DynamoDB table.

D. Creating a VPC endpoint for DynamoDB allows the EKS pod to access DynamoDB privately within the VPC, without the need for internet connectivity. The VPC endpoint provides a direct and secure connection to DynamoDB, eliminating the need for traffic to flow over the internet.
upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: AD

A. By attaching an IAM role to the EKS pod, you can grant the necessary permissions for the pod to access DynamoDB. The IAM role should have appropriate policies allowing access to the DynamoDB table.

D. Creating a VPC endpoint for DynamoDB allows the EKS pod to access DynamoDB privately within the VPC, without the need for internet connectivity. The VPC endpoint provides a direct and secure connection to DynamoDB, eliminating the need for traffic to flow over the internet.

B is incorrect because attaching an IAM user to the pod is not a recommended approach. IAM users are meant for accessing AWS services through the AWS Management Console or AP.

C is incorrect because configuring outbound connectivity through network ACLs would not provide a secure and direct connection to DynamoDB.

E is incorrect because embedding access keys in the code is not a recommended security practice. It can lead to potential security vulnerabilities. It is better to use IAM roles or other secure mechanisms for providing access to AWS services.

upvoted 2 times

✉ **Bmarodi** 10 months ago

Selected Answer: AD

A & D options fulfill the requirements.

upvoted 1 times

✉ **LuckyAro** 1 year, 2 months ago

Selected Answer: AD

Definitely

upvoted 1 times

✉ **Aninina** 1 year, 2 months ago

Selected Answer: AD

A D are the correct options

upvoted 1 times

✉ **venice1234** 1 year, 2 months ago

Selected Answer: AD

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

<https://aws.amazon.com/about-aws/whats-new/2019/09/amazon-eks-adds-support-to-assign-iam-permissions-to-kubernetes-service-accounts/>

upvoted 2 times

✉ **Parsons** 1 year, 2 months ago

Selected Answer: AD

A, D is the correct answer.

upvoted 2 times

✉ **mhmt4438** 1 year, 2 months ago

Selected Answer: AD

The correct answer is A,D

upvoted 1 times

Question #224

Topic 1

A company recently migrated its web application to AWS by rehosting the application on Amazon EC2 instances in a single AWS Region. The company wants to redesign its application architecture to be highly available and fault tolerant. Traffic must reach all running EC2 instances randomly.

Which combination of steps should the company take to meet these requirements? (Choose two.)

- A. Create an Amazon Route 53 failover routing policy.
- B. Create an Amazon Route 53 weighted routing policy.
- C. Create an Amazon Route 53 multivalue answer routing policy.
- D. Launch three EC2 instances: two instances in one Availability Zone and one instance in another Availability Zone.
- E. Launch four EC2 instances: two instances in one Availability Zone and two instances in another Availability Zone.

Correct Answer: CE

Community vote distribution



✉ **cookieMr** 9 months ago

Selected Answer: CE

C. A multivalue answer routing policy in Route 53 allows you to configure multiple values for a DNS record, and Route 53 responds to DNS queries with multiple random values. This enables the distribution of traffic randomly among the available EC2 instances.

E. By launching EC2 instances in different AZs, you achieve high availability and fault tolerance. Launching four instances (two in each AZ) ensures that there are enough resources to handle the traffic load and maintain the desired level of availability.

A. Failover routing is designed to direct traffic to a backup resource or secondary location only when the primary resource or location is unavailable.

B. Although a weighted routing policy allows you to distribute traffic across multiple EC2 instances, it does not ensure random distribution.

D. While launching instances in multiple AZs is important for fault tolerance, having only three instances does not provide an even distribution of traffic. With only three instances, the traffic may not be evenly distributed, potentially leading to imbalanced resource utilization.

upvoted 13 times

✉ **Steve_4542636** 1 year ago

Selected Answer: BE

I went back and rewatched the lectures from Udemy on Weighted and Multi-Value. The lecturer said that Multi-value is *not* as substitute for ELB and he stated that DNS load balancing is a good use case for Weighted routing policies

upvoted 8 times

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

Weighted routing based on weight assigned, it can not do randomly choose, please see last sentence of the question choose randomly.

upvoted 8 times

✉ **foha2012** 2 months ago

what about 50 50 weighted ?

upvoted 1 times

✉ **bujuman** 1 month, 2 weeks ago

Selected Answer: CE

CE seems good to me due to " highly available and fault tolerant" and following explanation:
<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy-multivalue.html>

upvoted 1 times

✉ **bujuman** 1 month, 2 weeks ago

Specifically with this requirement : "Traffic must reach all running EC2 instances randomly"

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Selected Answer: CE

E: For HA

C: Random routing can only be created with multivalue answer routing policy.

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

"To route traffic approximately randomly to multiple resources, such as web servers, you create one multivalue answer record for each resource and, optionally, associate a Route 53 health check with each record."

upvoted 2 times

 **Ruffyit** 4 months ago

C. A multivalue answer routing policy in Route 53 allows you to configure multiple values for a DNS record, and Route 53 responds to DNS queries with multiple random values. This enables the distribution of traffic randomly among the available EC2 instances.

E. By launching EC2 instances in different AZs, you achieve high availability and fault tolerance. Launching four instances (two in each AZ) ensures that there are enough resources to handle the traffic load and maintain the desired level of availability.

A. Failover routing is designed to direct traffic to a backup resource or secondary location only when the primary resource or location is unavailable.

B. Although a weighted routing policy allows you to distribute traffic across multiple EC2 instances, it does not ensure random distribution.

upvoted 1 times

 **mohamoha** 4 months, 2 weeks ago

First I thought it was weighted but after research C is the correct answer :

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

upvoted 1 times

 **daniel33** 5 months, 3 weeks ago

Selected Answer: CE

Multivalue routing can do random load balancing according to the AWS website:

To route traffic approximately randomly to multiple resources, such as web servers, you create one multivalue answer record for each resource and, optionally, associate a Route 53 health check with each record.

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

upvoted 4 times

 **Tom123456ac** 5 months, 3 weeks ago

This question is so wired , 3 instances nothing wrong with it

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

I guess it's the "highly available AND fault tolerant" requirement. If AZ 1 fails, you have only a single server left in the other region.

upvoted 2 times

 **Techi47** 6 months ago

Option CE Correct:

To route traffic roughly and randomly to multiple resources, such as web servers, you create a multi-value response record for each resource and optionally associate a Route 53 health check with each record.

<https://disaster-recovery.workshop.aws/en/services/networking/route53/routing-policies/routing-multiple-answer.html>

upvoted 1 times

 **kwang312** 6 months ago

Selected Answer: CE

CE is correct

upvoted 1 times

 **TariqKipkemei** 6 months ago

Selected Answer: CE

Highly available and fault tolerant = two instances in two AZs

Route traffic randomly = Amazon Route 53 multivalue answer routing policy

upvoted 1 times

 **LazyTs** 6 months, 3 weeks ago

Selected Answer: CE

Multivalue answer routing policy – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random. You can use multivalue answer routing to create records in a private hosted zone.

Weighted routing policy – Use to route traffic to multiple resources in proportions that you specify. You can use weighted routing to create records in a private hosted zone.

upvoted 1 times

 **foha2012** 2 months ago

what about 50 50 weighted routing ?

upvoted 1 times

 **Zeezie** 8 months ago

I chose CE, but couldn't it also be BE? If you set all of the weights to the same, equal value? Wouldn't then the traffic be distributed randomly and evenly among all healthy instances?

upvoted 1 times

✉ **jacob_ho** 6 months, 3 weeks ago

This is "equal distribution", not "random distribution"; think about the differences
upvoted 4 times

✉ **samsoft556** 9 months ago

Selected Answer: CE

Randomly is the key word
upvoted 2 times

✉ **secdgs** 9 months, 2 weeks ago

Selected Answer: CE

C: Multi-value To route traffic approximately randomly to multiple resources and have health check
B: Weighted default use for when you need load to one server more than other server. if you need for random to all servers should be letter in this C options "and weight to all servers with same value".
upvoted 1 times

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

Selected Answer: CE

Must C and E, B is not correct because it based on the assigned weight it can not do randomly
upvoted 1 times

✉ **ChrisAn** 9 months, 3 weeks ago

Selected Answer: CE

Option C, creating an Amazon Route 53 multivalue answer routing policy, is the correct choice. With this routing policy, Route 53 returns multiple IP addresses for the same domain name, allowing the traffic to be distributed randomly among the available EC2 instances. This ensures that the traffic is evenly distributed across the instances launched in different Availability Zones, achieving the desired randomness and load balancing.

Option E is the correct choice. By launching instances in different Availability Zones, the company ensures that there are redundant copies of the application running in separate physical locations, providing fault tolerance. With two instances in one Availability Zone and two instances in another, traffic can be distributed randomly among them, improving availability and load balancing.

upvoted 1 times

Question #225

Topic 1

A media company collects and analyzes user activity data on premises. The company wants to migrate this capability to AWS. The user activity data store will continue to grow and will be petabytes in size. The company needs to build a highly available data ingestion solution that facilitates on-demand analytics of existing data and new data with SQL.

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

- A. Send activity data to an Amazon Kinesis data stream. Configure the stream to deliver the data to an Amazon S3 bucket.
- B. Send activity data to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliver the data to an Amazon Redshift cluster.
- C. Place activity data in an Amazon S3 bucket. Configure Amazon S3 to run an AWS Lambda function on the data as the data arrives in the S3 bucket.
- D. Create an ingestion service on Amazon EC2 instances that are spread across multiple Availability Zones. Configure the service to forward data to an Amazon RDS Multi-AZ database.

Correct Answer: A

Community vote distribution

B (94%) 6%

≡ **beginnercloud** 7 months ago

Selected Answer: B

Petabyte scale- Redshift
upvoted 9 times

≡ **Berny** 1 year, 2 months ago

Selected Answer: B

Data ingestion through Kinesis data streams will require manual intervention to provide more shards as data size grows. Kinesis firehose will ingest data with the least operational overhead.
upvoted 6 times

≡ **scar0909** 2 weeks, 1 day ago

Selected Answer: B

Kinesis data stream cannot detined to s3
upvoted 1 times

≡ **Ruffyt** 4 months ago

1- Kinesis Data Stream provides a fully managed platform for custom data processing and analysis. Or we can say that used for custom data processing and analysis which required more manual intervention.
2- Kinesis Data Firehose simplifies the delivery of streaming data to various destinations without the need for complex transformations.
Option B is more suitable for the given scenario.
upvoted 4 times

≡ **David_Ang** 5 months ago

Selected Answer: B

always if you have a service that is meant for a specific job, it the correct answer, is logic. "A" is not good enough for this situation
upvoted 1 times

≡ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: B

B. Send activity data to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliver the data to an Amazon Redshift cluster.
upvoted 2 times

≡ **NVenkatS** 7 months ago

Selected Answer: B

Petabyte scale- Redshift
upvoted 4 times

≡ **A1975** 7 months, 3 weeks ago

Selected Answer: B

1- Kinesis Data Stream provides a fully managed platform for custom data processing and analysis. Or we can say that used for custom data processing and analysis which required more manual intervention.

2- Kinesis Data Firehose simplifies the delivery of streaming data to various destinations without the need for complex transformations. Option B is more suitable for the given scenario.

upvoted 2 times

sickcow 8 months, 3 weeks ago

Selected Answer: B

Petabyte Scale sounds like Redshift!

upvoted 2 times

cookieMr 9 months ago

Selected Answer: B

B provides a fully managed and scalable solution for data ingestion and analytics. KDF simplifies the data ingestion process by automatically scaling to handle large volumes of streaming data. It can directly load the data into a Redshift cluster, which is a powerful and fully managed data warehousing solution.

A. While Kinesis can handle streaming data, it requires additional processing to load the data into an analytics solution.

C. Although S3 and Lambda can handle the storage and processing of data, it requires more manual configuration and management compared to the fully managed solution offered by KDF and Redshift.

D. This option involves more operational overhead, as it requires managing and scaling the EC2 instances and RDS database infrastructure manually.

Therefore, option B with KDF delivering the data to Redshift cluster offers the most streamlined and operationally efficient solution for ingesting and analyzing the user activity data in the given scenario.

upvoted 1 times

pisica134 9 months ago

petabytes in size => redshift

upvoted 2 times

mattcl 9 months, 2 weeks ago

It's A. Data Stream is better in this case, and you can query data in S3 with Athena

upvoted 2 times

Yadav_Sanjay 9 months, 1 week ago

Data Stream Can't write to S3. That's why B is only left correct answer.

upvoted 1 times

baba365 9 months ago

Answer A... key phrase' least operational overhead'

KDF can write to S3 ... <https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html>

upvoted 1 times

JoeGuan 7 months, 1 week ago

<https://aws.amazon.com/streaming-data/> a good explanation of either option. firehose appears to be an option for Least operational overhead, as the streams product requires some building of apps etc.

upvoted 1 times

Bmarodi 10 months ago

Selected Answer: B

Option B is correct answer.

upvoted 1 times

kruasan 11 months ago

Selected Answer: B

This solution meets the requirements as follows:

- Kinesis Data Firehose can scale to ingest and process multiple terabytes per hour of streaming data. This can easily handle the petabyte-scale data volumes.
- Firehose can deliver the data to Redshift, a petabyte-scale data warehouse, enabling on-demand SQL analytics of the data.
- Redshift is a fully managed service, minimizing operational overhead. Firehose is also fully managed, handling scalability, availability, and durability of the streaming data ingestion.

upvoted 4 times

gold4otas 12 months ago

Selected Answer: B

B: The answer is certainly option "B" because ingesting user activity data can easily be handled by Amazon Kinesis Data streams. The ingested data can then be sent into Redshift for Analytics.

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. Amazon Redshift Serverless lets you access and analyze data without all of the configurations of a provisioned data warehouse.

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

upvoted 2 times

GalileoEC2 1 year ago

the Key sentence here is: "that facilitates on-demand analytics", that's the reason because we need to choose Kinesis Data streams over Data Firehose

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Why that? Analytics is done in Redshift, not by Kinesis.

upvoted 1 times

 **alexleely** 1 year, 2 months ago

Selected Answer: B

B: Kinesis Data Firehose service automatically load the data into Amazon Redshift and is a petabyte-scale data warehouse service. It allows you to perform on-demand analytics with minimal operational overhead. Since the requirement didn't state what kind of analytics you need to run, we can assume that we do not need to set up additional services to provide further analytics. Thus, it has the least operational overhead.

Why not A: It is a viable solution, but storing the data in S3 would require you to set up additional services like Amazon Redshift or Amazon Athena to perform the analytics.

upvoted 2 times

Question #226

Topic 1

A company collects data from thousands of remote devices by using a RESTful web services application that runs on an Amazon EC2 instance. The EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket. The number of remote devices will increase into the millions soon. The company needs a highly scalable solution that minimizes operational overhead.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Use AWS Glue to process the raw data in Amazon S3.
- B. Use Amazon Route 53 to route traffic to different EC2 instances.
- C. Add more EC2 instances to accommodate the increasing amount of incoming data.
- D. Send the raw data to Amazon Simple Queue Service (Amazon SQS). Use EC2 instances to process the data.
- E. Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3.

Correct Answer: AE*Community vote distribution*

 AE (100%)

 **Parsons**  1 year, 2 months ago

Selected Answer: AE

A, E is the correct answer

"RESTful web services" => API Gateway.

"EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket" => GLUE with (Extract - Transform - Load)

upvoted 10 times

 **Ruffyt**  4 months ago

A - Use AWS Glue to process the raw data in Amazon S3

E - Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3

upvoted 1 times

 **TariqKipkemei** 6 months ago

Selected Answer: AE

E then A no doubt.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: AE

A. It automatically discovers the schema of the data and generates ETL code to transform it.

E. API Gateway can be used to receive the raw data from the remote devices via RESTful web services. It provides a scalable and managed infrastructure to handle the incoming requests. The data can then be sent to an Amazon Kinesis data stream, which is a highly scalable and durable real-time data streaming service. From there, Amazon Kinesis Data Firehose can be configured to use the data stream as a source and deliver the transformed data to Amazon S3. This combination of services allows for the seamless ingestion and processing of data while minimizing operational overhead.

upvoted 1 times

 **ibu007** 6 months, 3 weeks ago

Selected Answer: AE

A - Use AWS Glue to process the raw data in Amazon S3

E - Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3

upvoted 2 times

 **GCB1990** 7 months ago

Correct answer: D and E

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: AE

A. It automatically discovers the schema of the data and generates ETL code to transform it.

E. API Gateway can be used to receive the raw data from the remote devices via RESTful web services. It provides a scalable and managed infrastructure to handle the incoming requests. The data can then be sent to an Amazon Kinesis data stream, which is a highly scalable and durable real-time data streaming service. From there, Amazon Kinesis Data Firehose can be configured to use the data stream as a source and deliver the transformed data to Amazon S3. This combination of services allows for the seamless ingestion and processing of data while minimizing operational overhead.

B. It does not directly address the need for scalable data processing and storage. It focuses on managing DNS and routing traffic to different endpoints.

C. Adding more EC2 can lead to increased operational overhead in terms of managing and scaling the instances.

D. Using SQS and EC2 for processing data introduces more complexity and operational overhead.

upvoted 3 times

✉  **wRhIh** 9 months, 1 week ago

Why not BC?

upvoted 1 times

✉  **AnnieTran_91** 9 months, 2 weeks ago

Why it not CE?

Add more EC2 instances to accommodate the increasing amount of incoming data?

upvoted 1 times

✉  **TTaws** 9 months, 1 week ago

EC2 is not server-less. they want to minimize overhead

upvoted 1 times

✉  **studynoplay** 10 months, 1 week ago

Selected Answer: AE

minimizes operational overhead = Serverless

Glue, Kinesis Datastream, S3 are serverless

upvoted 1 times

✉  **KZM** 1 year, 1 month ago

How about "C" to increase EC2 instances for the increased devices soon?

upvoted 1 times

✉  **Aninina** 1 year, 2 months ago

Selected Answer: AE

Glue and API

upvoted 2 times

✉  **mhmt4438** 1 year, 2 months ago

Selected Answer: AE

<https://www.examtopics.com/discussions/amazon/view/83387-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Question #227

Topic 1

A company needs to retain its AWS CloudTrail logs for 3 years. The company is enforcing CloudTrail across a set of AWS accounts by using AWS Organizations from the parent account. The CloudTrail target S3 bucket is configured with S3 Versioning enabled. An S3 Lifecycle policy is in place to delete current objects after 3 years.

After the fourth year of use of the S3 bucket, the S3 bucket metrics show that the number of objects has continued to rise. However, the number of new CloudTrail logs that are delivered to the S3 bucket has remained consistent.

Which solution will delete objects that are older than 3 years in the MOST cost-effective manner?

- A. Configure the organization's centralized CloudTrail trail to expire objects after 3 years.
- B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.
- C. Create an AWS Lambda function to enumerate and delete objects from Amazon S3 that are older than 3 years.
- D. Configure the parent account as the owner of all objects that are delivered to the S3 bucket.

Correct Answer: B

Community vote distribution

✉ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: B

This is the most cost-effective option because:

- Versioning has caused the number of objects to increase over time, even as current objects are deleted after 3 years. By deleting previous versions as well, this will clean up old object versions and reduce storage costs.
- An S3 Lifecycle policy incurs no additional charges and requires no additional resources to configure and run. It is a native S3 tool for managing object lifecycles cost-effectively.

upvoted 5 times

✉ **Mikado211** 3 months, 3 weeks ago

Selected Answer: B

I did something similar recently : Lifecycle is triggered more or less each 24 hours, in my case it removed hundreds of gigabytes and millions of small files in one shot. Using another mechanism like a script would have taken days if not weeks.

upvoted 1 times

✉ **Ruffyit** 4 months ago

This is the most cost-effective option because:

- Versioning has caused the number of objects to increase over time, even as current objects are deleted after 3 years. By deleting previous versions as well, this will clean up old object versions and reduce storage costs.
- An S3 Lifecycle policy incurs no additional charges and requires no additional resources to configure and run. It is a native S3 tool for managing object lifecycles cost-effectively.

upvoted 2 times

✉ **TariqKipkemei** 6 months ago

Selected Answer: B

Ensure to delete previous versions as well.

upvoted 1 times

✉ **cookieMr** 9 months ago

Selected Answer: B

By configuring the S3 Lifecycle policy to delete previous versions as well as current versions, the older versions of the CloudTrail logs will be deleted. This ensures that objects older than 3 years are removed from the S3 bucket, reducing the object count and controlling storage costs.

- A. This option is not directly related to managing objects in the S3. It focuses on configuring the expiration of CloudTrail trails, which may not address the need to delete objects from the S3 bucket.
- C. While it is technically possible to create a Lambda to delete objects older than 3 years, this approach would introduce additional complexity and operational overhead.
- D. Changing the ownership of the objects in the S3 bucket does not directly address the need to delete objects older than 3 years. Ownership does not affect the deletion behavior of the objects.

upvoted 4 times

✉ **Bmarodi** 10 months ago

Selected Answer: B

I go for option B.

upvoted 1 times

ruqui 10 months ago

I don't think it's possible to configure an S3 lifecycle policy to delete all versions of an object, so B is wrong ... I think the question is improperly worded

upvoted 1 times

Rahulbit34 10 months, 3 weeks ago

- Versioning has caused the number of objects to increase over time, even as current objects are deleted after 3 years. By deleting previous versions as well, this will clean up old object versions and reduce storage costs.
- An S3 Lifecycle policy incurs no additional charges and requires no additional resources to configure and run. It is a native S3 tool for managing object lifecycles cost-effectively.

upvoted 1 times

kruasan 11 months ago

Selected Answer: B

This is the most cost-effective option because:

- Versioning has caused the number of objects to increase over time, even as current objects are deleted after 3 years. By deleting previous versions as well, this will clean up old object versions and reduce storage costs.
- An S3 Lifecycle policy incurs no additional charges and requires no additional resources to configure and run. It is a native S3 tool for managing object lifecycles cost-effectively.

upvoted 3 times

kruasan 11 months ago

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

upvoted 2 times

bullrem 1 year, 2 months ago

Selected Answer: C

A more cost-effective solution would be to configure the organization's centralized CloudTrail trail to expire objects after 3 years. This would ensure that all objects, including previous versions, are deleted after the specified retention period.

Another option would be to create an AWS Lambda function to enumerate and delete objects from Amazon S3 that are older than 3 years, this would allow you to have more control over the deletion process and to write a custom logic that best fits your use case.

upvoted 3 times

pentium75 2 months, 4 weeks ago

As long as versioning on the S3 bucket is enabled, any deletion, whether performed by CloudTrail or by your custom Lambda function, will simply add a new version with a deletion marker but will not delete the previous version.

upvoted 2 times

JayBee65 1 year, 2 months ago

Selected Answer: B

The question clearly says "An S3 Lifecycle policy is in place to delete current objects after 3 years". This implies that previous versions are not deleted, since this is a separate setting, and since logs are constantly changed, it would seem to make sense to delete previous versions so, so B. D is wrong, since the parent account (the management account) will already be the owner of all objects delivered to the S3 bucket, "All accounts in the organization can see MyOrganizationTrail in their list of trails, but member accounts cannot remove or modify the organization trail. Only the management account or delegated administrator account can change or delete the trail for the organization.", see <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

upvoted 2 times

John_Zhuang 1 year, 2 months ago

Selected Answer: B

B is the right answer. Ref: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html#:~:text=The%20CloudTrail%20trail,time%20has%20passed>.

Option A is wrong. No way to expire the cloudtrail logs

upvoted 3 times

techhb 1 year, 2 months ago

Selected Answer: B

Configure the S3 Lifecycle policy to delete previous versions

upvoted 2 times

Aninina 1 year, 2 months ago

Selected Answer: B

B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.

upvoted 1 times

Aninina 1 year, 2 months ago

B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.

upvoted 1 times

Parsons 1 year, 2 months ago

Selected Answer: B

B is correct answer

upvoted 2 times

 **AHUI** 1 year, 2 months ago

Ans: A

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

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. Users with CloudTrail permissions in member accounts can see this trail when they log into the AWS CloudTrail console from their AWS accounts, or when they run AWS CLI commands such as describe-trail. However, users in member accounts do not have sufficient permissions to delete the organization trail, turn logging on or off, change what types of events are logged, or otherwise change the organization trail in any way.

upvoted 1 times

 **AHUI** 1 year, 2 months ago

correction: Ans D is the answer.

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

upvoted 1 times

Question #228

Topic 1

A company has an API that receives real-time data from a fleet of monitoring devices. The API stores this data in an Amazon RDS DB instance for later analysis. The amount of data that the monitoring devices send to the API fluctuates. During periods of heavy traffic, the API often returns timeout errors.

After an inspection of the logs, the company determines that the database is not capable of processing the volume of write traffic that comes from the API. A solutions architect must minimize the number of connections to the database and must ensure that data is not lost during periods of heavy traffic.

Which solution will meet these requirements?

- A. Increase the size of the DB instance to an instance type that has more available memory.
- B. Modify the DB instance to be a Multi-AZ DB instance. Configure the application to write to all active RDS DB instances.
- C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.
- D. Modify the API to write incoming data to an Amazon Simple Notification Service (Amazon SNS) topic. Use an AWS Lambda function that Amazon SNS invokes to write data from the topic to the database.

Correct Answer: C

Community vote distribution

C (100%)

✉  **mwwt2022** 3 months ago

Selected Answer: C

//minimize the number of connections to the database and must ensure that data is not lost during periods of heavy traffic//

I go for C

upvoted 1 times

✉  **Ruffyit** 4 months ago

Decouple the API and the DB with Amazon Simple Queue Service (Amazon SQS) queue.

upvoted 2 times

✉  **oluolope** 5 months, 1 week ago

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-lambda-function-trigger.html>
SQS can invoke lambda indeed. Initially I picked D because I wasn't sure it was possible but , this article shows it is. It makes this question even more confusing for me as it is also possible to trigger lambda from SNS:

<https://docs.aws.amazon.com/sns/latest/dg/sns-lambda-as-subscriber.html>

I don't know which option between C and D makes more sense. I still have a preference for D as it seems less hacky than C.

upvoted 1 times

✉  **TariqKipkemei** 6 months ago

Selected Answer: C

Decouple the API and the DB with Amazon Simple Queue Service (Amazon SQS) queue.

upvoted 2 times

✉  **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: C

C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.

upvoted 1 times

✉  **cookieMr** 9 months ago

Selected Answer: C

By leveraging SQS as a buffer and using an Lambda to process and write data from the queue to the database, the solution provides scalability, decoupling, and reliability while minimizing the number of connections to the database. This approach handles fluctuations in traffic and ensures data integrity during high-traffic periods.

A. Increasing the size of the DB instance may provide more memory, but it does not address the issue of handling high write traffic efficiently and minimizing connections to the database.

B. Modifying the DB instance to be a Multi-AZ instance and writing to all active instances can improve availability but does not address the issue of efficiently handling high write traffic and minimizing connections to the database.

D. Using SNS and an Lambda can provide decoupling and scalability, but it is not suitable for handling heavy write traffic efficiently and minimizing connections to the database.

upvoted 2 times

 **Moccorso** 9 months, 1 week ago

I think D, "Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database" SQS can't invokes Lambda because SQS is pull.

upvoted 3 times

 **pentium75** 2 months, 4 weeks ago

"Invoke a Lambda function from an Amazon SQS trigger"

https://docs.aws.amazon.com/lambda/latest/dg/example_serverless_SQS_Lambda_section.html

upvoted 1 times

 **shivamrulz** 9 months, 2 weeks ago

Why not B

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

a) You can't write to multiple instances at the same time

b) If you could, it would probably not increase performance

c) if it would increase performance then it would probably double performance, which might not be enough

Decoupling is the way to go - let clients submit data via APIs, and write it asynchronously to the database. Don't let clients wait until data has been written.

upvoted 2 times

 **Russ99** 1 year ago

C is indeed the correct answer for the use case

upvoted 1 times

 **kaushald** 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

 **Steve_4542636** 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

 **maciekmaciek** 1 year, 1 month ago

Selected Answer: C

C looks ok

upvoted 1 times

 **iamjaehyuk** 1 year, 1 month ago

why not D?

upvoted 1 times

 **Parsons** 1 year, 2 months ago

Selected Answer: C

C is correct.

upvoted 2 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: C

C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.

To minimize the number of connections to the database and ensure that data is not lost during periods of heavy traffic, the company should modify the API to write incoming data to an Amazon SQS queue. The use of a queue will act as a buffer between the API and the database, reducing the number of connections to the database. And the use of an AWS Lambda function invoked by SQS will provide a more flexible way of handling the data and processing it. This way, the function will process the data from the queue and insert it into the database in a more controlled way.

upvoted 2 times

 **Aninina** 1 year, 2 months ago

Did you use ChatGPT?

upvoted 6 times

 **Nguyen25183** 1 year ago

same question as you :D

upvoted 1 times

Question #229

Topic 1

A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.

Which solution meets these requirements?

- A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.
- B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.
- C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
- D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

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

✉️  **cookieMr**  9 months ago

Selected Answer: A

Migrating the databases to Aurora Serverless provides automated scaling and replication capabilities. Aurora Serverless automatically scales the capacity based on the workload, allowing for seamless addition or removal of compute capacity as needed. It also offers improved performance, durability, and high availability without requiring manual management of replication and scaling.

- B. Incorrect because it suggests migrating to a different database engine, which may introduce compatibility issues and require significant code modifications.
 - C. Incorrect because consolidating into a larger MySQL database on larger EC2 instances does not provide the desired scalability and automation.
 - D. Incorrect because using EC2 Auto Scaling groups for the database tier still requires manual management of replication and scaling.
- upvoted 5 times

✉️  **TariqKipkemei**  6 months ago

Selected Answer: A

Migrate the databases to Amazon Aurora Serverless for Aurora MySQL

upvoted 1 times

✉️  **Undisputed** 8 months ago

Selected Answer: A

Aurora MySQL

upvoted 1 times

✉️  **Bmarodi** 10 months ago

Selected Answer: A

Option A is right answer.

upvoted 1 times

✉️  **Bhrino** 1 year, 1 month ago

Selected Answer: A

A is correct because aurora might be more expensive but its serverless and is much faster

upvoted 1 times

✉️  **mp165** 1 year, 2 months ago

Selected Answer: A

A is porper

<https://aws.amazon.com/rds/aurora/serverless/>

upvoted 3 times

✉️  **Aninina** 1 year, 2 months ago

Selected Answer: A

Aurora MySQL

upvoted 1 times

✉️  **mhmt4438** 1 year, 2 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/51509-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

Question #230

Topic 1

A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application. A solutions architect wants to implement a solution that is highly available, fault tolerant, and automatically scalable.

What should the solutions architect recommend?

- A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
- B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
- C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.
- D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

Correct Answer: C

Community vote distribution



✉️ **pentium75** Highly Voted 2 months, 4 weeks ago

Selected Answer: C

See <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>
upvoted 5 times

✉️ **MiniYang** Most Recent 3 months, 3 weeks ago

Selected Answer: B

Highly available, fault tolerant and automatically scalable=> Autoscaling and Diffrent AZ
upvoted 1 times

✉️ **pentium75** 2 months, 4 weeks ago

NAT instances are legacy technology. "If you're already using a NAT instance, we recommend that you replace it with a NAT gateway." Thus C.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>
upvoted 3 times

✉️ **TariqKipkemei** 6 months ago

Selected Answer: C

Highly available, fault tolerant, and automatically scalable = two NAT gateways in different Availability Zones
upvoted 2 times

✉️ **Undisputed** 8 months ago

Selected Answer: C

Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones
upvoted 1 times

✉️ **cookieMr** 9 months ago

Selected Answer: C

This recommendation ensures high availability and fault tolerance by distributing the NAT gateways across multiple AZs. NAT gateways are managed AWS services that provide scalable and highly available outbound NAT functionality. By deploying NAT gateways in different AZs, the company can achieve redundancy and avoid a single point of failure. This solution also provides automatic scaling to handle increasing traffic without manual intervention.

Option A is incorrect because placing both NAT gateways in the same Availability Zone does not provide fault tolerance.

Option B is incorrect because using Auto Scaling groups with Network Load Balancers is not the recommended approach for NAT instances.

Option D is incorrect because Spot Instances are not suitable for critical infrastructure components like NAT instances.
upvoted 3 times

✉️ **Axeashes** 9 months, 3 weeks ago

Selected Answer: C

HA: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>
Scalability: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>
upvoted 1 times

✉️ **Bhrino** 1 year, 1 month ago

Selected Answer: C

fyi yall in most cases nat instances are a bad thing because their customer managed while nat gateways are AWS Managed. So in this case I already know to get rid of the nat instances the reason its c is because it wants high availability meaning different AZs
upvoted 4 times

✉ **Theodorz** 1 year, 1 month ago

Could anybody teach me why the B cannot be correct answer? This solution also seems providing Scalability(Auto Scaling Group), High Availability(different AZ), and Fault Tolerance(NLB & AZ).

I honestly think that C is not enough, because each NAT gateway can provide a few scalability, but the bandwidth limit is clearly explained in the document. The C exactly mentioned "two NAT gateways" so the number of NAT is fixed, which will reach its limit soon.

upvoted 3 times

✉ **KZM** 1 year, 1 month ago

Option B proposes to use an Auto Scaling group with Network Load Balancers to continue using the existing two NAT instances. However, NAT instances do not support automatic failover without a script, unlike NAT gateways which provide this functionality. Additionally, using Network Load Balancers to balance traffic between NAT instances adds more complexity to the solution.

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

upvoted 3 times

✉ **mwwt2022** 3 months ago

Thx for your explanation!

upvoted 1 times

✉ **JayBee65** 1 year, 2 months ago

C. If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html#nat-gateway-basics>

upvoted 2 times

✉ **techhb** 1 year, 2 months ago

Selected Answer: C

Replace NAT Instances with Gateway

upvoted 2 times

✉ **mhmt4438** 1 year, 2 months ago

Selected Answer: C

Correct answer is C

upvoted 2 times

Question #231

Topic 1

An application runs on an Amazon EC2 instance that has an Elastic IP address in VPC A. The application requires access to a database in VPC B. Both VPCs are in the same AWS account.

Which solution will provide the required access MOST securely?

- A. Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.
- B. Configure a VPC peering connection between VPC A and VPC B.
- C. Make the DB instance publicly accessible. Assign a public IP address to the DB instance.
- D. Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.

Correct Answer: B

Community vote distribution

B (86%)

14%

✉️  **JayBee65**  1 year, 2 months ago

A is correct. B will work but is not the most secure method, since it will allow everything in VPC A to talk to everything in VPC B and vice versa, not at all secure. A on the other hand will only allow the application (since you select its IP address) to talk to the application server in VPC A - you are allowing only the required connectivity. See the link for this exact use case:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.RDSSecurityGroups.html>

upvoted 13 times

✉️  **mhmt4438** 1 year, 1 month ago

" allows all traffic from the public IP address" Nice bro niceee This is absolutely the most secure method at all. :))

upvoted 13 times

✉️  **test_devops_aws** 1 year ago

:))))))))

upvoted 1 times

✉️  **datz** 11 months, 3 weeks ago

he must be the security engineer lolol :D

"Jaybee" - Please dont ever say that traffic over the public internet is secure :D

upvoted 4 times

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

Both VPCs are in the "SAME AWS ACCOUNT" and the requirement specifies allowing traffic from the *PUBLIC IP of the APPLICATION SERVER*. In this case the traffic remains inside the AWS infrastructure or will it go through the public internet?

upvoted 2 times

✉️  **pentium75** 2 months, 4 weeks ago

Answer A (not "the requirement") specifies "allowing traffic from the public IP", which is for sure NOT the "most secure" option.

upvoted 2 times

✉️  **DUBURA**  4 months ago

Selected Answer: B

B. Configure a VPC peering connection between VPC A and VPC B.

The most secure solution is to configure a VPC peering connection between the two VPCs. This allows private communication between the application server and the database, without exposing resources to the public internet.

Option A exposes the database to the public internet by allowing inbound traffic from a public IP address.

Option C makes the database instance itself public, which is insecure.

Option D adds complexity with a proxy that is not needed when a VPC peering connection can enable private communication between VPCs.

So option B is the most secure while allowing the necessary connectivity between the application server and the database in the separate VPCs.
upvoted 7 times

✉️  **Ruffyit**  4 months ago

When you establish peering relationships between VPCs across different AWS Regions, resources in the VPCs (for example, EC2 instances and Lambda functions) in different AWS Regions can communicate with each other using private IP addresses, without using a gateway, VPN connection, or network appliance. The traffic remains in the private IP space. All inter-Region traffic is encrypted with no single point of failure, or bandwidth bottleneck. Traffic always stays on the global AWS backbone, and never traverses the public internet, which reduces threats, such as

common exploits, and DDoS attacks. Inter-Region VPC peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy.

upvoted 1 times

 **rlamberti** 5 months ago

Selected Answer: B

Most secure = not leaving AWS network.

VPC peering is the way.

upvoted 2 times

 **TariqKipkemei** 6 months ago

Selected Answer: B

VPC to VPC comms = VPC peering

upvoted 1 times

 **Sutariya** 6 months, 3 weeks ago

B is correct : Setup VPC peering and connect Application from VPC A to connect with VPC B in private subnet so DB instance always secure with internet.

upvoted 1 times

 **_d1rk_** 7 months, 1 week ago

Am I missing something or simply A is wrong because, without VPC peering (or other inter-connection sharing mechanisms such as Transit Gateway or VPN), VPC A and VPC B cannot communicate each other?

upvoted 1 times

 **jacob_ho** 6 months, 3 weeks ago

can use vpc endpoints but no option use that

upvoted 1 times

 **A1975** 7 months, 3 weeks ago

Selected Answer: B

When you establish peering relationships between VPCs across different AWS Regions, resources in the VPCs (for example, EC2 instances and Lambda functions) in different AWS Regions can communicate with each other using private IP addresses, without using a gateway, VPN connection, or network appliance. The traffic remains in the private IP space. All inter-Region traffic is encrypted with no single point of failure, or bandwidth bottleneck. Traffic always stays on the global AWS backbone, and never traverses the public internet, which reduces threats, such as common exploits, and DDoS attacks. Inter-Region VPC peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

upvoted 2 times

 **animefan1** 8 months, 3 weeks ago

Selected Answer: B

With peering, we EC2 can communicate with RDS. RDS SG can have inbound from EC2 IP rather than VPC CIDR for more security

upvoted 1 times

 **maggie135** 8 months, 4 weeks ago

Selected Answer: B

VPC peering uses AWS network.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: B

By configuring a VPC peering connection between VPC A and VPC B, you can establish private and secure communication between the EC2 instance in VPC A and the database in VPC B. VPC peering allows traffic to flow between the two VPCs using private IP addresses, without the need for public IP addresses or exposing the database to the internet.

Option A is not the best solution as it requires allowing all traffic from the public IP address of the application server, which can be less secure.

Option C involves making the DB instance publicly accessible, which introduces security risks by exposing the database directly to the internet.

Option D adds unnecessary complexity by launching an additional EC2 instance in VPC B and proxying all requests through it, which is not the most efficient and secure approach in this scenario.

upvoted 4 times

 **joechen2023** 9 months, 2 weeks ago

Selected Answer: B

I don't like A because the security group setting is wrong as it set up to allow all public IP addresses. If the security group setting is correct, then I will go for A

I don't like B because it needs to set up security group as well on top of peering.

for exam purpose only, I will go with the least worst choice which is B

upvoted 1 times

 **Bmarodi** 9 months, 2 weeks ago

Selected Answer: A

The keywords are: "access MOST securely", hence the option A meets these requirements.

upvoted 1 times

 **smartegnine** 9 months, 2 weeks ago

Selected Answer: A

Each VPC security group rule makes it possible for a specific source to access a DB instance in a VPC that is associated with that VPC security group. The source can be a range of addresses (for example, 203.0.113.0/24), or another VPC security group.

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

upvoted 1 times

 **MostafaWardany** 9 months, 3 weeks ago

Selected Answer: B

Most secure = VPC peering

upvoted 1 times

 **Bmarodi** 10 months ago

Selected Answer: B

I vote for option B.

upvoted 1 times

 **Piccalo** 10 months ago

Selected Answer: B

BBBB. A is not secure

upvoted 1 times

Question #232

Topic 1

A company runs demonstration environments for its customers on Amazon EC2 instances. Each environment is isolated in its own VPC. The company's operations team needs to be notified when RDP or SSH access to an environment has been established.

- A. Configure Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected.
- B. Configure the EC2 instances with an IAM instance profile that has an IAM role with the AmazonSSMManagedInstanceCore policy attached.
- C. Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state.
- D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

Correct Answer: C

Community vote distribution



✉️ **cookieMr** Highly Voted 9 months ago

Selected Answer: C

By publishing VPC flow logs to CloudWatch Logs and creating metric filters to detect RDP or SSH access, the operations team can configure an CloudWatch metric alarm to notify them when the alarm is triggered. This will provide the desired notification when RDP or SSH access to an environment is established.

Option A is incorrect because CloudWatch Application Insights is not designed for detecting RDP or SSH access.

Option B is also incorrect because configuring an IAM instance profile with the AmazonSSMManagedInstanceCore policy does not directly address the requirement of notifying the operations team when RDP or SSH access occurs.

Option D is wrong because configuring an EventBridge rule to listen for EC2 Instance State-change Notification events and using an SNS topic as a target will notify the operations team about changes in the instance state, such as starting or stopping instances. However, it does not specifically detect or notify when RDP or SSH access is established, which is the requirement stated in the question.

upvoted 11 times

✉️ **Vickysss** Highly Voted 1 year, 2 months ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>

upvoted 8 times

✉️ **NitiATOS** 1 year, 1 month ago

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#flow-log-example-accepted-rejected>

Adding this to support that VPC flow logs can be used to capture Accepted or Rejected SSH and RDP traffic.

upvoted 3 times

✉️ **ruqui** 10 months ago

I don't think C would be an acceptable solution ... the request is to be notified WHEN a SSH and/or RDP connection is established so it requires real-time monitoring and that is something the C solution does not provide ... I would select A as a correct answer

upvoted 1 times

✉️ **pentium75** Most Recent 2 months, 2 weeks ago

Selected Answer: C

C sounds complex, but is the only answer that can work.

Not A - Application Insights has nothing to do with SSH/RDP access to the OS; also we need a notification, not an OpsItem

Not B - Just attaching a role does not create a notification

Not D - Establishing SSH/RDP access is not a "state change" that would trigger this

upvoted 2 times

✉️ **pentium75** 2 months, 4 weeks ago

Selected Answer: C

A bit clueless here. AWS-recommended approach involves the CloudWatch Logs Agent on each EC2 instance, but that is not involved in any of the answers.

A: Sounds good at first read, but "CloudWatch Application Insights" cannot detect RDP or SSH access.

B: Would allow RDP or SSH access via Systems Manager, but would NOT prevent access without Systems Manager; also we'd need to configure notifications in Systems Manager which is not mentioned here.

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

C: Could work but it seems overkill to capture VPC flow logs just to detect SSH and RDP traffic. Also it is not real-time, and it's unclear how and when exactly the state transitions and notifications will be triggered. At best you'd get notification few minutes AFTER (not "when") "access has been established". Still, it has most similarity with the recommended approach to detect failed connections:
<https://aws.amazon.com/tr/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>

D: Won't work because establishment of a connection is not an instance state change.

upvoted 2 times

 **Ruffyit** 4 months ago

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#flow-log-example-accepted-rejected>

Adding this to support that VPC flow logs can be used to capture Accepted or Rejected SSH and RDP traffic.

upvoted 1 times

 **TariqKipkemei** 6 months ago

Selected Answer: C

Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state

upvoted 1 times

 **Bmarodi** 9 months, 2 weeks ago

Selected Answer: C

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to the following locations: Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose. After you create a flow log, you can retrieve and view the flow log records in the log group, bucket, or delivery stream that you configured.

Flow logs can help you with a number of tasks, such as:

Diagnosing overly restrictive security group rules

Monitoring the traffic that is reaching your instance

Determining the direction of the traffic to and from the network interfaces

Ref link: <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

upvoted 2 times

 **cokutan** 9 months, 3 weeks ago

Selected Answer: C

seems like c:

<https://aws.amazon.com/tr/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

This link does not mention VPC flow logs at all.

upvoted 1 times

 **ChrisAn** 9 months, 3 weeks ago

Selected Answer: D

D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic. This setup allows the EventBridge rule to capture instance state change events, such as when RDP or SSH access is established. The rule can then send notifications to the specified SNS topic, which is subscribed by the operations team.

upvoted 2 times

 **markw92** 9 months, 1 week ago

D is wrong. EC2 instance state change is only for pending, running etc. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-instance-state-changes.html> you can't have state change of ssh or rdp.

upvoted 1 times

 **datz** 11 months, 3 weeks ago

Selected Answer: C

C:

<https://www.youtube.com/watch?v=KAe3Eju59OU>

upvoted 1 times

 **Abhineet9148232** 1 year ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>

upvoted 1 times

 **bullrem** 1 year, 2 months ago

Selected Answer: A

A. Configuring Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected would be the most appropriate solution in this scenario. This would allow the operations team to be notified when RDP or SSH access has been established and provide them with the necessary information to take action if needed. Additionally, Amazon CloudWatch Application Insights would allow for monitoring and troubleshooting of the system in real-time.

upvoted 1 times

Training4aBetterLife 1 year, 2 months ago

Selected Answer: C

EC2 Instance State-change Notifications are not the same as RDP or SSH established connection notifications. Use Amazon CloudWatch Logs to monitor SSH access to your Amazon EC2 Linux instances so that you can monitor rejected (or established) SSH connection requests and take action.

upvoted 4 times

alexleely 1 year, 2 months ago

Selected Answer: A

The Answer can be A or C depending on the requirement if it requires real-time notification.

A: Allows the operations team to be notified in real-time when access is established, and also provides visibility into the access events through the OpsItems.

C: The logs will need to be analyzed and metric filters applied to detect access, and then the alarm will trigger based on that analysis. This method could have a delay in providing notifications. Thus, not the best solution if real-time notification is required.

Why not D: RDP or SSH access does not cause an EC2 instance to have a state change. The state change events that Amazon EventBridge can listen for include stopping, starting, and terminated instances, which do not apply to RDP or SSH access. But RDP or SSH connection to an EC2 instance does generate an event in the system, such as a log entry which can be used to notify the Operation team. Since its a log, you would require a service that monitors logs like CloudTrail, VPC Flow logs, or AWS Systems Manager Session Manager.

upvoted 3 times

JayBee65 1 year, 2 months ago

I completely agree with the logic here, but I'm thinking C, since I believe you will need to "Create required metric filters" in order to detect RDP or SSH access, and this is not specified in the question, see <https://docs.aws.amazon.com/systems-manager/latest/userguide/OpsCenter-create-OpsItems-from-CloudWatch-Alarms.html>

upvoted 2 times

owlminus 1 year, 2 months ago

Selected Answer: C

It's C fam. RDP or SSH connections won't change the state of the EC2 instance, so D doesn't make sense.

upvoted 4 times

forzadejan 1 year, 2 months ago

D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

EC2 instances sends events to the EventBridge when state change occurs, such as when a new RDP or SSH connection is established, you can use EventBridge to configure a rule that listens for these events and trigger an action, like sending an email or SMS, when the connection is detected. The operations team can be notified by subscribing to the Amazon Simple Notification Service (Amazon SNS) topic, which can be configured as the target of the EventBridge rule.

upvoted 3 times

alanp 1 year, 2 months ago

Are state changes pending:

- running
- stopping
- stopped
- shutting-down
- terminated

<https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>

upvoted 2 times

mhmt4438 1 year, 2 months ago

Selected Answer: D

Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic. This approach allows you to set up a rule that listens for state change events on the EC2 instances, specifically for when RDP or SSH access is established, and trigger a notification via Amazon SNS to the operations team. This way they will be notified when RDP or SSH access to an environment has been established.

upvoted 3 times

CapJackSparrow 1 year ago

um, isn't "EC2 Instance State-change" like running, terminated, or stopped?

upvoted 2 times

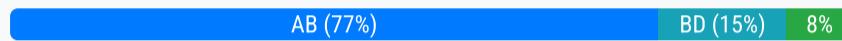
Question #233

Topic 1

A solutions architect has created a new AWS account and must secure AWS account root user access.

Which combination of actions will accomplish this? (Choose two.)

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Correct Answer: AB
Community vote distribution


Ruffyt 4 months ago

Ensure the root user uses a strong password. Enable multi-factor authentication to the root user.

upvoted 1 times

TariqKipkemei 6 months ago

Selected Answer: AB

Ensure the root user uses a strong password. Enable multi-factor authentication to the root user.

upvoted 1 times

cookieMr 9 months ago

Selected Answer: AB

A. Setting a strong password for the root user is an essential security measure to prevent unauthorized access.

B. Enabling MFA adds an extra layer of security by requiring an additional authentication factor, such as a code from a mobile app or a hardware token, in addition to the password.

C. Root user access keys should be avoided whenever possible, and it is best to use IAM users with restricted permissions instead.

D. The root user already has unrestricted access to all resources and services in the account, so granting additional administrative permissions could increase the risk of unauthorized actions.

E. Instead, it is recommended to create IAM users with appropriate permissions and use those users for day-to-day operations, while keeping the root user secured and only using it for necessary administrative tasks.

upvoted 4 times

DiscussionMonke 9 months, 1 week ago

Selected Answer: AB

Options A & B are the CORRECT answers.

upvoted 1 times

Bmarodi 10 months ago

Selected Answer: AB

Options A & B are the right answers.

upvoted 1 times

luisgu 10 months, 3 weeks ago

Selected Answer: AB

See <https://docs.aws.amazon.com/SetUp/latest/UserGuide/best-practices-root-user.html>

upvoted 1 times

Kunj7 12 months ago

Selected Answer: AB

A and B are the correct answers:

Option A: A strong password is always required for any AWS account you create, and should not be shared or stored anywhere as there is always a risk.

Option B: This is following AWS best practice, by enabling MFA on your root user which provides another layer of security on the account and unauthorised access will be denied if the user does not have the correct password and MFA.

upvoted 1 times

 **Whericanstart** 1 year ago

Selected Answer: AB

AB are the right answers.

upvoted 1 times

 **fkie4** 1 year ago

This is probably the hardest question in AWS history

upvoted 3 times

 **ProfXsamson** 1 year, 1 month ago

Selected Answer: AB

AB is the only feasible answer here.

upvoted 3 times

 **bullrem** 1 year, 2 months ago

Selected Answer: BE

B. Enabling multi-factor authentication for the root user provides an additional layer of security to ensure that only authorized individuals are able to access the root user account.

E. Applying the required permissions to the root user with an inline policy document ensures that the root user only has the necessary permissions to perform the necessary tasks, and not any unnecessary permissions that could potentially be misused.

upvoted 2 times

 **bullrem** 1 year, 2 months ago

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

upvoted 1 times

 **bullrem** 1 year, 2 months ago

The other options are not sufficient to secure the root user access because:

A. A strong password alone is not enough to protect against potential security threats such as phishing or brute force attacks.

C. Storing the root user access keys in an encrypted S3 bucket does not address the root user's authentication process.

D. Adding the root user to a group with administrative permissions does not address the root user's authentication process and does not provide an additional layer of security.

upvoted 1 times

 **[Removed]** 11 months, 2 weeks ago

Strong passwords + multi factor is the counter to brute force...

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

E is wrong because you can't attach permissions or policies to the root user.

A is right because MFA alone won't help too much if the password is "123".

upvoted 3 times

 **Pindol** 1 year, 2 months ago

Selected Answer: AB

AB obviously

upvoted 1 times

 **david76x** 1 year, 2 months ago

Selected Answer: AB

Root user already has admin, so D is not correct

upvoted 1 times

 **Aninina** 1 year, 2 months ago

Selected Answer: AB

AB are correct

upvoted 1 times

 **wmp7039** 1 year, 2 months ago

Selected Answer: AB

D is incorrect as root user already has full admin access.

upvoted 2 times

 **swolfgang** 1 year, 2 months ago

Selected Answer: AB

D. Add the root user to a group containing administrative permissions. >> its not about security, actually its unsecure so >> a&B

upvoted 1 times

 **raf123123** 1 year, 2 months ago

Selected Answer: BD

BD is correct

upvoted 2 times

✉ **pentium75** 2 months, 4 weeks ago

D is wrong because the root user is outside of IAM, thus you can't put him into a group. Also he does not need "administrative permissions" as he has those anyway.

upvoted 1 times

✉ **awsgeek75** 2 months, 3 weeks ago

root user is literally the super admin account. What more permissions could you possibly give to the root user by adding it to admin group?

upvoted 1 times

Question #234

Topic 1

A company is building a new web-based customer relationship management application. The application will use several Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS) volumes behind an Application Load Balancer (ALB). The application will also use an Amazon Aurora database. All data for the application must be encrypted at rest and in transit.

Which solution will meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) certificates on the ALB to encrypt data in transit. Use AWS Certificate Manager (ACM) to encrypt the EBS volumes and Aurora database storage at rest.
- B. Use the AWS root account to log in to the AWS Management Console. Upload the company's encryption certificates. While in the root account, select the option to turn on encryption for all data at rest and in transit for the account.
- C. Use AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and Aurora database storage at rest. Attach an AWS Certificate Manager (ACM) certificate to the ALB to encrypt data in transit.
- D. Use BitLocker to encrypt all data at rest. Import the company's TLS certificate keys to AWS Key Management Service (AWS KMS) Attach the KMS keys to the ALB to encrypt data in transit.

Correct Answer: C

Community vote distribution

C (100%)

 **cookieMr**  9 months ago

Selected Answer: C

AWS KMS can be used to encrypt the EBS and Aurora database storage at rest.

ACM can be used to obtain an SSL/TLS certificate and attach it to the ALB. This encrypts the data in transit between the clients and the ALB.

A is incorrect because it suggests using ACM to encrypt the EBS, which is not the correct service for encrypting EBS.

B is incorrect because relying on the AWS root account and selecting an option in the AWS Management Console to enable encryption for all data at rest and in transit is not a valid approach.

D is incorrect because BitLocker is not a suitable solution for encrypting data in AWS services. It is primarily used for encrypting data on Windows-based operating systems. Additionally, importing TLS certificate keys to AWS KMS and attaching them to the ALB is not the recommended approach for encrypting data in transit.

upvoted 7 times

 **Ruffyit**  4 months ago

To encrypt data at rest, AWS Key Management Service (AWS KMS) can be used to encrypt EBS volumes and Aurora database storage.

To encrypt data in transit, an AWS Certificate Manager (ACM) certificate can be attached to the Application Load Balancer (ALB) to enable HTTPS and TLS encryption.

upvoted 1 times

 **TariqKipkemei** 6 months ago

Selected Answer: C

Use AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and Aurora database storage at rest. Attach an AWS Certificate Manager (ACM) certificate to the ALB to encrypt data in transit

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: C

C is the best answer.

To encrypt data at rest, AWS Key Management Service (AWS KMS) can be used to encrypt EBS volumes and Aurora database storage.

To encrypt data in transit, an AWS Certificate Manager (ACM) certificate can be attached to the Application Load Balancer (ALB) to enable HTTPS and TLS encryption.

upvoted 1 times

 **MAMADOU9** 9 months, 2 weeks ago

Selected Answer: C

Option C it's correct

upvoted 1 times

 **Bmarodi** 10 months ago

Selected Answer: C

Option C fulfills the requirements.

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: C

C is correct ,A REVERSES the work of each service.

upvoted 3 times

 **Aninina** 1 year, 2 months ago

Selected Answer: C

C is correct!

upvoted 3 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: C

c is correct answer

upvoted 2 times

Question #235

Topic 1

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

- A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.
- B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Correct Answer: C

Community vote distribution



✉ **aakashkumar1999** Highly Voted 1 year, 1 month ago

Selected Answer: C

C : because we need SCT to convert from Oracle to PostgreSQL, and we need memory optimized machine for databases not compute optimized.
upvoted 11 times

✉ **hissein** 6 months, 2 weeks ago

why it is memory optimized and not compute optimized machine ?
upvoted 5 times

✉ **pentium75** 2 months, 4 weeks ago

Maybe it doesn't matter, but in D we create a table mapping only for "the largest tables" while obviously we need "all tables" as in C.
upvoted 5 times

✉ **Guru4Cloud** 6 months, 2 weeks ago

A memory-optimized replication instance is recommended because the database has a high number of reads and writes. Memory-optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.
upvoted 14 times

✉ **hissein** 5 months, 3 weeks ago

thank you
upvoted 2 times

✉ **TechStuff** Most Recent 1 month ago

B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.

This approach leverages AWS DataSync for the initial data migration, which is optimized for high-speed transfer of large amounts of data. Then, AWS DMS is used to create a replication task with full load plus change data capture (CDC), ensuring ongoing synchronization between the on-premises Oracle database and Amazon Aurora PostgreSQL. By selecting all tables, the migration process ensures that all applications can continue to read from and write to the database without interruption during the migration period.

upvoted 1 times

✉ **MrPCarrot** 1 month, 1 week ago

Answer is C - AWS Schema Conversion Tool (AWS SCT) supports heterogeneous database migrations by automatically converting the source database schema and a majority of the custom code to a format compatible with the target database.

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Selected Answer: C

Has to be SCT + DMS for all the tables so C is the choice. Why do you need SCT? Read this:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-data-from-an-on-premises-oracle-database-to-aurora-postgresql.html>

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

AB-> DataSync has nothing to do with DB Migration (<https://aws.amazon.com/datasync/>)
D: Only migrates the largest table

I think these questions are more for seeing how much of AWS product catalogue can you remember efficiently with associated features. Afterall AWS SA is also a salesperson for the right product! I now look at product cheat-sheets to look them up at work.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Selected Answer: C
Oracle -> PostgreSQL, we need SCT, thus A and B are out.
D maps only "the largest tables" but we need all tables
upvoted 3 times

 **ansagr** 3 months, 2 weeks ago

Selected Answer: C
Another reason to rule out D is because it states "a table mapping to select the largest tables", whereas selecting all tables (as stated in option C) in the table mapping is necessary to ensure a comprehensive migration.
upvoted 4 times

 **Ruffyit** 4 months ago

because we need SCT to convert from Oracle to PostgreSQL, and we need memory optimized machine for databases not compute optimized.
A memory-optimized replication instance is recommended because the database has a high number of reads and writes. Memory-optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.

upvoted 2 times

 **Po_chih** 5 months, 3 weeks ago

Selected Answer: C
because we need SCT to convert from Oracle to PostgreSQL, and we need memory optimized machine for databases not compute optimized.
<https://repost.aws/zh-Hant/knowledge-center/dms-optimize-aws-sct-performance>
upvoted 1 times

 **TariqKipkemei** 6 months ago

Selected Answer: C
Oracle database to Amazon Aurora PostgreSQL = AWS Schema Conversion Tool
High number of reads and writes = memory optimized replication instance
upvoted 2 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: C
A memory-optimized replication instance is recommended because the database has a high number of reads and writes. Memory-optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.
upvoted 1 times

 **_d1rk_** 7 months, 1 week ago

Selected Answer: C
DataSync is for file-level synch, so A and B can be excluded. C is better than D because memory-optimized instances are recommended to handle the high number of reads and writes
upvoted 2 times

 **ukivanlamipi** 7 months, 1 week ago

Selected Answer: A
why not a? only capture the change is sufficient
upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

Oracle -> PostgreSQL requires SCT
upvoted 1 times

 **Mmmmmmkkkk** 8 months, 3 weeks ago

Bbbbbbb
upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: C
The AWS SCT is used to convert the schema and code of the Oracle database to be compatible with Aurora PostgreSQL. AWS DMS is utilized to migrate the data from the Oracle database to Aurora PostgreSQL. Using a memory-optimized replication instance is recommended to handle the high number of reads and writes during the migration process.
By creating a full load plus CDC replication task, the initial data migration is performed, and ongoing changes in the Oracle database are continuously captured and applied to the Aurora PostgreSQL database. Selecting all tables for table mapping ensures that all the applications writing to the same tables are migrated.

Option A & B are incorrect because using AWS DataSync alone is not sufficient for database migration and data synchronization.

Option D is incorrect because using a compute optimized replication instance is not the most suitable choice for handling the high number of reads and writes.

upvoted 2 times

 **omoakin** 10 months ago

BBBBBBBBBBBBBBB

upvoted 2 times

 **SimiTik** 11 months, 1 week ago

B chatgpt

upvoted 2 times

 **KZM** 1 year, 1 month ago

DMS+SCT for Oracle to Aurora PostgreSQL migration

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-oracle-database-to-aurora-postgresql-using-aws-dms-and-aws-sct.html>

upvoted 2 times

Question #236

Topic 1

A company has a three-tier application for image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance for the application layer, and a third EC2 instance for a MySQL database. A solutions architect must design a scalable and highly available solution that requires the least amount of change to the application.

Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer. Use AWS Lambda functions for the application layer. Move the database to an Amazon DynamoDB table. Use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS DB instance with multiple read replicas to serve users' images.
- C. Use Amazon S3 to host the front-end layer. Use a fleet of EC2 instances in an Auto Scaling group for the application layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images.

Correct Answer: A

Community vote distribution



✉️ **PDR** 1 year, 1 month ago

Selected Answer: B

B and D very similar with D being the 'best' solution but it is not the one that requires the least amount of development changes as the application would need to be changed to store images in S3 instead of DB

upvoted 12 times

✉️ **pentium75** 2 months, 4 weeks ago

B is wrong because single "RDS DB instance" is not HA.

No one says that the images are currently stored in S3. Also the requirement is "least amount of change [not "no change"] to the application".

upvoted 5 times

✉️ **Aninina** 1 year, 2 months ago

Selected Answer: D

for "Highly available": Multi-AZ &

for "least amount of changes to the application": Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring

upvoted 8 times

✉️ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: D

A: Requires changing EC2 application to Lambda. Seems like a big change

B: RDS DB is not best option for serve images and also single instance isn't HA

C: Memory optimised instance is not HA

D: Multi-AZ EBS is lift and shift for EC2 front-end and app later. RDS Multi AZ is HA. S3 for static images is best performance/scalability/availability.

upvoted 3 times

✉️ **ansagr** 3 months, 2 weeks ago

Selected Answer: D

Using Amazon RDS for serving images might not be the optimal solution, as RDS is more suitable for storing structured data in a relational database rather than BLOBs like images. Storing and serving images can be more efficiently handled by object storage services like Amazon S3.

upvoted 1 times

✉️ **Ruffyit** 4 months ago

Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images

upvoted 1 times

✉️ **rlamberti** 5 months ago

Option B - DB is not a good option to store images. Read replicas won't improve HA for write, only scales reading IO. Therefore no true HA achieved.

D is the goal for me.

upvoted 1 times

✉ **TariqKipkemei** 6 months ago

Selected Answer: D

Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images

upvoted 2 times

✉ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

Use Elastic Beanstalk load-balanced environments for the web and app tiers. This provides auto scaling and high availability with minimal effort. Move the database to RDS Multi-AZ. This handles scaling reads and storage, and provides HA with automated failover.

Use S3 for serving user images. S3 is highly scalable and durable storage.

The application code remains unchanged using this approach.

upvoted 2 times

✉ **Mia2009687** 9 months ago

Selected Answer: A

AWS Elastic Beanstalk makes it even easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

I don't quite understand why people choose D.

upvoted 1 times

✉ **cookieMr** 9 months ago

Selected Answer: D

By using load-balanced Multi-AZ AWS EBS, you achieve scalability and high availability for both layers without requiring significant changes to the application. Moving the DB to an RDS Multi-AZ DB ensures high availability and automatic failover. Storing and serving users' images through S3 provides a scalable and highly available solution.

A is incorrect because using S3 for the front-end layer and Lambda for the application layer would require significant changes to the application architecture. Moving the DB to DynamoDB would require rewriting the DB-related code.

B is incorrect because using load-balanced Multi-AZ AWS EBS environments and an RDS DB with read replicas for serving images would be a more suitable solution. RDS with read replicas can handle the image-serving workload more efficiently than using S3 for this purpose.

C is incorrect because using S3 for the front-end layer and an ASG of EC2 for the application layer would require modifying the application architecture. Storing and serving images from a memory-optimized EC2 type may not be the most efficient and scalable approach compared to using S3.

upvoted 3 times

✉ **markw92** 9 months, 1 week ago

"least amount of change to the application." - A has lots of changes, completely revamping the application and lots of new pieces. D is closest with only addition of s3 to store images which is right move. You do not want images to store in any database anyway.

upvoted 3 times

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

Thats what I was thinking, but the question doesn't mention anything about storing users' images anywhere. Are we supposed to just assume that they wanted to store the images in a DB even though that is a bad idea?

upvoted 1 times

✉ **Bmarodi** 10 months ago

Selected Answer: D

Option D meets the requirements.

upvoted 1 times

✉ **Grace83** 1 year ago

D is correct

upvoted 2 times

✉ **focus_23** 1 year, 1 month ago

Selected Answer: D

RDS multi AZ.

upvoted 2 times

✉ **wmp7039** 1 year, 2 months ago

Selected Answer: D

D is correct as application changes needs to me minimal

upvoted 2 times

✉ **mhmt4438** 1 year, 2 months ago

Selected Answer: D

Correct answer is D

upvoted 2 times

 **Morinator** 1 year, 2 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/24840-exam-aws-certified-solutions-architect-associate-saa-c02/>

Please ExamTopics, review your own answers

upvoted 4 times

Question #237

Topic 1

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both VPCs are in separate AWS accounts. The network administrator needs to design a solution to configure secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

- A. Set up a VPC peering connection between VPC-A and VPC-B.
- B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
- C. Attach a virtual private gateway to VPC-B and set up routing from VPC-A.
- D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A.

Correct Answer: A

Community vote distribution



LuckyAro Highly Voted 1 year, 1 month ago

Selected Answer: A

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
upvoted 13 times

cookieMr Highly Voted 9 months ago

Selected Answer: A

A VPC peering connection allows secure communication between instances in different VPCs using private IP addresses without the need for internet gateways, VPN connections, or NAT devices. By setting it up, the application running in VPC-A can directly access the EC2 in VPC-B without going through the public internet or any single point of failure.

B is incorrect because VPC gateway endpoints are used for accessing S3 or DynamoDB from a VPC without going over the internet. They are not designed for establishing connectivity between EC2 instances in different VPCs.

C is incorrect because it would require configuring a VPN connection between the VPCs. This would introduce additional complexity and potential single points of failure.

D is incorrect because creating a private VIF and adding routes would be applicable for establishing a direct connection between on-premises infrastructure and VPC-B using Direct Connect, but it is not suitable for the scenario of communication between EC2 instances in separate VPCs within different AWS accounts.

upvoted 8 times

Faridtnx Most Recent 1 week, 1 day ago

Selected Answer: A

You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. Peering within the same AZ is free of charge.

upvoted 1 times

lostmagnet001 1 month, 2 weeks ago

Selected Answer: A

I get a little confused about B and A but, because, with a VPC endpoint in B it will work too access from A.

upvoted 1 times

pentium75 2 months, 4 weeks ago

Selected Answer: A

B is wrong because "VPC gateway endpoint" is for S3 or DynamoDB, not EC2

C is overkill, would require a second gateway in VPC-A, not be HA and have limited bandwidth

D is wrong because VIF is for Direct Connect, has nothing to do with VPC-to-VPC communication

upvoted 3 times

Ruffyit 4 months ago

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

A. Set up a VPC peering connection between VPC-A and VPC-B
upvoted 1 times

 **MNotABot** 8 months, 1 week ago

<https://www.bing.com/search?pglt=41&q=can+we+do+VPC+peering+across+AWS+accounts&cvid=48a8ceec85a429c9ddd698b01055890&aqs=edge..69i57j0l8j69i11004.10897j0j1&FORM=ANNAB1&PC=LCTS>
upvoted 1 times

 **Anmol_1010** 9 months, 2 weeks ago

D, VPC PEERINGVIS IN SAME ACCOUNT
upvoted 1 times

 **im6h** 9 months, 1 week ago

No, VPC Peering can use across account.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

upvoted 3 times

 **omoakin** 10 months ago

DDDDDDDDDDDDDDDD
upvoted 2 times

 **omoakin** 10 months ago

This is the only viable solution
Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A
upvoted 1 times

 **michellemeloc** 10 months, 1 week ago

Selected Answer: A

"You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account."

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

upvoted 4 times

 **PDR** 1 year, 1 month ago

Selected Answer: A

correct answer is A and as mentioned by JayBee65 below, key reason being that solution should not have a single point of failure and bandwidth restrictions

the following paragraph is taken from the AWS docs page linked below that backs this up

"AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck."

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

upvoted 2 times

 **LuckyAro** 1 year, 2 months ago

Selected Answer: B

A VPC endpoint gateway to the EC2 Instance is more specific and more secure than forming a VPC peering that exposes the whole of the VPC infrastructure just for one connection.

upvoted 2 times

 **JayBee65** 1 year, 2 months ago

Your logic is correct but security is not a requirement here - the requirements are "The connectivity should not have a single point of failure or bandwidth concerns." A VPC gateway endpoint would form a single point of failure, so B is incorrect, (and C and D are incorrect for the same reason, they create single points of failure).

upvoted 4 times

 **pentium75** 2 months, 4 weeks ago

B is about a Gateway endpoint, which can be used to connect to S3 or DynamoDB, NOT to another EC2 instance.

upvoted 1 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **Aninina** 1 year, 2 months ago

Selected Answer: A

VPC peering allows resources in different VPCs to communicate with each other as if they were within the same network. This solution would establish a direct network route between VPC-A and VPC-B, eliminating the need for a single point of failure or bandwidth concerns.

upvoted 1 times

 **waiyiu9981** 1 year, 2 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/27763-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 4 times

Question #238

Topic 1

A company wants to experiment with individual AWS accounts for its engineer team. The company wants to be notified as soon as the Amazon EC2 instance usage for a given month exceeds a specific threshold for each account.

What should a solutions architect do to meet this requirement MOST cost-effectively?

- A. Use Cost Explorer to create a daily report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
- B. Use Cost Explorer to create a monthly report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
- C. Use AWS Budgets to create a cost budget for each account. Set the period to monthly. Set the scope to EC2 instances. Set an alert threshold for the budget. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.
- D. Use AWS Cost and Usage Reports to create a report with hourly granularity. Integrate the report data with Amazon Athena. Use Amazon EventBridge to schedule an Athena query. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.

Correct Answer: B

Community vote distribution

C (96%) 4%

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

Selected Answer: C

AWS Budgets allows you to create budgets for your AWS accounts and set alerts when usage exceeds a certain threshold. By creating a budget for each account, specifying the period as monthly and the scope as EC2 instances, you can effectively track the EC2 usage for each account and be notified when a threshold is exceeded. This solution is the most cost-effective option as it does not require additional resources such as Amazon Athena or Amazon EventBridge.

upvoted 10 times

 **Ruffyit** Most Recent 4 months ago

AWS Budgets allows you to create budgets for your AWS accounts and set alerts when usage exceeds a certain threshold. By creating a budget for each account, specifying the period as monthly and the scope as EC2 instances, you can effectively track the EC2 usage for each account and be notified when a threshold is exceeded. This solution is the most cost-effective option as it does not require additional resources such as Amazon Athena or Amazon EventBridge.

upvoted 1 times

 **vijaykamal** 5 months, 4 weeks ago

Selected Answer: C

Option A and Option B suggest using Cost Explorer to create reports and send notifications. While Cost Explorer is useful for analyzing costs, it does not provide the real-time alerting capability that AWS Budgets offers.

Option D suggests using AWS Cost and Usage Reports integrated with Amazon Athena and Amazon EventBridge, which can be a more complex and potentially costlier solution compared to AWS Budgets for this specific use case. It's also more suitable for fine-grained, custom analytics rather than straightforward threshold-based alerts.

upvoted 3 times

 **TariqKipkemei** 6 months ago

Selected Answer: C

AWS Budgets was designed to handle this scenario.

upvoted 2 times

 **Undisputed** 8 months ago

Selected Answer: C

Use AWS Budgets to create a cost budget for each account. Set the period to monthly. Set the scope to EC2 instances. Set an alert threshold for the budget. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: C

By creating a cost budget for each account, specifying the period as monthly and scoping it to EC2, you can track and monitor the costs associated with EC2 specifically. Set an alert threshold in the budget, which will trigger a notification when the specified threshold is exceeded. Configure an SNS to receive the notification, which can be subscribed to by the company to receive immediate alerts.

A and B are not the most cost-effective solutions as they involve using Cost Explorer to create reports, which may not provide real-time notifications when the threshold is exceeded. Additionally, A. suggests using a daily report, while B. suggests using a monthly report, which may not provide the desired level of granularity for immediate notifications.

D involves using Cost and Usage Reports with Athena and EventBridge. This solution provides more flexibility and data analysis capabilities, it is more complex and may incur additional costs for using Athena and generating hourly reports.

upvoted 1 times

 **Samuel03** 1 year, 1 month ago

Selected Answer: D

I go with D. It says "as soon as", "daily" reports seems to be a bit longer time frame to wait in my opinion.

upvoted 1 times

 **Samuel03** 1 year, 1 month ago

Actually, I take that back. It clearly says "Cost effective."

upvoted 4 times

 **Bofi** 1 year ago

Athena can only be used in s3, that is enough to discard D

upvoted 2 times

 **alexleely** 1 year, 2 months ago

C: AWS Budgets allows you to set a budget for costs and usage for your accounts and you can set alerts when the budget threshold is exceeded in real-time which meets the requirement.

Why not B: B would be the most cost-effective if the requirements didn't ask for real-time notification. You would not incur additional costs for the daily or monthly reports and the notifications. But doesn't provide real-time alerts.

upvoted 4 times

 **mp165** 1 year, 2 months ago

Selected Answer: C

Agree...C

upvoted 2 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: C

Answer is C

upvoted 1 times

 **venice1234** 1 year, 2 months ago

Selected Answer: C

<https://aws.amazon.com/getting-started/hands-on/control-your-costs-free-tier-budgets/>

upvoted 1 times

 **Morinator** 1 year, 2 months ago

Selected Answer: C

AWS budget IMO, it's done for it

upvoted 2 times

Question #239

Topic 1

A solutions architect needs to design a new microservice for a company's application. Clients must be able to call an HTTPS endpoint to reach the microservice. The microservice also must use AWS Identity and Access Management (IAM) to authenticate calls. The solutions architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x.

Which solution will deploy the function in the MOST operationally efficient way?

- A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.
- B. Create a Lambda function URL for the function. Specify AWS_IAM as the authentication type.
- C. Create an Amazon CloudFront distribution. Deploy the function to Lambda@Edge. Integrate IAM authentication logic into the Lambda@Edge function.
- D. Create an Amazon CloudFront distribution. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

Correct Answer: A

Community vote distribution

A (65%)

B (35%)

 **mhmt4438**  1 year, 2 months ago

Selected Answer: A

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API. This option is the most operationally efficient as it allows you to use API Gateway to handle the HTTPS endpoint and also allows you to use IAM to authenticate the calls to the microservice. API Gateway also provides many additional features such as caching, throttling, and monitoring, which can be useful for a microservice.

upvoted 19 times

 **hro**  1 week, 3 days ago

I think from a decoupling and separation of concerns A is the answer. You don't want to have a heavy reliance on the Lambda function with you have specific services for what is being required.
there is operationally efficient incorrect and operationally efficient correct.
So A is the best answer.

upvoted 1 times

 **bujuman** 1 month ago

Selected Answer: B

According to this statement "MOST operationally efficient way" and the following link related to Lambda Function URL security:
<https://docs.aws.amazon.com/lambda/latest/dg/urls-auth.html>

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

I originally voted B but after reading this article, I am not sure if A is wrong or is just badly worded.
If A actually said "Configure the [authorization] method to use the Lambda function" then it would be way more logical than B but this could be intentional. Although I think this is AWS test not IELTS so picking right answers based on small word mistakes is not the intention!

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

upvoted 2 times

 **upliftinghut** 2 months, 2 weeks ago

Selected Answer: B

A&B are all good. The requirement is most operationally efficient so B is faster. In real life, I won't risk B for production, dev & test makes sense but no production please

upvoted 1 times

 **upliftinghut** 2 months, 2 weeks ago

Reference link why B is here: <https://aws.amazon.com/blogs/aws/announcing-aws-lambda-function-urls-built-in-https-endpoints-for-single-function-microservices/>

upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

Selected Answer: B

I think this question has 2 answers as both A and B will work. However, B is more operationally efficient due to Lambda function URL and direct support for AWS_IAM as the auth type for this setup.

<https://docs.aws.amazon.com/lambda/latest/dg/urls-auth.html#urls-auth-iam>

C, D are not operationally efficient and GO is not supported on Lambda@Edge or CloudFront functions. Even if AWS start supporting it, the operational efficiency will increase because of CloudFront

upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

* meant to say "operational efficiency will decrease" because of CloudFront

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Selected Answer: B

We know that the application provides "an HTTPS endpoint" but we don't even know whether it is a REST API. The question is not mentioning any other requirements besides IAM authentication, which can be handled by Lambda alone.

A would work, but would be an additional processing step (lowering operational efficiency). It would also provide benefits but none of those is asked for in the question.

C and D is wrong because Lambda@Edge does not support Go.

upvoted 2 times

 **meowruki** 3 months, 3 weeks ago

Selected Answer: A

Options B, C, and D involve using Lambda function URLs or CloudFront, but they lack the full set of features provided by API Gateway, such as built-in IAM authentication, throttling, and other API management capabilities.

upvoted 1 times

 **google_platform_team** 4 months ago

Selected Answer: B

I think it is B - most operationally efficient. A is a better answer, but more complicated.

upvoted 1 times

 **swap001** 5 months, 1 week ago

Selected Answer: B

There is no need of an additional API gateway when Lambda itself can support the need. This is more operationally efficient.

upvoted 2 times

 **OlehKom** 5 months, 3 weeks ago

Why not B? I agree that A is a nice choice, but it clearly says "MOST operationally efficient way", there is nothing said about API. B in this case suits absolutely fine, it's simpler and cheaper.

upvoted 1 times

 **TariqKipkemei** 6 months ago

Selected Answer: A

Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API. This option is the most operationally efficient as it allows you to use API Gateway to handle the HTTPS endpoint and also allows you to use IAM to authenticate the calls to the microservice. API Gateway also provides many additional features such as caching, throttling, and monitoring, which can be useful for a microservice.

upvoted 2 times

 **Smart** 7 months, 3 weeks ago

Selected Answer: B

C & D (incorrect) - what will be the origin for CDN? Plus Go is not supported. Plus for option D, IAM is not supported.

A, why develop and manage API in API GW?

Just enable Lambda function URL...

upvoted 2 times

 **Zeezie** 8 months ago

B -- MOST operationally efficient. Just look at the Lambda Create function console...

Enable function URL >

Use function URLs to assign HTTP(S) endpoints to your Lambda function.

Auth type

Choose the auth type for your function URL. >

AWS_IAM

Only authenticated IAM users and roles can make requests to your function URL.

upvoted 2 times

 **testopesto** 8 months ago

Selected Answer: B

The MOST operationally efficient way

<https://docs.aws.amazon.com/lambda/latest/dg/urls-auth.html>

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

upvoted 3 times

 **Undisputed** 8 months ago

Selected Answer: A

Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.

upvoted 1 times

Question #240

Topic 1

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

- A. Host the visualization tool on premises and query the data warehouse directly over the internet.
- B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.
- C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

Correct Answer: C

Community vote distribution



✉️ AlessandraSAA Highly Voted 1 year ago

Selected Answer: D

- A. --> No since if you access via internet you are creating egress traffic.
- B. --> It's a good choice to have both DWH and visualization in the same region to lower the egress transfer (i.e. data going egress/out of the region) but if you access over internet you might still have egress transfer.
- C. -> Valid but in this case you send out of AWS 50MB if you query the DWH instead of the visualization tool, D removes this need since puts the visualization tools in AWS with the DWH so reduces data returned out of AWS from 50MB to 500KB
- D. --> Correct, see explanation on answer C

Useful links:

AWS Direct Connect connection create a connection in an AWS Direct Connect location to establish a network connection from your premises to an AWS Region.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>

upvoted 11 times

✉️ hro 1 week, 3 days ago

I thought Direct Connect is exclusively for on-prem to VPC. Why would you use DirectConnect to connect to a service in your own Region in the AWS Cloud?

I believe C is correct.

upvoted 2 times

✉️ chickenmf 1 week, 1 day ago

Agree with you 100%

upvoted 1 times

✉️ hro Most Recent 1 week, 3 days ago

The answer is C. At no point does the question suggest that the DWH source is out of Region.

upvoted 1 times

✉️ reviewmine 1 month ago

Selected Answer: D

It's D. Host the visualization on the same region to avoid egress cost and access the tool via AWS Direct connection.

upvoted 2 times

✉️ upliftinghut 2 months, 2 weeks ago

Selected Answer: D

Leverage the existing DirectConnect so not incur data transfer charge

upvoted 1 times

✉️ Ruffyt 4 months ago

D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

upvoted 1 times

✉️ TariqKipkemei 6 months ago

Selected Answer: D

Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region

upvoted 1 times

Guru4Cloud 6 months, 2 weeks ago

Selected Answer: D

D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

upvoted 1 times

jtexam 8 months, 2 weeks ago

Selected Answer: B

by hosting in same region, you have 500kb transfer charged on internet transfer tier, 50MB charged in inter-region tier.

using direct link, both are charged in direct link tier. direct link tier is not cheap.

so i go for B

upvoted 1 times

pentium75 2 months, 4 weeks ago

We don't want "lowest cost", we want "lowest data transfer egress cost". And "data transfer egress" cost for Direct Connect is WAY lower than for Internet. (Therefor the circuit itself is expensive, but that does exist anyway.)

upvoted 1 times

Mmmmmmkkkk 8 months, 3 weeks ago

Aaaaaaaa

upvoted 1 times

cookieMr 9 months ago

Selected Answer: D

Hosting the visualization tool in the same AWS Region as the data warehouse and accessing it over a Direct Connect connection within the same Region eliminates data transfer fees and ensures low-latency, high-bandwidth connectivity.

A. Hosting the visualization tool on premises and querying the data warehouse over the internet incurs data transfer costs for every query result, as well as potential latency and bandwidth limitations.

B. Hosting the visualization tool in the same AWS Region as the data warehouse but accessing it over the internet still incurs data transfer costs for each query result.

C. Hosting the visualization tool on premises and querying the data warehouse over a Direct Connect connection within the same AWS Region incurs data transfer costs for every query result and adds complexity by requiring on-premises infrastructure.

upvoted 2 times

dexpos 1 year, 1 month ago

Selected Answer: D

D let you reduce at minimum the data transfer costs

upvoted 1 times

alexleely 1 year, 2 months ago

Selected Answer: D

D: Direct Connect connection at a location in the same Region will provide the lowest data transfer egress cost, improved performance, and lower complexity

Why it is not C is because the visualization tool is hosted on-premises, as it's not hosted in the same region as the data warehouse the data transfer between them would occur over the internet, thus, would incur in egress data transfer costs.

upvoted 4 times

markw92 9 months, 1 week ago

C option doesn't travel through internet because we have a direct connect. If you are hosting your visualization tool in same region why you need a direct connection which D has? Doesn't make sense. So, C is the right answer.

upvoted 1 times

Vickysss 1 year, 2 months ago

Selected Answer: C

<https://www.nops.io/reduce-aws-data-transfer-costs-dont-get-stung-by-hefty-egress-fees/>

upvoted 2 times

JayBee65 1 year, 2 months ago

Whilst "Direct Connect can help lower egress costs even after taking the installation costs into account. This is because AWS charges lower transfer rates." D removes the need to send the query results out of AWS and instead returns the web page, so reduces data returned from 50MB to 500KB, so D

upvoted 3 times

mhmt4438 1 year, 2 months ago

Selected Answer: D

Correct answer is D

upvoted 4 times

 **Aninina** 1 year, 2 months ago

Selected Answer: D

Should be D

<https://aws.amazon.com/directconnect/pricing/>

<https://aws.amazon.com/blogs/aws/aws-data-transfer-prices-reduced/>

upvoted 2 times

 **Morinator** 1 year, 2 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/47140-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

Question #241

Topic 1

An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.

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

- A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
- B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
- C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
- D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Correct Answer: C

Community vote distribution

C (79%) B (21%)

✉ **Steve_4542636** 1 year ago

Selected Answer: C

Multi az is not the same as multi regional
upvoted 37 times

✉ **alexleely** 1 year, 2 months ago

Selected Answer: B

B: Amazon RDS Multi-AZ feature automatically creates a synchronous replica in another availability zone and failover to the replica in the event of an outage. This will provide high availability and data durability across multiple AWS regions which fit the requirements.

Though C may sound good, it in fact requires manual management and monitoring of the replication process due to the fact that Amazon RDS read replicas are asynchronous, meaning there is a delay between the primary and read replica. Therefore, there will be a need to ensure that the read replica is constantly up-to-date and someone still has to fix any read replica errors during the replication process which may cause data inconsistency. Lastly, you still have to configure additional steps to make it fail over to the read replica.

upvoted 14 times

✉ **Rehan33** 1 year, 1 month ago

I go with option B because:
Multi-AZ is for high availability
Read replicas are for low-latency
in question they talk about available online
upvoted 4 times

✉ **awsgeek75** 2 months, 1 week ago

They also ask for multiple regions which is not covered by Multi AZ
upvoted 1 times

✉ **Mahadeva** 1 year, 2 months ago

But the question is clearly asking for Multiple Regions. Multi-AZ is not across Regions.
upvoted 21 times

✉ **alexleely** 1 year, 2 months ago

You are right, Multi-AZ is only within one Region. C would be the right answer.
upvoted 14 times

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

<https://aws.amazon.com/rds/features/multi-az/>

smartegnine 0 minutes ago Awaiting moderator approval

Selected Answer: B

In an Amazon RDS Multi-AZ deployment, Amazon RDS automatically creates a primary database (DB) instance and synchronously replicates the data to an instance in a different AZ.

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

Selected Answer: C

A - Just no
B - Multi-AZ is multiple AZs in same region, does not meet "Multiple AWS Regions" requirement
C - Meets requirements
D - Does not meet the "online ... at all times" requirement

upvoted 6 times

 **Ruffyit** 3 months, 2 weeks ago

Multi az is not the same as multi regional

upvoted 2 times

 **vijaykamal** 5 months, 4 weeks ago

Selected Answer: B

Option C, while providing a read replica in another Region, adds complexity to the architecture and may introduce some additional operational overhead compared to Multi-AZ. Cross-Region replication involves setting up and managing replication between two separate RDS instances.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

But data must be online "across multiple AWS regions"!

upvoted 2 times

 **TariqKipkemei** 6 months ago

Selected Answer: C

Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region

upvoted 2 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: C

Multi-AZ is not the same as Multi-Regional

upvoted 3 times

 **Valder21** 6 months, 3 weeks ago

can someone explain why not D

upvoted 3 times

 **pentium75** 2 months, 4 weeks ago

"Data must be online (!) across multiple AWS regions at all times (!)". Snapshots are not online.

upvoted 2 times

 **beginnercloud** 7 months ago

Selected Answer: C

key words "AWS Regions at all times" so C is correct

upvoted 1 times

 **fuzzycr** 8 months, 2 weeks ago

Selected Answer: C

key words "AWS Regions at all times"

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: C

By migrating the PostgreSQL database to an RDS for PostgreSQL DB instance and creating a read replica in another AWS Region, you can achieve data availability and online access across multiple Regions. This solution requires less operational overhead compared to managing a PostgreSQL cluster on EC2 instances (Option A) or setting up manual replication using snapshots (Option D). Additionally, Amazon RDS handles the underlying infrastructure and replication setup, reducing the operational complexity for the company.

Option B, is a valid solution for achieving high availability within a single AWS Region. However, it does not meet the requirement of having the data available and online across multiple AWS Regions at all times, which is specified in the question. The Multi-AZ feature in RDS provides automatic failover within the same Region, but it does not replicate the data to multiple Regions.

upvoted 4 times

 **mal1903** 9 months, 1 week ago

Selected Answer: B

C and D just specify another single region. This does not translate to multiple regions.

B (Multi-AZ) means the solution will be highly available.

The data will be available in multiple regions for both B and C but B is a better solution!

upvoted 1 times

 **Guru4Cloud** 6 months, 1 week ago

its data is available and online across multiple AWS Regions at all times

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

"Another single region" plus the original region ARE of course "multiple regions", what else? While B "Multi-AZ" is two AZs in the same region.

upvoted 1 times

 **MrAWSAssociate** 9 months, 2 weeks ago

Selected Answer: C

Answer B is not right, because "RDS Multi-AZ" always spans at least two Availability Zones within a single region and the question requirement RDS DB should be available in multiple regions. Therefore, C is the most suitable answer for this question.

upvoted 2 times

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

I would like to change my answer to "B". The question has some distractor words: "its data is available and online across multiple AWS Regions at all times". We agree that AWS Lambda is a serverless service available online around the world in 99 regions. So the option "B" is the most appropriate answer, since multi-AZ focuses on the availability factor and it has the LEAST amount of operational overhead.

upvoted 1 times

✉ **abhishek2021** 9 months, 2 weeks ago

Selected Answer: B

B & C both make data available. However, B is less overhead.

What I think, the question is asking for data availability across multiple regions not for a DR solution. So, RDS being accessible over public IP will do the trick for data being available across regions.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 1 week ago

Multi-AZ is not the same as Multi-Regional

upvoted 1 times

✉ **Bmarodi** 9 months, 2 weeks ago

Selected Answer: C

Option meets the requirements, ref. link: <https://aws.amazon.com/blogs/database/best-practices-for-amazon-rds-for-postgresql-cross-region-read-replicas/>

upvoted 1 times

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

Selected Answer: B

In an Amazon RDS Multi-AZ deployment, Amazon RDS automatically creates a primary database (DB) instance and synchronously replicates the data to an instance in a different AZ.

<https://aws.amazon.com/rds/features/multi-az/>

upvoted 1 times

✉ **ruqui** 10 months ago

Selected Answer: C

B is wrong because Multi AZ feature doesn't allow to have replicas in another region!!!! (the requirement is that "data should be available and online across multiple AWS Regions at all times") ... only feasible option is C

upvoted 1 times

Question #242

Topic 1

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.

Which policy should be used to meet this requirement?

- A. Simple routing policy
- B. Latency routing policy
- C. Multivalue routing policy
- D. Geolocation routing policy

Correct Answer: C

Community vote distribution

✉️ **LuckyAro** 1 year, 2 months ago

Selected Answer: C

Use a multivalue answer routing policy to help distribute DNS responses across multiple resources. For example, use multivalue answer routing when you want to associate your routing records with a Route 53 health check. For example, use multivalue answer routing when you need to return multiple values for a DNS query and route traffic to multiple IP addresses.

<https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/>
upvoted 11 times

✉️ **cookieMr** 9 months ago

The Multivalue routing policy allows Route 53 to respond to DNS queries with multiple healthy IP addresses for the same resource. This is particularly useful in scenarios where multiple instances are serving the same purpose and need to be load balanced or failover capable. With the Multivalue routing policy, Route 53 returns multiple IP addresses in a random order to distribute the traffic across all healthy instances.

Option A (Simple routing policy) would only return a single IP address in response to DNS queries and does not support returning multiple addresses.

Option B (Latency routing policy) is used to route traffic based on the lowest latency to the resource and does not fulfill the requirement of returning all healthy IP addresses.

Option D (Geolocation routing policy) is used to route traffic based on the geographic location of the user and does not fulfill the requirement of returning all healthy IP addresses.

Therefore, the Multivalue routing policy is the most suitable option for returning the IP addresses of all healthy EC2 instances in response to DNS queries.

upvoted 9 times

✉️ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: C

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

"Multivalue answer routing policy – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random. You can use multivalue answer routing to create records in a private hosted zone."

Company requires that the IP addresses of "ALL" healthy EC2 instances be returned so C is the only option.

upvoted 3 times

✉️ **Ruffyit** 3 months, 2 weeks ago

Use a multivalue answer routing policy to help distribute DNS responses across multiple resources. For example, use multivalue answer routing when you want to associate your routing records with a Route 53 health check. For example, use multivalue answer routing when you need to return multiple values for a DNS query and route traffic to multiple IP addresses.

upvoted 1 times

✉️ **TariqKipkemei** 6 months ago

Selected Answer: C

Use Multivalue answer routing policy when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
upvoted 1 times

✉️ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: C

C. Multivalue routing policy

upvoted 1 times

✉ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

This is for a different question I guess

upvoted 1 times

✉ **animefan1** 8 months, 3 weeks ago

multivalue supports health checks

upvoted 1 times

✉ **MLCL** 1 year ago

IP are returned RANDOMLY for multi-value Routing, is this what we want ?

upvoted 4 times

✉ **WhericanIstart** 1 year ago

Selected Answer: C

Multivalue answer routing policy ...answer is C

upvoted 1 times

✉ **mhmt4438** 1 year, 2 months ago

Selected Answer: C

Answer is C

upvoted 2 times

✉ **Aninina** 1 year, 2 months ago

Selected Answer: C

Should be C

upvoted 1 times

✉ **bamishr** 1 year, 2 months ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/46491-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

✉ **Morinator** 1 year, 2 months ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/46491-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Question #243

Topic 1

A medical research lab produces data that is related to a new study. The lab wants to make the data available with minimum latency to clinics across the country for their on-premises, file-based applications. The data files are stored in an Amazon S3 bucket that has read-only permissions for each clinic.

What should a solutions architect recommend to meet these requirements?

- A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic
- B. Migrate the files to each clinic's on-premises applications by using AWS DataSync for processing.
- C. Deploy an AWS Storage Gateway volume gateway as a virtual machine (VM) on premises at each clinic.
- D. Attach an Amazon Elastic File System (Amazon EFS) file system to each clinic's on-premises servers.

Correct Answer: C

Community vote distribution



✉ **mhmt4438** Highly Voted 1 year, 2 months ago

Selected Answer: A

- A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. By deploying a file gateway as a virtual machine on each clinic's premises, the medical research lab can provide low-latency access to the data stored in the S3 bucket while maintaining read-only permissions for each clinic. This solution allows the clinics to access the data files directly from their on-premises file-based applications without the need for data transfer or migration.

upvoted 19 times

✉ **pentium75** Most Recent 2 months, 4 weeks ago

Selected Answer: A

- A: does exactly that is required here
 B: "Migrate", as to MOVE the files out from S3, doesn't make sense
 C: Volume Gateway provides iSCSI volumes backed by an object in AWS-managed S3, it does not provide access to S3 objects
 D: You can do that but it would have high (not "minimum") latency, and the data is not in that EFS volume, it's in S3

upvoted 3 times

✉ **Ruffyit** 3 months, 2 weeks ago

AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. By deploying a file gateway as a virtual machine on each clinic's premises, the medical research lab can provide low-latency access to the data stored in the S3 bucket while maintaining read-only permissions for each clinic. This solution allows the clinics to access the data files directly from their on-premises file-based applications without the need for data transfer or migration.

upvoted 1 times

✉ **TariqKipkemei** 6 months ago

Selected Answer: A

The Amazon S3 File Gateway enables you to store and retrieve objects in Amazon Simple Storage Service (S3) using file protocols such as Network File System (NFS) and Server Message Block (SMB). Objects written through S3 File Gateway can be directly accessed in S3.

upvoted 2 times

✉ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

- A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

upvoted 2 times

✉ **cookieMr** 9 months ago

- A. It allows the clinics to access the data files stored in the S3 bucket through a file interface. The file gateway caches frequently accessed data locally, reducing latency and providing fast access to the data.
 B. It involves transferring the data files from the Amazon S3 bucket to each clinic's on-premises applications using AWS DataSync. While this enables data migration, it may not provide real-time access and may introduce additional latency.
 C. It is suitable for block-level access to data rather than file-level access. It may not be the most efficient solution for file-based applications.
 D. It involves using Amazon EFS, which is a scalable file storage service, to provide file-level access to the data. However, it may introduce additional complexity and latency compared to using a file gateway solution.

upvoted 4 times

✉ **Bmarodi** 9 months, 4 weeks ago

Selected Answer: A

Option A meets the requirements.

upvoted 1 times

✉ **jaswantn** 11 months, 1 week ago

For File-based applications use File Gateway: (Option A)

upvoted 1 times

✉ **Grace83** 1 year ago

Definitely A.

Why are there so many wrong answers by Admins?

upvoted 4 times

✉ **maggie135** 8 months, 4 weeks ago

I guess to force us to read and think, so one can't just memorize the answer and go to exam ?

upvoted 3 times

✉ **AlessandraSAA** 1 year ago

Selected Answer: A

Amazon S3 File Gateway enables you to store file data as objects in Amazon S3 cloud storage for data lakes, backups, and Machine Learning workflows. With Amazon S3 File Gateway, each file is stored as an object in Amazon S3 with a one-to-one mapping between a file and an object.

Volume Gateway provides block storage volumes over iSCSI, backed by Amazon S3, and provides point-in-time backups as Amazon EBS snapshots. Volume Gateway integrates with AWS Backup, an automated and centralized backup service, to protect Storage Gateway volumes.

So it's A

upvoted 4 times

✉ **Steve_4542636** 1 year ago

Selected Answer: A

A for answer

upvoted 1 times

✉ **bdp123** 1 year, 1 month ago

Selected Answer: A

<https://cloud.in28minutes.com/aws-certification-aws-storage-gateway>

upvoted 1 times

✉ **kbaruu** 1 year, 2 months ago

Selected Answer: A

A. Deploy an AWS Storage Gateway file gateway...

upvoted 1 times

✉ **imisioluwa** 1 year, 2 months ago

Selected Answer: A

The correct answer is A.

<https://www.knowledgehut.com/tutorials/aws/aws-storage-gateway#:~:text=AWS%20Storage%20Gateway%20helps%20in%20connecting,as%20well%20as%20providing%20data%20security.&text=AWS%20Storage%20Gateway%20helps,as%20providing%20data%20security.&text=Gateway%20helps%20in%20connecting,as%20well%20as%20providing>

upvoted 1 times

✉ **venice1234** 1 year, 2 months ago

Selected Answer: C

I think C (Volume Gateway) is correct as it has an option to have Local Storage with Asynchronous sync with S3. This would give low latency access to all local files not just cached/recent files.

upvoted 2 times

✉ **pentium75** 2 months, 4 weeks ago

Volume gateway provides an iSCSI volume and stores that as a single object in an AWS-managed S3 bucket. It does not provide access to S3 objects.

upvoted 1 times

✉ **laicos** 1 year, 2 months ago

Selected Answer: A

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

upvoted 1 times

✉ **Aninina** 1 year, 2 months ago

Selected Answer: A

A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

upvoted 1 times

Question #244

Topic 1

A company is using a content management system that runs on a single Amazon EC2 instance. The EC2 instance contains both the web server and the database software. The company must make its website platform highly available and must enable the website to scale to meet user demand.

What should a solutions architect recommend to meet these requirements?

- A. Move the database to Amazon RDS, and enable automatic backups. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer in the Availability Zone, and set the two instances as targets.
- B. Migrate the database to an Amazon Aurora instance with a read replica in the same Availability Zone as the existing EC2 instance. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer, and set the two EC2 instances as targets.
- C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.
- D. Move the database to a separate EC2 instance, and schedule backups to Amazon S3. Create an Amazon Machine Image (AMI) from the original EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

Correct Answer: C

Community vote distribution

C (97%)

✉ **mhmt4438** Highly Voted 1 year, 2 months ago

Selected Answer: C

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

This approach will provide both high availability and scalability for the website platform. By moving the database to Amazon Aurora with a read replica in another availability zone, it will provide a failover option for the database. The use of an Application Load Balancer and an Auto Scaling group across two availability zones allows for automatic scaling of the website to meet increased user demand. Additionally, creating an AMI from the original EC2 instance allows for easy replication of the instance in case of failure.

upvoted 17 times

✉ **Bmarodi** 9 months, 4 weeks ago

Very good explanations!

upvoted 1 times

✉ **awsgeek75** Most Recent 2 months, 3 weeks ago

Selected Answer: C

C is the only option via deduction logic based on the assumption the CMS database is Aurora compatible. Other solutions don't promise scaling as much as Aurora solution in option C does.

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Just to clarify, the question is vague as we don't know anything about the DB types on the CMS so making an assumption that Aurora will work with the CMS.

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

Selected Answer: C

A and B involve manual steps and do not include scaling (it's just two fixed instances)

D scales the application part but leaves the database on a single EC2 instance which would be neither "highly available" nor "scalable"

upvoted 3 times

✉ **Ruffyt** 3 months, 2 weeks ago

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

upvoted 1 times

✉ **TariqKipkemei** 6 months ago

Selected Answer: C

Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

upvoted 1 times

Guru4Cloud 6 months, 2 weeks ago

Selected Answer: C

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

upvoted 1 times

MutiverseAgent 8 months ago

Selected Answer: D

The question does not say if the current application is using a relational database, so how we can be sure that it can move to RDS or aurora as answers A, B & C states? In my opinion the right answer is D.

upvoted 1 times

pentium75 2 months, 4 weeks ago

In D, you "move the database to a separate EC2 instance" BEFORE creating the AMI for the Auto Scaling group. So you'd still have a single EC2 instance running the database, which would meet neither the availability nor the scalability requirement.

upvoted 1 times

animefan1 8 months, 3 weeks ago

Selected Answer: C

has all options needed for HA

upvoted 1 times

cookieMr 9 months ago

Selected Answer: C

Option A does not provide a solution for high availability or scalability. Manually launching another EC2 instance in the same AZ may not ensure high availability, as a failure in that AZ would result in downtime.

Option B improves database performance and provides a level of fault tolerance, it does not address the scalability aspect of the website platform.

Option C provides both high availability and fault tolerance. Creating an AMI allows for easy replication of the EC2 instance across AZs. Configuring an ALB in two AZs and attaching an ASG ensures scalability and load distribution across multiple instances.

Option D does not provide the high availability and scalability required by the company. Scheduled backups to S3 address data protection but do not contribute to website availability or scalability.

upvoted 2 times

Bmarodi 9 months, 4 weeks ago

Selected Answer: C

Option C meets the requirements.

upvoted 1 times

ssoffline 10 months ago

Why not D?

Are we just assuming that there will be no write to the db?

upvoted 1 times

antropaws 10 months, 1 week ago

Selected Answer: C

Absolutely C.

upvoted 1 times

Aninina 1 year, 2 months ago

Selected Answer: C

C: This will allow the website platform to be highly available by using Aurora, which provides automatic failover and replication. Additionally, by creating an AMI from the original EC2 instance, the Auto Scaling group can automatically launch new instances in multiple availability zones and use the Application Load Balancer to distribute traffic across them. This way, the website will be able to handle the increased traffic, and will be less likely to go down due to a single point of failure.

upvoted 3 times

Question #245

Topic 1

A company is launching an application on AWS. The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group. The instances are in an Auto Scaling group for each environment. The company requires a development environment and a production environment. The production environment will have periods of high traffic.

Which solution will configure the development environment MOST cost-effectively?

- A. Reconfigure the target group in the development environment to have only one EC2 instance as a target.
- B. Change the ALB balancing algorithm to least outstanding requests.
- C. Reduce the size of the EC2 instances in both environments.
- D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group.

Correct Answer: A

Community vote distribution



mhmt4438 Highly Voted 1 year, 2 months ago

Selected Answer: D

D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group

This option will configure the development environment in the most cost-effective way as it reduces the number of instances running in the development environment and therefore reduces the cost of running the application. The development environment typically requires less resources than the production environment, and it is unlikely that the development environment will have periods of high traffic that would require a large number of instances. By reducing the maximum number of instances in the development environment's Auto Scaling group, the company can save on costs while still maintaining a functional development environment.

upvoted 14 times

JayBee65 1 year, 2 months ago

No, it will not reduce the number of instances being used, since a minimum of 2 will be used at all times.

upvoted 9 times

pentium75 2 months, 4 weeks ago

But it will keep the number of instances at two, while the production environment has "AT LEAST two".

upvoted 1 times

TheFivePips Most Recent 4 weeks ago

Selected Answer: D

The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group

You are required to keep at least two instances in each target group. A sets it to one, which would be more cost effective, but doesn't meet the requirement.

upvoted 2 times

Priyapani 2 months, 1 week ago

Selected Answer: D

In the question it is said minimum it should have 2 instances in Target group. So in development group we can reduce the the target group. In option A. It is said it will have only one instance in development group that doesn't match to our question

upvoted 3 times

awsgeek75 2 months, 3 weeks ago

Selected Answer: D

B and C don't actually save any cost without impacting performance during high traffic on production.

A and D are basically same thing but A enforces a limit of one EC2 instance which is not acceptable as the question asks: "Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group. The instances are in an Auto Scaling group for each environment"

Hence D is the only valid answer.

upvoted 4 times

pentium75 2 months, 4 weeks ago

Selected Answer: D

A modifies only the ALB target group (= directs traffic only to one node), but does not affect the number of nodes (and the cost)

B balances load between nodes but does not affect the cost

C impacts the prod environment so that would be unable to handle its "periods of high traffic"

D makes sure that the dev environment will not scale to more than 2 instances, as does the prod environment

upvoted 4 times

 **ddaannnn** 3 months ago

The most cost-effective solution is to reconfigure the target group in the development environment to have only one EC2 instance as a target. This will ensure that the development environment only uses the resources that it needs, which will save the company money.

The other solutions are not as cost-effective. Changing the ALB balancing algorithm to least outstanding requests will not reduce the number of EC2 instances that are used, and it may actually increase the amount of traffic that is directed to each instance. Reducing the size of the EC2 instances will also not reduce the number of instances that are used, and it may actually make the application slower. Reducing the maximum number of EC2 instances in the development environment's Auto Scaling group will only reduce the number of instances that are used when the traffic is high, and it will not reduce the number of instances that are used on average.

Therefore, the most cost-effective solution is to reconfigure the target group in the development environment to have only one EC2 instance as a target.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

No, you're confusing "target group" (of the ALB) with "Auto Scaling group". Answer A will direct ALB traffic only to one node, but it does not affect the number of nodes in any way (it will still be "at least two").

upvoted 2 times

 **chasingsummer** 3 months ago

Selected Answer: A

By reconfiguring the target group in the development environment to have only one EC2 instance as a target, it reduces the number of instances handling the development environment's traffic. This ensures the minimum setup required for the development environment's functionality without incurring unnecessary costs associated with multiple instances.

This solution optimizes costs by scaling down the infrastructure specifically in the development environment where lower traffic or fewer resources might be acceptable for testing or development purposes, thus reducing unnecessary expenses related to running multiple instances.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

No, you're confusing "target group" (of the ALB) with "Auto Scaling group". Answer A will direct ALB traffic only to one node, but it does not affect the number of nodes in any way (it will still be "at least two").

upvoted 4 times

 **MiniYang** 3 months ago

Selected Answer: D

the correct answer is D. This is from Amazon Q : The most cost-effective way to configure the development environment would be to reduce the maximum number of EC2 instances in the development environment's Auto Scaling group (Option D). The most cost-effective way to configure the development environment would be to reduce the maximum number of EC2 instances in the development environment's Auto Scaling group (Option D).The most cost-effective way to configure the development environment would be to reduce the maximum number of EC2 instances in the development environment's Auto Scaling group (Option D).

upvoted 3 times

 **meowruki** 3 months, 3 weeks ago

Selected Answer: A

Option D: Reducing the maximum number of EC2 instances in the development environment's Auto Scaling group could limit scalability but might not directly optimize costs. Min can still be the same number of EC2

upvoted 1 times

 **saymolet** 3 weeks, 2 days ago

"might not directly optimize." No, it does, you're paying less for fewer machines. This is the most direct cost optimisation practice there could ever be. The correct answer is D

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

No, you're confusing "target group" (of the ALB) with "Auto Scaling group". Answer A will direct ALB traffic only to one node, but it does not affect the number of nodes in any way (it will still be "at least two").

upvoted 3 times

 **Chef_couincouin** 3 months, 4 weeks ago

Answer is A but I'm not agree. We use only one instance with A and D.

But with D, by default, instance is terminated whereas with A, instance still exist.

Answer should be D

upvoted 2 times

 **ravinperera** 4 months, 3 weeks ago

Selected Answer: D

This option is specific to the development environment and focuses on reducing the number of instances that can be spun up during scaling events. This means cost savings because fewer instances will be used even if the scaling policies are triggered.

Given the goal to configure the development environment in the most cost-effective way, without compromising the production environment, the best option is D

upvoted 2 times

 **Mandar15** 5 months, 4 weeks ago

Selected Answer: A

Option A
upvoted 1 times

✉ **TariqKipkemei** 6 months ago

Selected Answer: A
wont think much about this, option A is the most cost effective
upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Wrong, think more. A reduces to one instance whereas:

"The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group"

The ALB NEEDS at least 2 instances so where is your second instance?

upvoted 2 times

✉ **Its_SaKar** 6 months ago

Selected Answer: A

Option A because it can't be option D as there should be at least two EC2 instances in Auto scaling group, and can't be reduced to one as said in option D.

So, simply reconfigure the target group in the development environment to have only one EC2 instance as a target as said in option A to reduce cost.

upvoted 2 times

✉ **pentium75** 2 months, 4 weeks ago

No, you're confusing "target group" (of the ALB) with "Auto Scaling group". Answer A will direct ALB traffic only to one node, but it does not affect the number of nodes in any way (it will still be "at least two").

upvoted 2 times

✉ **Its_SaKar** 6 months ago

Selected Answer: D

Option A because it can't be option D as there should be at least two EC2 instances in Auto scaling group, and can't be reduced to one as said in option D.

So, simply reconfigure the target group in the development environment to have only one EC2 instance as a target as said in option A to reduce cost.

upvoted 1 times

✉ **Its_SaKar** 6 months ago

plz remove this comment as i mistakenly voted option D here. I have posted another comment above.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

A. Reconfigure the target group in the development environment to have only one EC2 instance as a target

upvoted 2 times

✉ **kwang312** 6 months, 3 weeks ago

Selected Answer: A

I choose A but cannot understand this question, which environment handles the traffic? The question is not clearly for have correct answer.

upvoted 1 times

Question #246

Topic 1

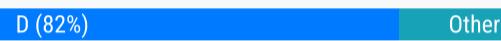
A company runs a web application on Amazon EC2 instances in multiple Availability Zones. The EC2 instances are in private subnets. A solutions architect implements an internet-facing Application Load Balancer (ALB) and specifies the EC2 instances as the target group. However, the internet traffic is not reaching the EC2 instances.

How should the solutions architect reconfigure the architecture to resolve this issue?

- A. Replace the ALB with a Network Load Balancer. Configure a NAT gateway in a public subnet to allow internet traffic.
- B. Move the EC2 instances to public subnets. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.
- C. Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.
- D. Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

Correct Answer: C

Community vote distribution



✉ **ktulu2602** Highly Voted 1 year ago

I think either the question or the answers are not formulated correctly because of this document:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/load-balancer-stickiness/subnets-routing.html>

A - Might be possible but it's quite impractical

B - Not needed as the setup described should work as is provided the SGs of the EC2 instances accept traffic from the ALB

C - Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route - not needed as the EC2 instances would receive the traffic from the ALB ENIs. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0 - the default behaviour of the SG is to allow outbound traffic only.

D - Create public subnets in each Availability Zone. Associate the public subnets with the ALB - if it's a internet facing ALB these should already be in place. Update the route tables for the public subnets with a route to the private subnets - no need as the local prefix entry in the route tables would take care of this point

I'm 110% sure the question or answers or both are wrong. Prove me wrong! :)

upvoted 16 times

✉ **UnluckyDucky** 1 year ago

Completely agreed, I was looking for an option to allow HTTPS traffic on port 443 from the ALB to the EC2 instance's security group.

Either the question or the answers are wrong.

upvoted 7 times

✉ **bdp123** Highly Voted 1 year, 1 month ago

Selected Answer: D

I change my answer to 'D' because of following link:

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

upvoted 12 times

✉ **sidharthwader** Most Recent 2 weeks, 1 day ago

D looks the best but still it must have a internet gateway and once it has internet gateway we must add the route table for private subnet to talk to the public subnet so by using the it should be able to access. I don't think lb can act like internet gateway

upvoted 1 times

✉ **bujuman** 1 month ago

Selected Answer: D

Considering these statements:

-The EC2 instances are in private subnets.

- However, the internet traffic is not reaching the EC2 instances.

A reliable solution is D according to following link:

<https://repost.aws/knowledge-center/public-load-balancer-private-ec2>

Answer C could not satisfy the requirements because only outbound traffic rules are mentioned

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

Selected Answer: D

A - "NAT gateway" is "to allow [outbound] internet traffic", but this is about inbound traffic

B - This is about outbound traffic while the problem is inbound

- C - This is about outbound traffic while the problem is inbound
 D - Sounds correct, though the "update the route tables" should not be required if both subnets are in same VPC
 upvoted 5 times

awsgeek75 2 months, 1 week ago

D is the "least wrong" answer here. I was also confused by the route table part and thought I was missing something critical in the question.
 upvoted 2 times

David_Ang 4 months, 3 weeks ago

Selected Answer: A

this is a bad formulated question with gaps, but my reason tells me that if you want to connect something from a private subnet to internet you need a NAT (instance or gateway, bastion).
 Creating public subnets in each Availability Zone and associating them with the Application Load Balancer (ALB) won't resolve the problem of allowing internet traffic to reach the private EC2 instances. Public subnets are typically used when you want your EC2 instances to have direct internet access, not when you want to keep them in private subnets with indirect access through a load balancer.

upvoted 3 times

vijaykamal 5 months, 4 weeks ago

Selected Answer: D

option A (replace ALB with Network Load Balancer and add a NAT gateway) is not the most straightforward solution because it changes the load balancer type and introduces a NAT gateway, which might be unnecessary if the goal is to use an ALB for web traffic. ALBs are commonly used for internet-facing web applications.

Option B (move EC2 instances to public subnets and modify security group rules) involves placing instances in public subnets, which is generally not recommended for security reasons. Additionally, it suggests modifying security group rules for outbound traffic, which might not be the best practice to resolve the issue.

Option C (update route tables and security group rules) addresses the route table update, but it also suggests moving instances to public subnets, which is not ideal from a security perspective.

upvoted 1 times

TariqKipkemei 6 months ago

Selected Answer: D

Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

upvoted 2 times

Its_SaKar 6 months ago

Selected Answer: D

Option A is incorrect Internet traffic is http and https so it cant be configured to NLB
 Option B and option C is incorrect because sending 0.0.0.0/0 is not best practices

Option D is correct because its the only option left. and updating the route tables for the public subnets with a route to the private subnets ensures internet access to EC2 instances in private subnet.

upvoted 2 times

Guru4Cloud 6 months, 2 weeks ago

Selected Answer: D

D. is the correct solution. By creating public subnets and associating them with the ALB, inbound internet traffic can reach the ALB. The route tables for the public subnets are updated to include a route to the private subnets, allowing traffic to reach the EC2 instances in the private subnets. This setup enables secure access to the application while allowing internet traffic to reach the EC2 instances through the ALB.

upvoted 2 times

A1975 7 months, 4 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-example-private-subnets-nat.html>

upvoted 2 times

cookieMr 9 months ago

Selected Answer: D

A. suggests using a different type of load balancer and configuring a NAT gateway, but it does not address the issue of internet traffic reaching the EC2 instances.

B. suggests exposing the EC2 instances to the public internet, which may pose security risks and does not address the issue of inbound internet traffic reaching the instances.

C. suggests configuring the EC2 instances to have outbound internet access, but it does not solve the problem of inbound internet traffic reaching the instances.

D. is the correct solution. By creating public subnets and associating them with the ALB, inbound internet traffic can reach the ALB. The route tables for the public subnets are updated to include a route to the private subnets, allowing traffic to reach the EC2 instances in the private subnets. This setup enables secure access to the application while allowing internet traffic to reach the EC2 instances through the ALB.

upvoted 3 times

Vinhkewl 9 months ago

Should be C

It would normally make sense to segregate your ALBs into public or private zones by security group and target group, but this is configuration rather than architectural placement - there is nothing preventing you from adding a rule to route specific paths or ports to a public subnet from an ALB that has until then been serving private subnets only.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

C allows the EC2 instances to be accessed directly from the Internet, which we don't want. It's the ALB (not the Internet) that can't access them. We must make sure that the ALB can be reached from the Internet and that the EC2 instances can be reached from the ALB.

upvoted 1 times

 **Abrar2022** 9 months, 2 weeks ago

Selected Answer: D

To attach Amazon EC2 instances that are located in a private subnet, first create public subnets

upvoted 4 times

 **Bmarodi** 9 months, 4 weeks ago

Selected Answer: D

I vote with the option D.

upvoted 1 times

 **antropaws** 10 months, 1 week ago

D is not quite accurate because subnets in a VPC have a local route by default, meaning that all subnets are able to communicate with each other: "Every route table contains a local route for communication within the VPC. This route is added by default to all route tables". This question is poorly formulated.

upvoted 2 times

 **kraken21** 12 months ago

Selected Answer: D

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

upvoted 2 times

Question #247

Topic 1

A company has deployed a database in Amazon RDS for MySQL. Due to increased transactions, the database support team is reporting slow reads against the DB instance and recommends adding a read replica.

Which combination of actions should a solutions architect take before implementing this change? (Choose two.)

- A. Enable binlog replication on the RDS primary node.
- B. Choose a failover priority for the source DB instance.
- C. Allow long-running transactions to complete on the source DB instance.
- D. Create a global table and specify the AWS Regions where the table will be available.
- E. Enable automatic backups on the source instance by setting the backup retention period to a value other than 0.

Correct Answer: AC*Community vote distribution*

fkie4 1 year ago

Who would know this stuff man...

upvoted 91 times

presetacsing 10 months, 1 week ago

exactly

upvoted 2 times

MNotABot 8 months, 2 weeks ago

"Allow long-running transactions to complete on the source DB instance." -- Makes sense / Also a backup before changing anything again made a sense.

upvoted 2 times

foha2012 2 months ago

Just take an intelligent guess. Eliminate 2 wrong answers and you will have a 50percent success chance.

upvoted 2 times

KelvinEM 1 year, 2 months ago

C,E

"An active, long-running transaction can slow the process of creating the read replica. We recommend that you wait for long-running transactions to complete before creating a read replica. If you create multiple read replicas in parallel from the same source DB instance, Amazon RDS takes only one snapshot at the start of the first create action."

When creating a read replica, there are a few things to consider. First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica"

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

upvoted 42 times

awsgeek75 2 months, 3 weeks ago

Selected Answer: CE

B and D don't have anything to do with the question.

E is a must have before doing major architecture changes

A is not something you need to do explicitly when creating read replicas as it is managed by RDS

C makes sense

* I think the options are really badly worded which makes it confusing. I doubt this is a real question.

upvoted 1 times

awsgeek75 2 months, 3 weeks ago

Also, to add, binlog replication is needed if you are replicating to a non RDS instance. This is why I think the question is badly phrased as it does not specify the location of read replica.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MySQL.Procedural.Importing.External.Repl.html>

upvoted 1 times

Ruffyit 3 months, 2 weeks ago

An active, long-running transaction can slow the process of creating the read replica. We recommend that you wait for long-running transactions to complete before creating a read replica. If you create multiple read replicas in parallel from the same source DB instance, Amazon RDS takes only one snapshot at the start of the first create action.

When creating a read replica, there are a few things to consider. First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica.

upvoted 1 times

 **meowruki** 3 months, 3 weeks ago

Selected Answer: AC

To improve the read performance of a database in Amazon RDS for MySQL by adding a read replica, you should take the following actions:

Enable binlog replication on the RDS primary node: This allows the primary node to stream its binary logs to the read replica, enabling data replication.

A. Enable binlog replication on the RDS primary node.

Allow long-running transactions to complete on the source DB instance: Before creating a read replica, it's advisable to let any long-running transactions complete to ensure consistency between the source and the replica.

C. Allow long-running transactions to complete on the source DB instance.

The other options are not directly related to setting up a read replica:

upvoted 1 times

 **meowruki** 3 months, 3 weeks ago

B. Choose a failover priority for the source DB instance: Failover priority is more relevant in a Multi-AZ setup where automatic failover might occur. It's not directly related to creating a read replica.

D. Create a global table and specify the AWS Regions where the table will be available: Global tables are used for cross-region replication, but they are not directly related to setting up a read replica for improved read performance.

E. Enable automatic backups on the source instance by setting the backup retention period to a value other than 0: While it's a good practice to have backups enabled, it is not a prerequisite for creating a read replica.

Therefore, the most appropriate actions are A and C.

upvoted 1 times

 **xdkonorek2** 4 months ago

Selected Answer: AE

A - it's essential for continuous replication

E - it's essential for setting up replication, initial data in replica is based on latest backup

other options:

B - we're not designing for HA, and it's related to multi-AZ RDS deployments

C - is this needed for adding read replica?

D - it's not a dynamodb to create global table

upvoted 3 times

 **vijaykamal** 5 months, 4 weeks ago

Selected Answer: CE

A. Enabling binlog replication is not something you need to do manually before creating a read replica. Amazon RDS for MySQL manages replication internally, and it's not necessary to enable binlog replication explicitly.

B. Choosing a failover priority is related to Multi-AZ configurations and automatic failover, but it is not specifically required when adding a read replica.

D. Creating a global table and specifying AWS Regions is related to Aurora Global Databases, which is not the same as creating a read replica for a standard RDS instance.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: CE

**C. Long-running transactions can prevent the read replica from catching up with the source DB instance. Allowing these transactions to complete before creating the read replica can help ensure that the replica is able to stay synchronized with the source.

**E. Automatic backups must be enabled on the source DB instance for read replicas to be created. This is done by setting the backup retention period to a value other than 0.

upvoted 1 times

 **cd93** 7 months, 1 week ago

Bin log (binary log) is a specific terminology to MySQL, it is a write-only file that logs all history and used for purposes such as point-in-time recovery and transaction replication.

Option A is technically correct but on AWS RDS, this MySQL feature is turned on by setting backup retention period > 0, that is why we must enable backup before replication can work (for MySQL, at least) => Option E is the more general answer for AWS RDS.

Option C is just a recommendation from AWS official documentation, it is there to prevent data mismatch on primary and secondaries when the long-running transactions have not been complete yet.

upvoted 1 times

✉ **A1975** 7 months, 4 weeks ago

Selected Answer: CE

Before a MySQL DB instance can serve as a replication source, make sure to enable automatic backups on the source DB instance. To do this, set the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica. Automatic backups are supported for read replicas running any version of MySQL. You can configure replication based on binary log coordinates for a MySQL DB instance

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html

upvoted 1 times

✉ **StacyY** 7 months, 4 weeks ago

A E. Binlog is needed for on-going replication setup and DB backup is needed for setup the replication DB

upvoted 1 times

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

Correction: c and e

upvoted 1 times

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

A and e

upvoted 1 times

✉ **cookieMr** 9 months ago

Selected Answer: CE

A. enables the binary log replication feature on the RDS primary node, which is necessary for setting up a read replica.

B. determines the order in which DB instances are promoted to the primary role during a failover scenario. It is not directly related to adding a read replica to address slow reads.

C. ensures that any ongoing transactions on the source DB instance are allowed to finish before implementing the change. It helps maintain data integrity and consistency during the transition to the read replica.

D. is a feature specific to DynamoDB. It allows for multi-region replication and high availability in DynamoDB, but it is not applicable in this scenario.

E. ensures that regular backups are taken for the source DB instance. This is important for data protection and recovery purposes, as it allows for point-in-time restoration in case of any issues during or after the addition of the read replica.

upvoted 1 times

✉ **Abrar2022** 9 months, 2 weeks ago

Selected Answer: CE

Before adding read replicas, one needs to allow long-running transactions to complete on the source DB instance otherwise you might end up interrupting transactions. Then, you should enable automatic backups on the source instance and set the backup retention period to a value other than 0.

upvoted 1 times

✉ **Bmarodi** 9 months, 4 weeks ago

Selected Answer: CE

The combination of actions should a solutions architect take before implementing this change are options C & E.

upvoted 1 times

✉ **omoakin** 10 months ago

AAAAAAAAAAAA EEEEEEEEEEEEEE

upvoted 1 times

Question #248

Topic 1

A company runs analytics software on Amazon EC2 instances. The software accepts job requests from users to process data that has been uploaded to Amazon S3. Users report that some submitted data is not being processed. Amazon CloudWatch reveals that the EC2 instances have a consistent CPU utilization at or near 100%. The company wants to improve system performance and scale the system based on user load.

What should a solutions architect do to meet these requirements?

- A. Create a copy of the instance. Place all instances behind an Application Load Balancer.
- B. Create an S3 VPC endpoint for Amazon S3. Update the software to reference the endpoint.
- C. Stop the EC2 instances. Modify the instance type to one with a more powerful CPU and more memory. Restart the instances.
- D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

Correct Answer: D

Community vote distribution



mhmt4438 Highly Voted 1 year, 2 months ago

Selected Answer: D

D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

By routing incoming requests to Amazon SQS, the company can decouple the job requests from the processing instances. This allows them to scale the number of instances based on the size of the queue, providing more resources when needed. Additionally, using an Auto Scaling group based on the queue size will automatically scale the number of instances up or down depending on the workload. Updating the software to read from the queue will allow it to process the job requests in a more efficient manner, improving the performance of the system.

upvoted 10 times

Pangian Most Recent 1 month, 1 week ago

Selected Answer: D

The based on the queue size doesn't seem a perfect approach though

upvoted 1 times

awsgeek75 2 months, 3 weeks ago

Selected Answer: D

D: Because this whole exam seems to be selling more and more SQS solutions...

upvoted 2 times

TariqKipkemei 6 months ago

Selected Answer: D

Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue

upvoted 1 times

Guru4Cloud 6 months, 2 weeks ago

Selected Answer: D

D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

upvoted 1 times

Kill3rasp3r 7 months, 1 week ago

Selected Answer: D

I would vote A if it was ALB targeting an EC2 auto scaling group.

I would vote D if the auto scaling group was based on CPU utilization rather than queue size.

So I think both answers are wrong but D is okay enough.

upvoted 1 times

cookieMr 9 months ago

Selected Answer: D

A. Creating a copy of the instance and placing all instances behind an ALB does not address the high CPU utilization issue or provide scalability based on user load.

B. Creating an S3 VPC endpoint for S3 and updating the software to reference the endpoint improves network performance but does not address the high CPU utilization or provide scalability based on user load.

C. Stopping the EC2 instances and modifying the instance type to one with a more powerful CPU and more memory may improve performance, but it does not address scalability based on user load.

D. Routing incoming requests to SQS, configuring an EC2 ASG based on queue size, and updating the software to read from the queue improves system performance and provides scalability based on user load.

Therefore, option D is the correct choice as it addresses the high CPU utilization, improves system performance, and enables scalability based on user load.

upvoted 1 times

✉ **Whericanstart** 1 year ago

Selected Answer: D

Autoscaling Group and SQS solves the problem.

SQS - Decouples the process

ASG - Autoscales the EC2 instances based on usage

upvoted 1 times

✉ **ak1ak** 1 year ago

Selected Answer: A

its definitely A

upvoted 1 times

✉ **wRhiH** 10 months ago

You don't "scale the system by load" by choosing A

upvoted 3 times

✉ **AHUI** 1 year, 2 months ago

D is correct. Decouple the process. autoscale the EC2 based on query size. best choice

upvoted 3 times

✉ **Aninina** 1 year, 2 months ago

I think it's A " A. Create a copy of the instance. Place all instances behind an Application Load Balancer.

upvoted 1 times

Question #249

Topic 1

A company is implementing a shared storage solution for a media application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.

Which AWS solution meets these requirements?

- A. Create an AWS Storage Gateway volume gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- B. Create an AWS Storage Gateway tape gateway. Configure tapes to use Amazon S3. Connect the application server to the tape gateway.
- C. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: D

Community vote distribution

D (100%)

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

Selected Answer: D

SMB + fully managed = fsx for windows imo
upvoted 16 times

✉  **devonwho**  1 year, 1 month ago

Selected Answer: D

Amazon FSx has native support for Windows file system features and for the industry-standard Server Message Block (SMB) protocol to access file storage over a network.

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>
upvoted 5 times

✉  **pentium75**  2 months, 4 weeks ago

Selected Answer: D

A: Volume Gateway provides virtual disks iSCSI, not SMB
B: Tape Gateway provides virtual tapes via iSCSI, not SMB
C: Not "fully managed"
upvoted 2 times

✉  **TariqKipkemei** 6 months ago

Selected Answer: D

SMB = Amazon FSx for Windows File Server
upvoted 3 times

✉  **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system
upvoted 1 times

✉  **Guru4Cloud** 6 months, 2 weeks ago

All who selected D. are correct - see more details from our community
upvoted 1 times

✉  **animefan1** 8 months, 3 weeks ago

Selected Answer: D

Fsx is fully managed. Plus it supports SMB protocol
upvoted 1 times

✉  **cookieMr** 9 months ago

Selected Answer: D

A. involves using Storage Gateway, but it does not specifically mention support for SMB clients. It may not meet the requirement of using SMB clients to access data.

- B. involves using Storage Gateway with tape gateway configuration, which is primarily used for archiving data to S3. It does not provide native support for SMB clients to access data.
- C. involves manually setting up and configuring a Windows file share on an EC2 Windows instance. While it allows SMB clients to access data, it is not a fully managed solution as it requires manual setup and maintenance.
- D. involves creating an FSx for Windows File Server file system, which is a fully managed Windows file system that supports SMB clients. It provides an easy-to-use shared storage solution with native SMB support.

Based on the requirements of using SMB clients and needing a fully managed solution, option D is the most suitable choice.

upvoted 4 times

 **LuckyAro** 1 year, 2 months ago

Selected Answer: D

Amazon FSx for Windows File Server file system

upvoted 1 times

 **techhb** 1 year, 2 months ago

amazon fsx for smb connectivity.

upvoted 1 times

 **Aninina** 1 year, 2 months ago

Selected Answer: D

FSX is the ans

upvoted 1 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/81115-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **bamishr** 1 year, 2 months ago

Selected Answer: D

D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.

upvoted 1 times

Question #250

Topic 1

A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.

What should a solutions architect do to meet these requirements when configuring the logs?

- A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days
- B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
- C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
- D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Correct Answer: A*Community vote distribution*

cookieMr 9 months ago

Selected Answer: D

A. suggests using CloudWatch as the target for VPC Flow Logs. However, it does not provide a mechanism for managing the retention of the logs for 90 days and then accessing them intermittently.

B. suggests using Kinesis as the target for VPC Flow Logs. While it can retain the logs for 90 days, it does not address the requirement for intermittent access to the logs.

C. suggests using CloudTrail as the target for VPC Flow Logs. However, CloudTrail is designed for auditing and monitoring API activity, not for capturing network traffic logs. It does not meet the requirement of capturing VPC Flow Logs.

D. suggests using S3 as the target for VPC Flow Logs and leveraging S3 Lifecycle policies to transition the logs to a cost-effective storage class after 90 days. It meets the requirement of retaining the logs for 90 days and provides the flexibility for intermittent access while optimizing storage costs.

upvoted 6 times

LuckyAro 1 year, 2 months ago

Selected Answer: D

D is the correct answer.

upvoted 5 times

RicardoD 1 month ago

Selected Answer: A

A is correct

You can change the log data retention setting for CloudWatch logs. By default, logs are kept indefinitely and never expire. You can adjust the retention policy for each log group, keeping the indefinite retention, or choosing a retention period between 10 years and one day.

<https://docs.aws.amazon.com/managedservices/latest/userguide/log-customize-retention.html>

upvoted 1 times

TariqKipkemei 6 months ago

Selected Answer: D

Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days

upvoted 1 times

Guru4Cloud 6 months, 2 weeks ago

Selected Answer: D

D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

upvoted 1 times

animefan1 8 months, 3 weeks ago

Selected Answer: D

S3 will store logs. With life cycle, we can move it to different class. With Option A, log groups expiration will simply remove the logs and failing the 2nd request in question

upvoted 1 times

markw92 9 months, 1 week ago

A doesn't solve "90 days and then accessed intermittently" this statement. It sets expire after 90. Not sure otherwise A seems to be right choice since you can create dashboards etc.

upvoted 1 times

Bmarodi 9 months, 4 weeks ago

Selected Answer: A

Option A meets these requirements.

upvoted 1 times

pentium75 2 months, 4 weeks ago

"Expiration of 90 days", but you need to access the log AFTER 90 days, just "intermittently".

upvoted 3 times

ocbn3wby 1 year, 1 month ago

Selected Answer: D

There's a table here that specifies that VPC Flow logs can go directly to S3. Does not need to go via CloudTrail and then to S3. Nor via CW.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AWS-logs-and-resource-policy.html#AWS-logs-infrastructure-S3>

upvoted 3 times

techhb 1 year, 2 months ago

Selected Answer: D

we need to preserve logs hence D

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogsConcepts.html>

upvoted 2 times

mp165 1 year, 2 months ago

Selected Answer: D

D...agree that retention is the key word

upvoted 2 times

swolfgang 1 year, 2 months ago

Selected Answer: D

a is not,retantion means delete after 90 days but questions say rarely access.

upvoted 2 times

mhmt4438 1 year, 2 months ago

Selected Answer: D

D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

By using Amazon S3 as the target for the VPC Flow Logs, the logs can be easily stored and accessed by the security team. Enabling an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days will automatically move the logs to a storage class that is optimized for infrequent access, reducing the storage costs for the company. The security team will still be able to access the logs as needed, even after they have been transitioned to S3 Standard-IA, but the storage cost will be optimized.

upvoted 4 times

laicos 1 year, 2 months ago

Selected Answer: D

I prefer D

"accessed intermittently" need logs after 90 days

upvoted 1 times

Parsons 1 year, 2 months ago

Selected Answer: D

No, D should be is correct.

"The logs will be frequently accessed for 90 days and then accessed intermittently." => We still need to store instead of deleting as the answer A.
upvoted 2 times

Aninina 1 year, 2 months ago

Selected Answer: D

D looks correct. This will meet the requirements of frequently accessing the logs for the first 90 days and then intermittently accessing them after that. S3 standard-IA is a storage class that is less expensive than S3 standard for infrequently accessed data, so it would be a more cost-effective option for storing the logs after the first 90 days.

upvoted 1 times

Morinator 1 year, 2 months ago

Selected Answer: A

Cloudwatch for this

<https://www.examtopics.com/discussions/amazon/view/59983-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

"Expiration of 90 days", but you need to access the log AFTER 90 days, just "intermittently".

upvoted 2 times

Question #251

Topic 1

An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.

What should a solutions architect do to meet these requirements?

- A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.
- B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.
- C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the NAT instance as the default route.
- D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

Correct Answer: B

Community vote distribution



✉ **mhmt4438** Highly Voted 1 year, 2 months ago

Selected Answer: B

B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.

This approach will allow the EC2 instance to access the internet and download the monthly security updates while still being located in a private subnet. By creating a NAT gateway and placing it in a public subnet, it will allow the instances in the private subnet to access the internet through the NAT gateway. And then, configure the private subnet route table to use the NAT gateway as the default route. This will ensure that all outbound traffic is directed through the NAT gateway, allowing the EC2 instance to access the internet while still maintaining the security of the private subnet.

upvoted 8 times

✉ **Manjunathkb** 11 months, 2 weeks ago

NAT gateway does not allow internet on its own. It needs internet gateway too. None of the answers make sense

upvoted 8 times

✉ **Manjunathkb** 11 months, 2 weeks ago

refer below link

<https://aws.amazon.com/about-aws/whats-new/2021/06/aws-removes-nat-gateways-dependence-on-internet-gateway-for-private-communications/>

upvoted 2 times

✉ **TOR_0511** 4 months ago

lol, that's for 'private connections'

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

B says "place it in a public subnet", a public subnet needs an Internet Gateway so that is included in the answer.

upvoted 2 times

✉ **pentium75** Most Recent 2 months, 4 weeks ago

Selected Answer: B

A - if you "configure the private subnet route table to use the internet gateway" then it's no longer a private subnet

B - Correct (you place NAT GW in a public subnet and add it to the private subnet's route table)

C - NAT instance is deprecated, and it would still be in a private subnet where it doesn't have Internet access

D - NAT instance is deprecated, and in that answer it is created but not even used

upvoted 2 times

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

yes, the nat gateway on its own does not allow connection to the internet. But the question specifies that it has been placed in a public subnet. public subnets are public because they have access to the internet via an internet gateway.

upvoted 1 times

✉ **xdkonorek2** 4 months ago

Selected Answer: C

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

Public subnet – The subnet has a direct route to an internet gateway. Resources in a public subnet can access the public internet.

Private subnet – The subnet does not have a direct route to an internet gateway. Resources in a private subnet require a NAT device to access the

public internet.

Both B and C have caveats but are both viable:

C - NAT Instance is used as a NAT device instead of NAT gateway, but it's still viable option

B - Have 2 redundant components - IGW and public subnet, and NAT gateway still would route traffic to IGW, and if VPC is a custom VPC routing has to be set up

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

"NAT instance in the same subnet where the EC2 instance is located", how would you "use the NAT instance as the default route" when it's in the same subnet?

upvoted 1 times

 **oluolope** 5 months, 1 week ago

Selected Answer: D

A NAT Gateway should have one interface in each network it is connected to. I don't understand what it means when they say it is located either in the private or in the public network. It should be in both. Therefore, B and D do not really make sense.

I choose D over B because there is a requirement to access the internet and although it is possible for the NAT to exist without an internet gateway, the later is still needed when internet access is required which is the case in this scenario.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

NAT Gateway must be in a public subnet as it needs Internet access. It can be specified in a private subnet's route table as a destination.

D doesn't make sense because you created an (outdated) NAT instance but don't use it (you point the route table to the Internet Gateway).

upvoted 1 times

 **TariqKipkemei** 6 months ago

Selected Answer: B

Internet Gateway is required anyway to access the internet.

Option B makes more sense: Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: B

B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.

upvoted 1 times

 **cookieMr** 9 months ago

A. provides direct internet access to the private subnet, which is not desired in this case as the goal is to restrict outbound internet access.

B. allows the EC2 in the private subnet to access the internet through the NAT gateway, which acts as a proxy. It provides controlled outbound internet access while maintaining the security of the private subnet.

C. is similar to using a NAT gateway, but it involves using a NAT instance. NAT instances require more manual configuration and management compared to NAT gateways, making them a less preferred option.

D. combines the use of an internet gateway and a NAT instance, which is not necessary. It introduces unnecessary complexity and adds a NAT instance that requires additional management.

Overall, option B is the most appropriate solution as it utilizes a NAT gateway placed in a public subnet to enable controlled outbound internet access for the EC2 instance in the private subnet.

NAT Gateways are preferred over NAT Instances by AWS and in general.

upvoted 3 times

 **Bmarodi** 9 months, 4 weeks ago

Selected Answer: B

Option B meets the requirements, hence B is right choice.

upvoted 1 times

 **Manjunathkb** 11 months, 2 weeks ago

D would have been the answer if NAT gateway is installed in public subnet and not where EC2 is located. None of the answers are correct.

upvoted 1 times

 **AlessandraSAA** 1 year ago

why not C?

upvoted 1 times

 **UnluckyDucky** 1 year ago

Because NAT Gateways are preferred over NAT Instances by AWS and in general.

I have yet to find a situation where a NAT Instance would be more applicable than NAT Gateway which is fully managed and is overall an easier solution to implement - both in AWS questions or the real world.

upvoted 2 times

✉  **TungPham** 1 year, 1 month ago

Selected Answer: B

Require NAT gateway

upvoted 1 times

✉  **techhb** 1 year, 2 months ago

Selected Answer: B

Answer explained here <https://medium.com/@tshemku/aws-internet-gateway-vs-nat-gateway-vs-nat-instance-30523096df22>

upvoted 1 times

✉  **techhb** 1 year, 2 months ago

Selected Answer: B

NAT Gateway is right choice

upvoted 1 times

✉  **bamishr** 1 year, 2 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/59966-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

Question #252

Topic 1

A solutions architect needs to design a system to store client case files. The files are core company assets and are important. The number of files will grow over time.

The files must be simultaneously accessible from multiple application servers that run on Amazon EC2 instances. The solution must have built-in redundancy.

Which solution meets these requirements?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon S3 Glacier Deep Archive
- D. AWS Backup

Correct Answer: A
Community vote distribution

 A (100%)

 **Aninina**  1 year, 2 months ago

Selected Answer: A

EFS Amazon Elastic File System (EFS) automatically grows and shrinks as you add and remove files with no need for management or provisioning.
upvoted 5 times

 **Chiquitabandita**  5 months, 3 weeks ago

Selected Answer: A

my choice is A but I think a better alternative would be S3 standard if offered wouldn't it be?
upvoted 2 times

 **TariqKipkemei** 6 months ago

Selected Answer: A

File system, scalable, multiple access = Amazon Elastic File System (Amazon EFS)
upvoted 2 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

Amazon Elastic File System (Amazon EFS)
upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: A

EFS provides a scalable and fully managed file storage service that can be accessed concurrently from multiple EC2. It offers built-in redundancy by storing data across multiple AZs within a region. With EFS, the client case files can be accessed by multiple application servers simultaneously, ensuring high availability and scalability as the number of files grows over time.

Option B, EBS, is a block-level storage service that is typically used for attaching to individual EC2 and does not provide concurrent access to multiple instances, making it unsuitable for this scenario.

Option C, S3 Glacier Deep Archive, is a long-term archival storage service and may not be suitable for active file access and simultaneous access from multiple application servers.

Option D, AWS Backup, is a centralized backup management service and does not provide the required simultaneous file access and redundancy features.

Therefore, the most suitable solution is Amazon EFS (option A).

upvoted 4 times

 **Bmarodi** 9 months, 4 weeks ago

Selected Answer: A

Option A meets the requirements, hence A is correct answer.
upvoted 1 times

 **moiraqi** 10 months ago

What does "The solution must have built-in redundancy" mean

upvoted 1 times

✉ **KZM** 1 year ago

If the application servers are running on Linux or UNIX operating systems, EFS is a the most suitable solution for the given requirements.

upvoted 1 times

✉ **TungPham** 1 year, 1 month ago

Selected Answer: A

"accessible from multiple application servers that run on Amazon EC2 instances"

upvoted 4 times

✉ **mhmt4438** 1 year, 2 months ago

Selected Answer: A

Correct answer is A

upvoted 2 times

✉ **bamishr** 1 year, 2 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/68833-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Question #253

Topic 1

A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.

Policy 1

```
{
  "Version": "2012-10-17", "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:Get*",
        "iam>List*",
        "kms>List*",
        "ec2:*",
        "ds:*",
        "logs:Get*",
        "logs:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Policy 2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ds>Delete*",
      "Resource": "*"
    }
  ]
}
```

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

- A. Deleting IAM users
- B. Deleting directories
- C. Deleting Amazon EC2 instances
- D. Deleting logs from Amazon CloudWatch Logs

Correct Answer: C

Community vote distribution

C (100%)

 **JayBee65**  1 year, 2 months ago

ec2:* Allows full control of EC2 instances, so C is correct

The policy only grants get and list permission on IAM users, so not A
 ds>Delete deny denies delete-directory, so not B, see <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ds/index.html>
 The policy only grants get and describe permission on logs, so not D
 upvoted 17 times

 **mwwt2022** 2 months, 4 weeks ago

great explanation

upvoted 1 times

 **Morinator**  1 year, 2 months ago

Selected Answer: C

Explicit deny on directories, only available action for deleting is EC2

upvoted 5 times

👤 **TariqKipkemei** Most Recent 6 months ago

Selected Answer: C

Deleting Amazon EC2 instances
upvoted 1 times

👤 **Aninina** 1 year, 2 months ago

Selected Answer: C

C : Deleting Amazon EC2 instances
upvoted 1 times

👤 **mhmt4438** 1 year, 2 months ago

Selected Answer: C

Answer is C
upvoted 2 times

👤 **Aninina** 1 year, 2 months ago

C : Deleting Amazon EC2 instances
upvoted 1 times

👤 **bamishr** 1 year, 2 months ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/27873-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 3 times

Question #254

Topic 1

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

- A. Create security group rules using the instance ID as the source or destination.
- B. Create security group rules using the security group ID as the source or destination.
- C. Create security group rules using the VPC CIDR blocks as the source or destination.
- D. Create security group rules using the subnet CIDR blocks as the source or destination.

Correct Answer: B

Community vote distribution

B (100%)

 **Aninina**  1 year, 2 months ago

Selected Answer: B

B. Create security group rules using the security group ID as the source or destination.

This way, the security team can ensure that the least privileged access is given to the application tiers by allowing only the necessary communication between the security groups. For example, the web tier security group should only allow incoming traffic from the load balancer security group and outgoing traffic to the application tier security group. This approach provides a more granular and secure way to control traffic between the different tiers of the application and also allows for easy modification of access if needed.

It's also worth noting that it's good practice to minimize the number of open ports and protocols, and use security groups as a first line of defense, in addition to network access control lists (ACLs) to control traffic between subnets.

upvoted 9 times

 **Wael216**  1 year ago

Selected Answer: B

By using security group IDs, the ingress and egress rules can be restricted to only allow traffic from the necessary source or destination, and to deny all other traffic. This ensures that only the minimum required traffic is allowed between the application tiers.

Option A is not the best choice because using the instance ID as the source or destination would allow traffic from any instance with that ID, which may not be limited to the specific application tier.

Option C is also not the best choice because using VPC CIDR blocks would allow traffic from any IP address within the VPC, which may not be limited to the specific application tier.

Option D is not the best choice because using subnet CIDR blocks would allow traffic from any IP address within the subnet, which may not be limited to the specific application tier.

upvoted 7 times

 **Guru4Cloud**  6 months, 2 weeks ago

Selected Answer: B

Create security group rules using the security group ID as the source or destination.

This way, the security team can ensure that the least privileged access is given to the application tiers by allowing only the necessary communication between the security groups. For example, the web tier security group should only allow incoming traffic from the load balancer security group and outgoing traffic to the application tier security group. This approach provides a more granular and secure way to control traffic between the different tiers of the application and also allows for easy modification of access if needed.

It's also worth noting that it's good practice to minimize the number of open ports and protocols, and use security groups as a first line of defense, in addition to network access control lists (ACLs) to control traffic between subnets.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: B

A. would limit the traffic based on specific instances, which may not be the most suitable solution for applying the principle of least privilege between application tiers.

B. By using security group IDs in the rules, you can precisely control the traffic between application tiers, allowing only the necessary communication and adhering to the principle of least privilege.

C. would apply broad rules based on the entire VPC CIDR blocks, which may not provide the necessary level of granularity required for secure communication between specific application tiers.

D. would limit the traffic based on subnet CIDR blocks, which may not be sufficient for ensuring proper security between application tiers.

In summary, using security group IDs (Option B) is the recommended approach as it allows for precise control of traffic between application tiers, aligning with the principle of least privilege.

upvoted 5 times

✉ **foha2012** 2 months ago

with option A. How would you use instance ID in security group inbound rules ?

upvoted 1 times

✉ **Bmarodi** 9 months, 4 weeks ago

Selected Answer: B

I vote for option B.

upvoted 1 times

✉ **LuckyAro** 1 year, 2 months ago

Selected Answer: B

. Create security group rules using the security group ID as the source or destination

upvoted 1 times

✉ **techhb** 1 year, 2 months ago

Security Group Rulesapply to instances

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>

upvoted 1 times

✉ **mhmt4438** 1 year, 2 months ago

Selected Answer: B

Correct answer is B

upvoted 2 times

✉ **bamishr** 1 year, 2 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/46463-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

✉ **Morinator** 1 year, 2 months ago

Selected Answer: B

B right

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>

upvoted 1 times

Question #255

Topic 1

A company has an ecommerce checkout workflow that writes an order to a database and calls a service to process the payment. Users are experiencing timeouts during the checkout process. When users resubmit the checkout form, multiple unique orders are created for the same desired transaction.

How should a solutions architect refactor this workflow to prevent the creation of multiple orders?

- A. Configure the web application to send an order message to Amazon Kinesis Data Firehose. Set the payment service to retrieve the message from Kinesis Data Firehose and process the order.
- B. Create a rule in AWS CloudTrail to invoke an AWS Lambda function based on the logged application path request. Use Lambda to query the database, call the payment service, and pass in the order information.
- C. Store the order in the database. Send a message that includes the order number to Amazon Simple Notification Service (Amazon SNS). Set the payment service to poll Amazon SNS, retrieve the message, and process the order.
- D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.

Correct Answer: D*Community vote distribution*

D (100%)

 **Aninina**  1 year, 2 months ago

Selected Answer: D

D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.
 This approach ensures that the order creation and payment processing steps are separate and atomic. By sending the order information to an SQS FIFO queue, the payment service can process the order one at a time and in the order they were received. If the payment service is unable to process an order, it can be retried later, preventing the creation of multiple orders. The deletion of the message from the queue after it is processed will prevent the same message from being processed multiple times.
 It's worth noting that FIFO queues guarantee that messages are processed in the order they are received, and prevent duplicates.

upvoted 7 times

 **cookieMr**  9 months ago

Selected Answer: D

A. is not a suitable solution for preventing the creation of multiple orders. This approach does not guarantee the sequential and reliable processing of orders.
 B. is not an appropriate solution for preventing the creation of multiple orders. CloudTrail is primarily used for logging and auditing API activity, and invoking a Lambda based on the logged request does not ensure the correct order processing.
 C. is not a suitable solution. SNS is a publish-subscribe messaging service, and polling it may result in delayed processing and potential order duplication.
 D. is the correct solution. Using an SQS FIFO ensures that the orders are processed in a sequential and reliable manner, preventing the creation of multiple orders for the same transaction.

upvoted 6 times

 **TariqKipkemei**  6 months ago

Selected Answer: D

if the backend can not keep up, queue the tasks.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.

upvoted 1 times

 **animefan1** 8 months, 3 weeks ago

Selected Answer: D

The question is related in breaking down the flow. SQS is go-to choice to decouple & DB will be used to store
 upvoted 1 times

 **antropaws** 9 months, 1 week ago

Why not A?

upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

Because Kinesis Data Firehose is for ingestion of streaming data, not queuing items.

upvoted 2 times

✉ **Wael216** 1 year ago

Selected Answer: D

The use of a FIFO queue in Amazon SQS ensures that messages are processed in the order they are received.

upvoted 1 times

✉ **mhmt4438** 1 year, 2 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/95026-exam-aws-certified-solutions-architect-associate-saa-c03/>

upvoted 3 times

✉ **bamishr** 1 year, 2 months ago

Selected Answer: D

answer is d

upvoted 2 times

Question #256

Topic 1

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Correct Answer: BD

Community vote distribution

BD (100%)

✉️ LoXoL 2 months ago

Selected Answer: BD

No Brainer: B & D

upvoted 1 times

✉️ TariqKipkemei 6 months ago

Selected Answer: BD

Prevent accidental deletion of the documents = Enable MFA Delete on the bucket

Ensure that all versions of the documents are available = Enable versioning on the bucket

upvoted 2 times

✉️ Guru4Cloud 6 months, 2 weeks ago

Selected Answer: BD

Options B & D are the correct answers.

upvoted 1 times

✉️ cookieMr 9 months ago

Selected Answer: BD

B. allows multiple versions of objects in the S3 bucket to be stored. This ensures that all versions of the documents are available, even if they are accidentally overwritten or deleted.

D. adds an extra layer of protection against accidental deletion of objects in the bucket. With MFA Delete enabled, a user would need to provide an additional authentication factor to successfully delete objects from the bucket. This helps prevent accidental or unauthorized deletions and provides an extra level of security for critical documents.

A. would restrict users from modifying or uploading documents. It would not meet the requirement of allowing users to download, modify, and upload documents.

C. can control access permissions to the bucket, it does not specifically address the requirement of preventing accidental deletion or ensuring availability of all versions of the documents.

E. Encryption focuses on data protection rather than versioning and deletion prevention.

upvoted 3 times

✉️ Bmarodi 9 months, 4 weeks ago

Selected Answer: BD

Options B & D are the correct answers.

upvoted 1 times

✉️ Wael216 1 year ago

Selected Answer: BD

no doubts

upvoted 2 times

✉️ MinHyeok 1 year, 1 month ago

아몰랑 ○□ㄹ○□ㄹ

upvoted 3 times

✉ **akdavsan** 1 year, 2 months ago

Selected Answer: BD

b and d ofc

upvoted 1 times

✉ **LuckyAro** 1 year, 2 months ago

Selected Answer: BD

B & D Definitely.

upvoted 1 times

✉ **david76x** 1 year, 2 months ago

Selected Answer: BD

B & D is correct

upvoted 1 times

✉ **Aninina** 1 year, 2 months ago

Selected Answer: BD

B and D for sure guys

upvoted 2 times

✉ **mhmt4438** 1 year, 2 months ago

Selected Answer: BD

<https://www.examtopics.com/discussions/amazon/view/21969-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

Question #257

Topic 1

A company is building a solution that will report Amazon EC2 Auto Scaling events across all the applications in an AWS account. The company needs to use a serverless solution to store the EC2 Auto Scaling status data in Amazon S3. The company then will use the data in Amazon S3 to provide near-real-time updates in a dashboard. The solution must not affect the speed of EC2 instance launches.

How should the company move the data to Amazon S3 to meet these requirements?

- A. Use an Amazon CloudWatch metric stream to send the EC2 Auto Scaling status data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
- B. Launch an Amazon EMR cluster to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
- C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.
- D. Use a bootstrap script during the launch of an EC2 instance to install Amazon Kinesis Agent. Configure Kinesis Agent to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

Correct Answer: A

Community vote distribution

A (83%)	C (17%)
---------	---------

✉ **pentium75** Highly Voted 2 months, 4 weeks ago

Selected Answer: A

B - EMR cluster is for Big Data, has nothing to do with this
 C - invokes the function "on a schedule", but you want to capture events
 D - Could work, but would be overcomplex and would "affect the speed of EC2 instance launches" (which it should not)
 upvoted 5 times

✉ **LoXoL** 2 months ago

Right.

upvoted 1 times

✉ **reviewmine** Most Recent 1 month ago

Selected Answer: A

Answer A: Near real time --> Amazon Kinesis Data Firehose
 upvoted 2 times

✉ **TariqKipkemei** 6 months ago

Selected Answer: A

You can use metric streams to continually stream CloudWatch metrics to a destination of your choice, with near-real-time delivery and low latency. Supported destinations include AWS destinations such as Amazon Simple Storage Service and several third-party service provider destinations. Main usage scenarios for CloudWatch metric streams: Data lake—Create a metric stream and direct it to an Amazon Kinesis Data Firehose delivery stream that delivers your CloudWatch metrics to a data lake such as Amazon S3.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Metric-Streams.html#:~:text=CloudWatch%20metric%20streams>

upvoted 3 times

✉ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

This solution meets the requirements because it is serverless and does not affect the speed of EC2 instance launches. Amazon CloudWatch metric streams can continuously stream CloudWatch metrics to destinations such as Amazon S3. Amazon Kinesis Data Firehose can capture, transform, and deliver streaming data into data lakes, data stores, and analytics services. It can directly put the data into Amazon S3, which can then be used for near-real-time updates in a dashboard.
 upvoted 4 times

✉ **Valder21** 6 months, 3 weeks ago

Selected Answer: C

Kinesis is for data streams not events. So, C
 upvoted 1 times

✉ **pentium75** 2 months, 4 weeks ago

C invokes the Lambda function "on a schedule". It would collect the scaling status during its runs. But you don't want the hourly status, you want to report "scaling events".

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: A

B. introduces unnecessary complexity and overhead for collecting and sending the EC2 Auto Scaling status data to S3. It is not the most efficient serverless solution for this specific requirement.

C. would introduce delays in data updates, as it is not triggered in real-time. Additionally, it adds unnecessary overhead and complexity compared to using a direct data stream.

D. introduces additional dependencies and management overhead. It may also impact the speed of EC2 instance launches, which is a requirement that needs to be avoided.

Overall, option A provides a streamlined and serverless solution by leveraging CloudWatch metric streams and Kinesis Data Firehose to efficiently capture and store the EC2 Auto Scaling status data in S3 without affecting the speed of EC2 instance launches.

upvoted 4 times

 **markw92** 9 months, 1 week ago

A: I was thinking D is the answer but the solution should not impact ec2 launches will make the difference and i fast read the question. A is a right choice.

upvoted 1 times

 **Rahulbit34** 10 months, 3 weeks ago

A because of near real time scenario

upvoted 3 times

 **UnluckyDucky** 1 year ago

Selected Answer: C

Both A and C are applicable - no doubt there.

C is more straightforward and to the point of the question imho.

upvoted 3 times

 **UnluckyDucky** 1 year ago

Changing my answer to *A* as the dashboard will provide near-real updates.

Unless the lambda is configured to run every minute which is not common with schedules - it is not considered near real-time.

upvoted 3 times

 **bdp123** 1 year, 1 month ago

Selected Answer: A

Serverless solution and near real time

upvoted 3 times

 **Stanislav4907** 1 year, 1 month ago

Selected Answer: A

near real time - eliminates c

upvoted 1 times

 **aakashkumar1999** 1 year, 1 month ago

Selected Answer: A

Answer is A

upvoted 1 times

 **devonwho** 1 year, 1 month ago

Selected Answer: A

You can use metric streams to continually stream CloudWatch metrics to a destination of your choice, with near-real-time delivery and low latency. One of the use cases is Data Lake: create a metric stream and direct it to an Amazon Kinesis Data Firehose delivery stream that delivers your CloudWatch metrics to a data lake such as Amazon S3.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Metric-Streams.html>

upvoted 2 times

 **Stanislav4907** 1 year, 1 month ago

Selected Answer: A

Option C, using an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule to send the EC2 Auto Scaling status data directly to Amazon S3, may not be the best choice because it may not provide real-time updates to the dashboard.

A schedule-based approach with an EventBridge rule and Lambda function may not be able to deliver the data in near real-time, as the EC2 Auto Scaling status data is generated dynamically and may not always align with the schedule set by the EventBridge rule.

Additionally, using a schedule-based approach with EventBridge and Lambda also has the potential to create latency, as there may be a delay between the time the data is generated and the time it is sent to S3.

In this scenario, using Amazon CloudWatch and Kinesis Data Firehose as described in Option A, provides a more reliable and near real-time solution.

upvoted 1 times

 **MikelH93** 1 year, 1 month ago

Selected Answer: A

A seems to be the right answer. Don't think C could be correct as it says "near real-time" and C is on schedule

upvoted 1 times

 **KAUS2** 1 year, 1 month ago

Selected Answer: C

C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

"On a schedule" but you want to capture events, not a regular status report.

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: A

A seemsright choice but serverless keyword confuses, and cloud watch metric steam is server less too.

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

But A is serverless.

upvoted 1 times

Question #258

Topic 1

A company has an application that places hundreds of .csv files into an Amazon S3 bucket every hour. The files are 1 GB in size. Each time a file is uploaded, the company needs to convert the file to Apache Parquet format and place the output file into an S3 bucket.

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

- A. Create an AWS Lambda function to download the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Invoke the Lambda function for each S3 PUT event.
- B. Create an Apache Spark job to read the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the Spark job.
- C. Create an AWS Glue table and an AWS Glue crawler for the S3 bucket where the application places the .csv files. Schedule an AWS Lambda function to periodically use Amazon Athena to query the AWS Glue table, convert the query results into Parquet format, and place the output files into an S3 bucket.
- D. Create an AWS Glue extract, transform, and load (ETL) job to convert the .csv files to Parquet format and place the output files into an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the ETL job.

Correct Answer: A

Community vote distribution



✉️ Parsons **Highly Voted** 1 year, 2 months ago

Selected Answer: D

No, D should be correct.

"LEAST operational overhead" => Should you fully manage service like Glue instead of manually like the answer A.
upvoted 13 times

✉️ awsgeek75 2 months, 3 weeks ago

I also think it's D but remember that D requires writing ETL logic in AWS Glue (nothing in question says how complex it will be). AWS Lambda for CSV could be simple also (imagine NodeJS and millions of libraries support or Python's parsing) so both could be operationally on par to each other. Logically D makes more sense but in practice, AWS Glue rarely works with out of the box ETL and becomes a maintenance overhead in itself.

upvoted 1 times

✉️ aws4myself **Highly Voted** 1 year, 1 month ago

Here A is the correct answer. The reason here is the least operational overhead.

A ==> S3 - Lambda - S3

D ==> S3 - Lambda - Glue - S3

Also, glue cannot convert on fly automatically, you need to write some code there. If you write the same code in lambda it will convert the same and push the file to S3

Lambda has max memory of 128 MB to 10 GB. So, it can handle it easily.

And we need to consider cost also, glue cost is more. Hope many from this forum realize these differences.

upvoted 5 times

✉️ LuckyAro 1 year, 1 month ago

We also need to stay with the question, cost was not a consideration in the question.

upvoted 1 times

✉️ nder 1 year ago

Cost is not a factor. AWS Glue is a fully managed service therefore, it's the least operational overhead

upvoted 3 times

✉️ TariqKipkemei **Most Recent** 6 months ago

Selected Answer: D

AWS Glue can run your extract, transform, and load (ETL) jobs as new data arrives. For example, you can configure AWS Glue to initiate your ETL jobs to run as soon as new data becomes available in Amazon Simple Storage Service (S3). Clearly you don't need a lambda function to initiate the ETL job.

<https://aws.amazon.com/glue/#:~:text=to%20initiate%20your-,ETL,-jobs%20to%20run>

Option A requires writing code to perform the file conversion.

In the exam option D would be the best answer.

upvoted 3 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

This solution meets the requirements with the least operational overhead because AWS Glue is a fully managed ETL service that makes it easy to move data between data stores. AWS Glue can read .csv files from an S3 bucket and write the data into Parquet format in another S3 bucket. The AWS Lambda function can be triggered by an S3 PUT event when a new .csv file is uploaded, and it can start the AWS Glue ETL job to convert the file to Parquet format. This solution does not require managing any servers or clusters, which reduces operational overhead.

upvoted 3 times

 **cookieMr** 9 months ago

D is correct

upvoted 1 times

 **cookieMr** 9 months ago

A. introduces significant operational overhead. This approach requires managing the Lambda, handling concurrency, and ensuring proper error handling for large file sizes, which can be challenging.

B. adds unnecessary complexity and operational overhead. Managing the Spark job, handling scalability, and coordinating the Lambda invocations for each file upload can be cumbersome.

C. introduces additional complexity and may not be the most efficient solution. It involves managing Glue resources, scheduling Lambda, and querying data even when no new files are uploaded.

Option D leverages AWS Glue's ETL capabilities, allowing you to define and execute a data transformation job at scale. By invoking the ETL job using an Lambda function for each S3 PUT event, you can ensure that files are efficiently converted to Parquet format without the need for manual intervention. This approach minimizes operational overhead and provides a streamlined and scalable solution.

upvoted 3 times

 **F629** 9 months, 1 week ago

Selected Answer: A

Both A and D can work, but A is more simple. It's closer to the "Least Operational effort".

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Creating, maintaining and supporting custom code that does the same as a ready-made serverless service is NEVER "least operational effort".

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Oh, and A can't handle 1 GB files.

upvoted 1 times

 **jaswantn** 1 month, 2 weeks ago

Now Lambda supports 1 GB to 10 GB.

upvoted 1 times

 **shanwford** 11 months, 3 weeks ago

Selected Answer: D

The maximum size for a Lambda event payload is 256 KB - so (A) didn't work with 1GB Files. Glue is recommended for the Parquet Transformation of AWS.

upvoted 2 times

 **jennyka76** 1 year, 1 month ago

ANS - d

<https://aws.amazon.com/blogs/database/how-to-extract-transform-and-load-data-for-analytic-processing-using-aws-glue-part-2/>

- READ ARTICLE -

upvoted 2 times

 **JayBee65** 1 year, 2 months ago

A is unlikely to work as Lambda may struggle with 1GB size: "< 64 MB, beyond which Lambda is likely to hit memory caps", see <https://stackoverflow.com/questions/41504095/creating-a-parquet-file-on-aws-lambda-function>

upvoted 2 times

 **jainparag1** 1 year, 2 months ago

Should be D as Glue is a self-managed service and provides the job for converting CSV files to Parquet off the shelf.

upvoted 1 times

 **Joxtat** 1 year, 2 months ago

Selected Answer: D

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>

upvoted 1 times

 **techhb** 1 year, 2 months ago

AWS Glue is the right solution here.

upvoted 1 times

 **mp165** 1 year, 2 months ago

Selected Answer: D

I am thinking D.

A says lambda will download the .csv...but to where? that seem manual based on that

upvoted 1 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: A

I think A

upvoted 1 times

 **bamishr** 1 year, 2 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/83201-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Question #259

Topic 1

A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.

Which solution should a solutions architect recommend to meet these requirements?

- A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.
- B. Configure a backup window for the RDS DB instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions.
- C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years.
- D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target. Configure S3 Lifecycle policies to delete the snapshots after 2 years.

Correct Answer: A

Community vote distribution

A (96%) 4%

cookieMr Highly Voted 9 months ago

Selected Answer: A

- A. suggests using AWS Backup, a centralized backup management service, to retain RDS backups. A backup vault is created, and a backup plan is defined with a daily schedule and a 2-year retention period for backups. RDS DB instances are assigned to this backup plan.
- B. it does not address the requirement for consistent and restorable backups. Snapshots are point-in-time backups and may not provide the desired level of consistency.
- C. it is not designed to provide the backup and restore functionality required for databases. It does not ensure the backups are consistent or provide an easy restore mechanism.
- D. it does not address the requirement for daily backups and retention of consistent backups. It focuses more on replication and change data capture rather than backup and restore.

upvoted 8 times

Ojonugwa Most Recent 4 days, 2 hours ago

The solution architect should recommend option B - Configure a backup window for the RDS DB instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions.

This meets the requirements of:

Retaining daily backups for a minimum of 2 years. The daily snapshots captured within the backup window provide consistent, restorable backups on a daily basis.

Assigning a snapshot retention policy of 2 years ensures the snapshots are retained for the required period.

Using Amazon DLM allows automatically deleting snapshots older than 2 years to comply with the retention period in a cost-effective manner without manual administration.

The other option of using AWS Backup vault is not as suitable since it has limitations such as 35 day maximum retention for automated backups. Option B provides a native RDS solution capable of meeting the long term 2 year retention requirements.

upvoted 1 times

vijaykamal 5 months, 4 weeks ago

Selected Answer: B

Here's why Option B is the best choice:

Backup Window: Configuring a backup window for daily snapshots ensures that consistent backups are taken at the specified time each day. This helps maintain data integrity and consistency.

Snapshot Retention Policy: Assigning a snapshot retention policy of 2 years to each RDS DB instance ensures that the backups are retained for the required duration.

Amazon Data Lifecycle Manager (Amazon DLM): Amazon DLM can be used to automate the management of EBS snapshots, including RDS snapshots. You can configure Amazon DLM to schedule snapshot deletions, making it easier to manage the retention policy without manual intervention.

Option A (AWS Backup) is primarily used for managing backups of resources that may not have built-in backup capabilities, but for Amazon RDS, it's better to use the built-in snapshot capabilities and Amazon DLM for snapshot retention.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

"AWS Backup is primarily used for managing backups of resources that may not have built-in backup capabilities" says who?

upvoted 2 times

 **TariqKipkemei** 6 months ago

Selected Answer: A

Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan

upvoted 1 times

 **animefan1** 8 months, 3 weeks ago

Selected Answer: A

Backups work with EBS, FSX, RDS. Its managed & can has vault option for more better control over backup retention

upvoted 3 times

 **markw92** 9 months, 1 week ago

Why not B?

upvoted 2 times

 **_deepsi_dee29** 10 months ago

Selected Answer: A

A is correct

upvoted 1 times

 **antropaws** 10 months ago

Why not D?

Creating tasks for ongoing replication using AWS DMS: You can create an AWS DMS task that captures ongoing changes from the source data store. You can do this capture while you are migrating your data. You can also create a task that captures ongoing changes after you complete your initial (full-load) migration to a supported target data store. This process is called ongoing replication or change data capture (CDC). AWS DMS uses this process when replicating ongoing changes from a source data store.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Requirement is backup, not migration.

upvoted 2 times

 **gold4otas** 12 months ago

Selected Answer: A

A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: A

A is right choice

upvoted 3 times

 **Aninina** 1 year, 2 months ago

Selected Answer: A

A A A A A A

upvoted 2 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **bamishr** 1 year, 2 months ago

Selected Answer: A

Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.

upvoted 4 times

Question #260

Topic 1

A company's compliance team needs to move its file shares to AWS. The shares run on a Windows Server SMB file share. A self-managed on-premises Active Directory controls access to the files and folders.

The company wants to use Amazon FSx for Windows File Server as part of the solution. The company must ensure that the on-premises Active Directory groups restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS. The company has created an FSx for Windows File Server file system.

Which solution will meet these requirements?

- A. Create an Active Directory Connector to connect to the Active Directory. Map the Active Directory groups to IAM groups to restrict access.
- B. Assign a tag with a Restrict tag key and a Compliance tag value. Map the Active Directory groups to IAM groups to restrict access.
- C. Create an IAM service-linked role that is linked directly to FSx for Windows File Server to restrict access.
- D. Join the file system to the Active Directory to restrict access.

Correct Answer: D

Community vote distribution



mhmt4438 1 year, 2 months ago

Selected Answer: D

D. Join the file system to the Active Directory to restrict access.

Joining the FSx for Windows File Server file system to the on-premises Active Directory will allow the company to use the existing Active Directory groups to restrict access to the file shares, folders, and files after the move to AWS. This option allows the company to continue using their existing access controls and management structure, making the transition to AWS more seamless.

upvoted 17 times

bujuman 1 month ago

Selected Answer: D

D is relevant and accurate answer when we consider this:

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/creating-joined-ad-file-systems.html>

"When you create a new FSx for Windows File Server file system, you can configure Microsoft Active Directory integration so that it joins to your self-managed Microsoft Active Directory domain. To do this, provide the following information for your Microsoft Active Directory"

upvoted 2 times

awsgeek75 2 months, 1 week ago

Selected Answer: A

The on-premise AD already has restrictions via group in place so D makes no sense as the groups are already linked to file system.

"The company must ensure that the on-premises Active Directory groups restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS."

The question is about linking the on-prem permissions to the new FSx server on AWS and this can only be done by A

upvoted 1 times

awsgeek75 2 months, 1 week ago

Actually neither A nor D make sense.

"A self-managed on-premises Active Directory controls access to the files and folders." This makes D sound useless and at the same time does not allow the on-prem AD to control file access on FSx.

A uses IAM roles which is irrelevant to this setup.

BC are totally wrong

upvoted 1 times

meowruki 3 months, 3 weeks ago

Selected Answer: D

Option A: Creating an Active Directory Connector and mapping groups to IAM groups is more relevant for AWS Directory Service, such as AWS Managed Microsoft AD, and not for integrating with existing on-premises Active Directory.

Option B: Using tags is typically not used for access control purposes. Tags are metadata and are not directly involved in user authentication and authorization.

Option C: Creating an IAM service-linked role directly linked to FSx for Windows File Server is not the standard approach for integrating with existing on-premises Active Directory.

upvoted 2 times

 **wrmari** 5 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html>

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

This allows the on-premises Active Directory to manage permissions to the FSx file shares, meeting the key requirement to use existing AD groups to control access after migrating to AWS.

Joining FSx to the AD domain allows the native file system permissions, users, and groups to be applied from Active Directory. Access is handled seamlessly via the trust relationship between FSx and AD.

The other options would not leverage the existing AD identities and groups

upvoted 2 times

 **Guru4Cloud** 6 months, 2 weeks ago

The other options would not leverage the existing AD identities and groups:

A) AD Connector and IAM groups would require re-mapping AD groups to IAM, adding complexity. Native AD integration is simpler.

B) Tags and IAM groups also don't use native AD semantics.

C) Service-linked roles are not applicable for managing end user access.

So D is the correct option to meet the requirements using the native Active Directory integration built into FSx for Windows.

upvoted 2 times

 **mtmayer** 7 months, 3 weeks ago

Selected Answer: A

The AD is on-premises... You need the connector.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: D

D. allows the file system to leverage the existing AD infrastructure for authentication and access control.

Option A is incorrect because mapping the AD groups to IAM groups is not applicable in this scenario. IAM is primarily used for managing access to AWS resources, while the requirement is to integrate with the on-premises AD for access control.

Option B is incorrect because assigning a tag with a Restrict tag key and a Compliance tag value does not provide the necessary integration with the on-premises AD for access control. Tags are used for organizing and categorizing resources and do not provide authentication or access control mechanisms.

Option C is incorrect because creating an IAM service-linked role linked directly to FSx for Windows File Server does not integrate with the on-premises AD. IAM roles are used within AWS for managing permissions and do not provide the necessary integration with external AD systems.

upvoted 4 times

 **Mia2009687** 9 months ago

Selected Answer: D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>

upvoted 1 times

 **kraken21** 12 months ago

Selected Answer: D

Other options are referring to IAM based control which is not possible. Existing AD should be used without IAM.

upvoted 2 times

 **Abhineet9148232** 1 year ago

Selected Answer: D

<https://aws.amazon.com/blogs/storage/using-amazon-fsx-for-windows-file-server-with-an-on-premises-active-directory/>

upvoted 2 times

 **somsundar** 1 year ago

Answer D. Amazon FSx does not support Active Directory Connector .

upvoted 2 times

 **Abhineet9148232** 1 year ago

Selected Answer: D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html>

upvoted 3 times

Yelizaveta 1 year, 1 month ago

Selected Answer: D

Note:

Amazon FSx does not support Active Directory Connector and Simple Active Directory.

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>

upvoted 3 times

aakashkumar1999 1 year, 1 month ago

Selected Answer: A

The answer will be AD connector so : A, it will create a proxy between your onpremises AD which you can use to restrict access
upvoted 2 times

Stanislav4907 1 year, 1 month ago

Selected Answer: D

Option D: Join the file system to the Active Directory to restrict access.

Joining the FSx for Windows File Server file system to the on-premises Active Directory allows the company to use the existing Active Directory groups to restrict access to the file shares, folders, and files after the move to AWS. By joining the file system to the Active Directory, the company can maintain the same access control as before the move, ensuring that the compliance team can maintain compliance with the relevant regulations and standards.

Options A and B involve creating an Active Directory Connector or assigning a tag to map the Active Directory groups to IAM groups, but these options do not allow for the use of the existing Active Directory groups to restrict access to the file shares in AWS.

Option C involves creating an IAM service-linked role linked directly to FSx for Windows File Server to restrict access, but this option does not take advantage of the existing on-premises Active Directory and its access control.

upvoted 3 times

KAUS2 1 year, 1 month ago

Selected Answer: A

A is correct

Use AD Connector if you only need to allow your on-premises users to log in to AWS applications and services with their Active Directory credentials. You can also use AD Connector to join Amazon EC2 instances to your existing Active Directory domain.

Pls refer - https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html#adconnector

upvoted 3 times

mbuck2023 9 months, 2 weeks ago

wrong, answer is D. Amazon FSx does not support Active Directory Connector and Simple Active Directory. See also <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html>.

upvoted 1 times

Question #261

Topic 1

A company recently announced the deployment of its retail website to a global audience. The website runs on multiple Amazon EC2 instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones.

The company wants to provide its customers with different versions of content based on the devices that the customers use to access the website.

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

- A. Configure Amazon CloudFront to cache multiple versions of the content.
- B. Configure a host header in a Network Load Balancer to forward traffic to different instances.
- C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.
- D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.
- E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.

Correct Answer: AC

Community vote distribution

AC (100%)

✉️  Parsons  1 year, 2 months ago

Selected Answer: AC

A, C is correct.

NLB lister rule only supports Protocol & Port (Not host/based routing like ALB) => D, E is incorrect.
NLB just works layer 4 (TCP/UDP) instead of Layer 7 (HTTP) => B is incorrect.

After eliminating, AC should be the answer.

upvoted 14 times

✉️  Guru4Cloud  6 months, 2 weeks ago

Selected Answer: AC

A. allows customers to receive the appropriate version of the content based on their location and device type.

C. By creating a Lambda@Edge, you can inspect the User-Agent header of incoming requests and determine the type of device being used. Based on this information, you can customize the response and send the appropriate version of the content to the user.

upvoted 5 times

✉️  Ruffyit  4 months, 1 week ago

A C

Configure Amazon CloudFront to cache multiple versions of the content.

Configure a function to send specific objects to users based on the User-Agent header.

upvoted 1 times

✉️  sunhouse 5 months, 1 week ago

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html>

upvoted 1 times

✉️  rrbrish73 5 months, 2 weeks ago

<https://medium.com/swlh/serve-different-content-based-on-user-agent-in-aws-cloudfront-using-lambda-edge-28877294340b>

upvoted 1 times

✉️  cookieMr 9 months ago

Selected Answer: AC

A. allows customers to receive the appropriate version of the content based on their location and device type.

C. By creating a Lambda@Edge, you can inspect the User-Agent header of incoming requests and determine the type of device being used. Based on this information, you can customize the response and send the appropriate version of the content to the user.

B. does not address the requirement of serving different content versions based on device types.

D. & E. do not address the device-specific content requirement.

Therefore, options A and C are the correct combination of actions to meet the requirement of providing different versions of content based on the devices that customers use to access the website.

upvoted 3 times

 **Yadav_Sanjay** 10 months, 1 week ago

Selected Answer: AC

NLB does not support routing

upvoted 1 times

 **omoakin** 10 months, 2 weeks ago

A C

Configure Amazon CloudFront to cache multiple versions of the content.

Configure a function to send specific objects to users based on the User-Agent header.

upvoted 1 times

 **omoakin** 10 months, 2 weeks ago

C

Configure a function to send specific objects to users based on the User-Agent header.

upvoted 1 times

 **GalileoEC2** 1 year ago

Using a Directory Connector to connect the on-premises Active Directory to AWS is one way to enable access to AWS resources, including Amazon FSx for Windows File Server. However, joining the Amazon FSx for Windows File Server file system to the on-premises Active Directory is a separate step that allows you to control access to the file shares using the same Active Directory groups that are used on-premises.

upvoted 1 times

 **LoXeras** 1 year ago

I guess this belongs to the question before #260

upvoted 2 times

 **wors** 1 year, 1 month ago

So will this mean the entire architecture needs to move to lambda in order to leverage off lambda edge? This doesn't make sense as the question outlines the architecture already in ec2, asg and elb?

Just looking for clarification if I am missing something

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

No, Lambda function will just do something like "if user-agent is 'iOS' then send content from elb-01 otherwise send content from elb-02".

upvoted 1 times

 **devonwho** 1 year, 1 month ago

Selected Answer: AC

AC are the correct answers.

For C:

IMPROVED USER EXPERIENCE

Lambda@Edge can help improve your users' experience with your websites and web applications across the world, by letting you personalize content for them without sacrificing performance.

Real-time Image Transformation

You can customize your users' experience by transforming images on the fly based on the user characteristics. For example, you can resize images based on the viewer's device type—mobile, desktop, or tablet. You can also cache the transformed images at CloudFront Edge locations to further improve performance when delivering images.

<https://aws.amazon.com/lambda/edge/>

upvoted 2 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: AC

Correct answer is A,C

upvoted 3 times

 **Aninina** 1 year, 2 months ago

Selected Answer: AC

C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.

Lambda@Edge allows you to run a Lambda function in response to specific CloudFront events, such as a viewer request, an origin request, a response, or a viewer response.

upvoted 2 times

 **Morinator** 1 year, 2 months ago

Selected Answer: AC

<https://www.examtopics.com/discussions/amazon/view/67881-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

Question #262

Topic 1

A company plans to use Amazon ElastiCache for its multi-tier web application. A solutions architect creates a Cache VPC for the ElastiCache cluster and an App VPC for the application's Amazon EC2 instances. Both VPCs are in the us-east-1 Region.

The solutions architect must implement a solution to provide the application's EC2 instances with access to the ElastiCache cluster.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
- B. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
- C. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the peering connection's security group to allow inbound connection from the application's security group.
- D. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the Transit VPC's security group to allow inbound connection from the application's security group.

Correct Answer: A

Community vote distribution

A (100%)

 **mhmt4438**  1 year, 2 months ago

Selected Answer: A

A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

Creating a peering connection between the VPCs allows the application's EC2 instances to communicate with the ElastiCache cluster directly and efficiently. This is the most cost-effective solution as it does not involve creating additional resources such as a Transit VPC, and it does not incur additional costs for traffic passing through the Transit VPC. Additionally, it is also more secure as it allows you to configure a more restrictive security group rule to allow inbound connection from only the application's security group.

upvoted 12 times

 **Ruffyit**  4 months, 1 week ago

A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

Creating a peering connection between the VPCs allows the application's EC2 instances to communicate with the ElastiCache cluster directly and efficiently. This is the most cost-effective solution as it does not involve creating additional resources such as a Transit VPC, and it does not incur additional costs for traffic passing through the Transit VPC. Additionally, it is also more secure as it allows you to configure a more restrictive security group rule to allow inbound connection from only the application's security group.

upvoted 1 times

 **TariqKipkemei** 6 months ago

Selected Answer: A

Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

Create a VPC peering connection between the Cache VPC and App VPC. This allows private IP connectivity between the VPCs. Add route table entries in each VPC to route traffic destined to the other VPC via the peering connection. This enables network routing. Configure security groups to allow inbound connections from the application instances to the ElastiCache cluster.

upvoted 1 times

 **cookieMr** 9 months ago

Selected Answer: A

Creating a peering connection between the VPCs is a cost-effective way to establish connectivity. By adding a route table entry for the peering connection in both VPCs, traffic can flow between them. Configuring an inbound rule in the ElastiCache cluster's security group allows inbound connections from the application's security group, enabling access to the ElastiCache cluster from the EC2 instances in the App VPC.

Option B suggests creating a Transit VPC, which adds unnecessary complexity and cost for this scenario.

Option C suggests configuring an inbound rule for the peering connection's security group, which is not necessary as the security group for the

ElastiCache cluster should be used to control inbound connections.

Option D suggests configuring an inbound rule for the Transit VPC's security group, which is not needed in this case and adds unnecessary complexity.

Therefore, option A is the most cost-effective solution to provide the application's EC2 instances with access to the ElastiCache cluster.
upvoted 2 times

 **smartegnine** 9 months, 2 weeks ago

Selected Answer: A

A is correct,

1. VPC transit is used for more complex architecture and can do VPCs to VPCs connectivity. But for simple VPC 2 VPC can use peer connection.
2.To enable private IPv4 traffic between instances in peered VPCs, you must add a route to the route tables associated with the subnets for both instances.

So base on 1, B and D are out, base on 2 C is out
upvoted 1 times

 **wRhIH** 9 months, 3 weeks ago

Why not C ? any explanation?

upvoted 1 times

 **smartegnine** 9 months, 2 weeks ago

To enable private IPv4 traffic between instances in peered VPCs, you must add a route to the route tables associated with the subnets for both instances.

<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-routing.html>

upvoted 1 times

 **smartegnine** 9 months, 1 week ago

Application read from ElasticCache, not viseversa, so inbound rule should be ElasticCach

upvoted 2 times

 **Cor5in** 9 months ago

Thank you Sir!

upvoted 1 times

 **nder** 1 year ago

Selected Answer: A

Cost Effectively!

upvoted 1 times

Question #263

Topic 1

A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

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

- A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.
- B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.
- C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.
- D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.
- E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Correct Answer: AD

Community vote distribution

AD (100%)

✉️  **TariqKipkemei** 6 months ago

Selected Answer: AD

Company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling = Serverless = ECS with Fargate.
upvoted 1 times

✉️  **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: AD

ECS allows deploying and managing containers without having to provision the underlying infrastructure. This minimizes maintenance effort. Using Fargate launch type means ECS will handle provisioning and scaling the infrastructure automatically. This removes the management overhead for the company.

Running multiple tasks and specifying desired count ≥ 2 will provide high availability across Availability Zones.

Together, ECS plus Fargate provide a fully managed container platform. The company doesn't need to provision or manage servers.
upvoted 2 times

✉️  **cookieMr** 9 months ago

Selected Answer: AD

Options B and E suggest deploying the Kubernetes control plane and worker nodes on EC2 instances, which would require managing the infrastructure and add ongoing maintenance overhead, contrary to the requirement of minimizing effort.

Option C suggests using the Amazon EC2 launch type for ECS, which still requires managing EC2 instances and is not as cost-effective and scalable as using Fargate.

Therefore, the combination of deploying an Amazon ECS cluster and an ECS service with a Fargate launch type (options A and D) is the most suitable for minimizing maintenance and scaling effort without managing additional infrastructure.
upvoted 4 times

✉️  **LoXeras** 1 year ago

Selected Answer: AD

AWS Fargate is server less solution to use on ECS: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/AWS_Fargate.html
upvoted 2 times

✉️  **lambda15** 1 year ago

why is c is incorrect ?

upvoted 1 times

✉️  **Julio98** 1 year ago

Because in the question says, "minimizes the amount of ongoing effort for maintenance and scaling", and EC2 instances you need effort to maintain the infrastructure unlike fargate that is serverless.
upvoted 3 times

✉️  **Whericanstart** 1 year ago

Selected Answer: AD

Amazon Fargate is a service that is fully manageable by Amazon; it offers provisioning, configuration and scaling feature. It is "serverless".

upvoted 1 times

✉️ **AlessandraSAA** 1 year ago

Selected Answer: AD

ECS has 2 launch type, EC2 (you maintain the infra) and Fargate (serverless). Since the question ask for no additional infra to manage it should be Fargate.

upvoted 4 times

✉️ **devonwho** 1 year, 1 month ago

Selected Answer: AD

AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers.

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html>

upvoted 3 times

✉️ **Aninina** 1 year, 2 months ago

A D is the correct answer

upvoted 1 times

✉️ **mhmt4438** 1 year, 2 months ago

Selected Answer: AD

A,D is correct answer

upvoted 2 times

✉️ **AHUI** 1 year, 2 months ago

AD:

<https://www.examtopics.com/discussions/amazon/view/60032-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

✉️ **Morinator** 1 year, 2 months ago

Selected Answer: AD

AD - EC2 out for this, cluster + fargate is the right answer

upvoted 4 times

Question #264

Topic 1

A company has a web application hosted over 10 Amazon EC2 instances with traffic directed by Amazon Route 53. The company occasionally experiences a timeout error when attempting to browse the application. The networking team finds that some DNS queries return IP addresses of unhealthy instances, resulting in the timeout error.

What should a solutions architect implement to overcome these timeout errors?

- A. Create a Route 53 simple routing policy record for each EC2 instance. Associate a health check with each record.
- B. Create a Route 53 failover routing policy record for each EC2 instance. Associate a health check with each record.
- C. Create an Amazon CloudFront distribution with EC2 instances as its origin. Associate a health check with the EC2 instances.
- D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

Correct Answer: D

Community vote distribution



✉️ **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

ALB performs health checks on the EC2 instances, so it will only route traffic to healthy instances. This avoids the timeout errors.

ALB provides load balancing across the instances, improving performance and availability.

Route 53 routes to the ALB DNS name, so you don't have to manage records for each EC2 instance.

This is a standard and robust architecture for public-facing web applications. The ALB acts as the entry point and handles health checks and scaling.
upvoted 9 times

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

Selected Answer: B

It is not clear from the question whether the 10 EC2s are running within the same region. ALB can only direct traffic within region, while route 53 can route traffic to multiple locations, hence C and D are wrong.

upvoted 7 times

✉️ **pentium75** 2 months, 4 weeks ago

But B has one primary record and 9 failover records. A is correct, simple policy with health checks, that makes sure that only IPs of healthy instances are returned.

upvoted 2 times

✉️ **Hrishi_707** 2 weeks, 3 days ago

Those who are confused between A and D, A is wrong as you can't associate a health check with Simple routing policy record.

upvoted 1 times

✉️ **MrPCarrot** 1 month, 1 week ago

D is the best answer

upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

If you focus on the question, both A and D seems to be correct.

A is correct because simple routing policy for health check is doable BUT it is also wrong because we don't know how to determine the health of instance.

D is correct because "The company occasionally experiences a timeout error when attempting to browse the application" which suggest application is being accessed by a browser with means it's HTTP based and ALB is better for HTTP based healthchecks.

A web application timing out is not necessarily unhealthy instance, strictly speaking. It's just bad web application running on a healthy instance! So A may not be correct also.

upvoted 3 times

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

Selected Answer: D

Although B can work as well, but it's nor a professional choice to associate the healthcheck with 10 EC2 instances, ALB is better option here.

A is incorrect: Simple Routing Policies Can't be associated with Health Checks

C is incorrect: Cloudfront is for caching content which is irrelevant.

upvoted 2 times

✉️ **awsgeek75** 2 months, 3 weeks ago

Simple routing policies can be associated with Health Checks <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-simple-configs.html>

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

Selected Answer: A

A meets the requirement ("overcome these timeout errors") without any other changes.

"If you configure health checking for all the records in a group of records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or failover), Route 53 responds to DNS queries by choosing a healthy record and returning the applicable value from that record. (<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-how-route-53-chooses-records.html>)

upvoted 2 times

 **pentium75** 2 months, 4 weeks ago

"You can use Route 53 health checking to configure active-active and active-passive failover configurations. You configure active-active failover using any routing policy (or combination of routing policies) other than failover. ... Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Route 53 can detect that it's unhealthy and stop including it when responding to queries.

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

In active-active failover, all the records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or latency) are active unless Route 53 considers them unhealthy. Route 53 can respond to a DNS query using any healthy record." (<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html#dns-failover-types-active-passive>)

upvoted 1 times

 **pentium75** 2 months, 4 weeks ago

B - No, "you configure active-active failover using any routing policy (or combination of routing policies) OTHER THAN FAILOVER". With B, all traffic would go one primary instance unless it is unhealthy.

C - Not sure how to configure multiple EC2 instances as the origin without an LB. Even if that would be possible it would introduce more changes and complexity, which is not asked for.

D - Would work if all EC2 instances are in the same region, which we don't know. But it would also incur additional cost and potentially have other effects.

upvoted 1 times

 **Ruffyit** 4 months, 1 week ago

B is wrong.

The DNS cache in clients could drive to timeouts. With ALB this issue won't happen since the DNS register will be the same and ALB will take care of unhealthy nodes.

upvoted 2 times

 **rlamberti** 5 months ago

Selected Answer: D

B is wrong.

The DNS cache in clients could drive to timeouts. With ALB this issue won't happen since the DNS register will be the same and ALB will take care of unhealthy nodes.

upvoted 2 times

 **daniel1** 5 months, 2 weeks ago

Selected Answer: D

D. **Application Load Balancer (ALB) with Health Checks, Routed via Route 53**:

- Creating an ALB in front of the EC2 instances and configuring health checks on the ALB will ensure that only healthy instances receive traffic. Route 53 can then direct traffic to the ALB, which in turn, routes traffic to healthy instances based on the health check results.

Among the provided options, the one that directly addresses the issue of routing traffic only to healthy instances is:

D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

upvoted 3 times

 **TariqKipkemei** 6 months ago

Selected Answer: B

Clearly the question is all about Amazon Route 53 that has Failover routing policy that is used when you want to configure active-passive failover.

upvoted 1 times

 **slackbot** 6 months, 2 weeks ago

i was looking at A, but indeed D is the best option, because the usually the TTL of the records is at least 60 seconds (nobody sets lower unless testing something ,because there is a charge per number of unique requests. ALB health check can be set as low as desired, which helps exclude the problematic ec2 faster than the DNS TTL expires

upvoted 2 times

 **cookieMr** 9 months ago

Selected Answer: D

By creating an ALB and configuring health checks, the architect ensures that only healthy instances receive traffic. The ALB periodically checks the health of the EC2 instances based on the configured health check settings.

Routing traffic to the ALB from Route 53 ensures that DNS queries return the IP address of the ALB instead of individual instances. This allows the ALB to distribute traffic only to healthy instances, avoiding timeouts caused by unhealthy instances.

A & B: While associating health checks with each record can help identify unhealthy instances, it does not provide automatic load balancing and distribution of traffic to healthy instances.

C: While CloudFront can improve performance and availability, it is primarily a CDN and may not directly address the issue of load balancing and distributing traffic to healthy instances.

Therefore, option D is the most appropriate solution to overcome the timeout errors by implementing an ALB with health checks and routing traffic through Route 53.

upvoted 3 times

 **joechen2023** 9 months, 1 week ago

Selected Answer: C

I believe both C and D will work, but C seems less complex.
hopefully somebody here is more advanced(not an old student learning AWS like me) to explain why not C.

upvoted 3 times

 **Abrar2022** 9 months, 4 weeks ago

Selected Answer: D

Option D allows for the creation of an Application Load Balancer which can detect unhealthy instances and redirect traffic away from them.

upvoted 2 times

 **Steve_4542636** 1 year ago

Selected Answer: D

I vote d

upvoted 1 times

 **techhb** 1 year, 2 months ago

Selected Answer: D

Its D only

upvoted 1 times

Question #265

Topic 1

A solutions architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.

Which solution meets these requirements and is MOST secure?

- A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- B. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
- C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Correct Answer: C

Community vote distribution

C (100%)

 **Aninina**  1 year, 2 months ago

C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.

This solution meets the requirements for a highly available application with web, application, and database tiers, as well as providing edge-based content delivery. Additionally, it maximizes security by having the ALB in a private subnet, which limits direct access to the web servers, while still being able to serve traffic over the Internet via the public ALB. This will ensure that the web servers are not exposed to the public Internet, which reduces the attack surface and provides a secure way to access the application.

upvoted 15 times

 **cookieMr**  9 months ago

Selected Answer: C

A. exposes the EC2 instances directly to the public internet, which may compromise security.
 B. lacks a load balancer in the public subnet, which is required for efficient load distribution and high availability.
 D. provides load balancing and HTTPS content delivery, it exposes the EC2 instances directly to the public internet, which may pose security risks.

C. provides high availability, secure access through private subnets, and optimized HTTPS content delivery using CloudFront with a public ALB as the origin.

upvoted 5 times

 **meowruki**  3 months, 3 weeks ago

C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.

Here's the reasoning:

Public ALB in Private Subnets: Placing the ALB in private subnets enhances security by preventing direct access from the internet. The ALB in private subnets can communicate with the application instances in the same private subnets.

CloudFront with ALB as Origin: Configuring CloudFront to deliver HTTPS content using the public ALB as the origin allows for content to be cached and distributed globally, reducing latency for end users.

upvoted 1 times

 **Ruffyit** 4 months, 1 week ago

C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.

This solution meets the requirements for a highly available application with web, application, and database tiers, as well as providing edge-based content delivery. Additionally, it maximizes security by having the ALB in a private subnet, which limits direct access to the web servers, while still being able to serve traffic over the Internet via the public ALB. This will ensure that the web servers are not exposed to the public Internet, which reduces the attack surface and provides a secure way to access the application.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: C

Keyword: Instances in private, ALB in public, point cloudfront to the public ALB
upvoted 1 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: C
Answer is C
upvoted 3 times

 **AHUI** 1 year, 2 months ago

ans: C
<https://www.examtopics.com/discussions/amazon/view/46401-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **Morinator** 1 year, 2 months ago

Selected Answer: C
Instances in private, ALB in public, point cloudfront to the public ALB
upvoted 4 times

Question #266

Topic 1

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.

Which solution meets these requirements?

- A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
- B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.

Correct Answer: A

Community vote distribution

A (100%)

 **Aninina**  1 year, 2 months ago

Selected Answer: A

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.

AWS Global Accelerator directs traffic to the optimal healthy endpoint based on health checks, it can also route traffic to the closest healthy endpoint based on geographic location of the client. By configuring an accelerator and attaching it to a Regional endpoint in each Region, and adding the ALB as the endpoint, the solution will redirect traffic to healthy endpoints, improving the user experience by reducing latency and ensuring that the application is running optimally. This solution will ensure that traffic is directed to the closest healthy endpoint and will help to improve the overall user experience.

upvoted 17 times

 **michellemeloc**  10 months, 1 week ago

Selected Answer: A

Delivery gaming content --> AWS GLOBAL ACCELERATOR

upvoted 9 times

 **pentium75**  2 months, 4 weeks ago

Selected Answer: A

Would have selected A just because B, C and D don't make any sense or have nothing to do with the requirements. But now learned that Global Accelerator checks health of resources BEHIND ALB/NLB, so it meets the requirements.

upvoted 3 times

 **mwwt2022** 2 months, 4 weeks ago

gaming platform -> Can't be CloudFront. Probably go for global accelerator

upvoted 3 times

 **Ruffyit** 4 months, 1 week ago

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.

AWS Global Accelerator directs traffic to the optimal healthy endpoint based on health checks, it can also route traffic to the closest healthy endpoint based on geographic location of the client. By configuring an accelerator and attaching it to a Regional endpoint in each Region, and adding the ALB as the endpoint, the solution will redirect traffic to healthy endpoints, improving the user experience by reducing latency and ensuring that the application is running optimally. This solution will ensure that traffic is directed to the closest healthy endpoint and will help to improve the overall user experience.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint

upvoted 1 times

 **bjexamprep** 8 months ago

Is any answer relevant to the question?

upvoted 3 times

 **cookieMr** 9 months ago

Selected Answer: A

B. While CloudFront can help with caching and content delivery, it does not provide the mechanism to monitor the health of the application or perform traffic redirection based on health checks.

C. This configuration is suitable for static content delivery but does not address the health monitoring and traffic redirection requirements of the application.

D. While this can enhance performance, it does not monitor the health of the application or redirect traffic based on health checks.

Therefore, option A is the most suitable solution as it leverages AWS Global Accelerator to monitor application health, route traffic to healthy endpoints, and optimize the user experience while addressing latency concerns.

upvoted 4 times

 **antropaws** 10 months ago

Selected Answer: A

Agree with A

upvoted 1 times

 **Bhrino** 1 year, 1 month ago

Selected Answer: A

Global accelerators can be used for non http cases such as UDP, tcp , gaming , or voip

upvoted 8 times

 **pentium75** 2 months, 4 weeks ago

Though we seem to have http/https here, otherwise they could not use ALBs

upvoted 1 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **AHUI** 1 year, 2 months ago

A:

<https://www.examtopics.com/discussions/amazon/view/46403-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **alanp** 1 year, 2 months ago

A. When you have an Application Load Balancer or Network Load Balancer that includes multiple target groups, Global Accelerator considers the load balancer endpoint to be healthy only if each target group behind the load balancer has at least one healthy target. If any single target group for the load balancer has only unhealthy targets, Global Accelerator considers the endpoint to be unhealthy.

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-health-check-options.html>

upvoted 8 times

 **Morinator** 1 year, 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-health-check-options.html>

upvoted 1 times

Question #267

Topic 1

A company has one million users that use its mobile app. The company must analyze the data usage in near-real time. The company also must encrypt the data in near-real time and must store the data in a centralized location in Apache Parquet format for further processing.

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

- A. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data. Invoke an AWS Lambda function to send the data to the Kinesis Data Analytics application.
- B. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data. Invoke an AWS Lambda function to send the data to the EMR cluster.
- C. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data.
- D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

Correct Answer: D

Community vote distribution

D (100%)

 **mhmt4438**  1 year, 2 months ago

Selected Answer: D

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

This solution will meet the requirements with the least operational overhead as it uses Amazon Kinesis Data Firehose, which is a fully managed service that can automatically handle the data collection, data transformation, encryption, and data storage in near-real time. Kinesis Data Firehose can automatically store the data in Amazon S3 in Apache Parquet format for further processing. Additionally, it allows you to create an Amazon Kinesis Data Analytics application to analyze the data in near real-time, with no need to manage any infrastructure or invoke any Lambda function. This way you can process a large amount of data with the least operational overhead.

upvoted 43 times

 **jainparag1** 1 year, 2 months ago

Nicely explained. Thanks.

upvoted 3 times

 **LuckyAro** 1 year, 2 months ago

Apache Parquet format processing was not mentioned in the answer options. Strange.

upvoted 7 times

 **WhericanIstart** 1 year ago

Thanks for the explanation!

upvoted 1 times

 **antropaws** 10 months ago

<https://aws.amazon.com/blogs/big-data/analyzing-apache-parquet-optimized-data-using-amazon-kinesis-data-firehose-amazon-athena-and-amazon-redshift/>

upvoted 1 times

 **cookieMr**  9 months ago

Selected Answer: D

A. requires invoking an Lambda to send the data to the analytics application. This introduces additional operational overhead and complexity.

B. While EMR is a powerful tool for big data processing, it requires more operational management and configuration compared to Kinesis Data Analytics.

C. introduces unnecessary complexity by involving EMR for data analysis when Kinesis Data Analytics can perform the analysis in a more streamlined and automated manner.

Therefore, option D is the most suitable solution as it leverages Kinesis Data Firehose for data ingestion, stores the data in S3, and utilizes Kinesis Data Analytics for near-real-time analysis, providing a low operational overhead solution for data usage analysis and encryption.

upvoted 6 times

 **farnamjam**  1 month, 3 weeks ago

Selected Answer: D

A and B are out.

Kinesis Data Streams cannot directly send data to S3 by itself

upvoted 1 times

 **Ruffyit** 4 months, 1 week ago

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

This solution will meet the requirements with the least operational overhead as it uses Amazon Kinesis Data Firehose, which is a fully managed service that can automatically handle the data collection, data transformation, encryption, and data storage in near-real time. Kinesis Data Firehose can automatically store the data in Amazon S3 in Apache Parquet format for further processing. Additionally, it allows you to create an Amazon Kinesis Data Analytics application to analyze the data in near real-time, with no need to manage any infrastructure or invoke any Lambda function. This way you can process a large amount of data with the least operational overhead.

upvoted 1 times

 **TariqKipkemei** 5 months, 4 weeks ago

Selected Answer: D

Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: D

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data

upvoted 1 times

 **AHUI** 1 year, 2 months ago

D:

<https://www.examtopics.com/discussions/amazon/view/82022-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Aninina** 1 year, 2 months ago

Selected Answer: D

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

Amazon Kinesis Data Firehose can automatically encrypt and store the data in Amazon S3 in Apache Parquet format for further processing, which reduces the operational overhead. It also allows for near-real-time data analysis using Kinesis Data Analytics, which is a fully managed service that makes it easy to analyze streaming data using SQL. This solution eliminates the need for setting up and maintaining an EMR cluster, which would require more operational overhead.

upvoted 2 times

Question #268

Topic 1

A gaming company has a web application that displays scores. The application runs on Amazon EC2 instances behind an Application Load Balancer. The application stores data in an Amazon RDS for MySQL database. Users are starting to experience long delays and interruptions that are caused by database read performance. The company wants to improve the user experience while minimizing changes to the application's architecture.

What should a solutions architect do to meet these requirements?

- A. Use Amazon ElastiCache in front of the database.
- B. Use RDS Proxy between the application and the database.
- C. Migrate the application from EC2 instances to AWS Lambda.
- D. Migrate the database from Amazon RDS for MySQL to Amazon DynamoDB.

Correct Answer: A

Community vote distribution

B (50%)

A (50%)

✉ **Steve_4542636** 1 year ago

Selected Answer: A

Rds proxy is for too many connections, not for performance
upvoted 28 times

✉ **Mkenya08** 1 month, 3 weeks ago

ElastiCache stores data in memory, which means it may not always have the most up-to-date information. This might be acceptable for certain use cases where slightly stale data is acceptable, but for applications like gaming scores, real-time accuracy is often crucial.
upvoted 2 times

✉ **Maru86** 1 month ago

"Data in the cache is never stale.
Because the data in the cache is updated every time it's written to the database, the data in the cache is always current and updated whenever data is written to the database." <https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/Strategies.html#Strategies.WriteThrough>
upvoted 3 times

✉ **Yadav_Sanjay** 10 months, 1 week ago

Can't use cache as score gates updated. If data would have been static then definitely can go with A. But here score is dynamic...
upvoted 8 times

✉ **r felipem** 9 months, 4 weeks ago

Users are starting to experience long delays and interruptions caused by the "read performance" of the database... While the score is dynamic, there is also read activity in the DB that is causing the delays and outages and this can be improved with Elastic Cache.
upvoted 4 times

✉ **vipyodha** 9 months ago

to use elasticache , you need to perform heavy code change ,and also elasticache do chaching that can improve read perfromance but will not provide scalability
upvoted 6 times

✉ **pentium75** 2 months, 2 weeks ago

We should "minimize", not "avoid", code changes.
upvoted 1 times

✉ **chickenmf** 1 week, 1 day ago

minimize *architectural changes, NOT code changes
upvoted 1 times

✉ **kraken21** 12 months ago

Selected Answer: B

RDX proxy will :"improve the user experience while minimizing changes".
upvoted 24 times

✉ **pentium75** 2 months, 2 weeks ago

.. but not address issues with "database read performance".
upvoted 1 times

alawada **Most Recent** 5 days, 8 hours ago

Selected Answer: A
ElastiCache stores data in memory RESOLVE THE READING ISSUE
upvoted 1 times

bujuman 3 weeks, 3 days ago

Selected Answer: A

A will be the best option regarding read performance and based on following link:
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/creating-elasticsearch-cluster-with-RDS-settings.html>
upvoted 2 times

TheFivePips 4 weeks ago

Selected Answer: B

A. Use Amazon ElastiCache in front of the database:
Caching frequently accessed data in ElastiCache can help reduce the load on the database and improve read performance.
However, it's essential to note that while ElastiCache can significantly enhance read performance by serving frequently accessed data from memory, it might not entirely eliminate long delays and interruptions if the root cause is related to the database itself or if the caching strategy is not effectively implemented.

B. Use RDS Proxy between the application and the database:

Helps improve database connection management, reducing the number of open connections to the database and enhancing overall performance.
RDS Proxy handles connection pooling, which means it can efficiently manage and reuse database connections, reducing the overhead of establishing new connections for each query.
It supports features like read/write splitting, which directs read queries to read replicas, further distributing the load.
upvoted 1 times

TheFivePips 4 weeks ago

In this scenario, game scores are updated frequently so caching seems less useful than a proxy

upvoted 1 times

MoshiurGCP 4 weeks, 1 day ago

The discussion is really helpful thanks everyone.
upvoted 1 times

sirasdf 4 weeks, 1 day ago

RDS Proxy between the application and the database would likely be the better solution to improve user experience while minimizing changes to the application's architecture.
upvoted 1 times

Maru86 1 month ago

Selected Answer: A

It's Implementing write-through caching strategy with ElastiCache "Data in the cache is never stale.
Because the data in the cache is updated every time it's written to the database, the data in the cache is always current and updated whenever data is written to the database." <https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/Strategies.html#Strategies.WriteThrough>
upvoted 2 times

SVDK 1 month ago

Selected Answer: B

Connection Pooling: RDS Proxy intelligently manages a pool of database connections, reusing them across multiple application requests. This dramatically reduces the overhead associated with constantly opening and closing database connections, especially during traffic surges.
Overload Protection: RDS Proxy can throttle or queue application requests if they would overwhelm the database. This protects your database from excessive load and helps maintain availability.
Efficient Scaling: RDS Proxy allows your applications to scale more gracefully without hitting database connection limits. It manages connection pooling and sharing, increasing the number of concurrent connections your database can support from individual applications.
Bursty Workloads: Great for applications experiencing unpredictable traffic patterns. RDS Proxy handles spikes in requests without disrupting database performance.
upvoted 1 times

vip2 1 month, 1 week ago

Selected Answer: A

A is correct.

ElastiCache for caching, which accelerates application and database performance

RDS proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability. It does not however specifically improve read performance like a caching layer would
upvoted 1 times

Rezaee 1 month, 3 weeks ago

Selected Answer: A

A. Use Amazon ElastiCache in front of the database.
upvoted 1 times

lucashpunkt 1 month, 3 weeks ago

Selected Answer: A

While RDS Proxy addresses problems regarding too many connections and time-outs, ElastiCache is the solution for read performance.
upvoted 1 times

✉ **Ditesh** 2 months ago

minimizing teh changes to application disqualifies elasticache thus RDS proxy is the only option left
upvoted 2 times

✉ **anikolov** 2 months, 2 weeks ago

Selected Answer: B

My vote is for "B". It is Not "A", because ElastiCache for Redis is designed to be protocol compliant with open source Redis, which will require "App Arch" changes
upvoted 2 times

✉ **awsgeek75** 2 months, 1 week ago

No one is talking about Redis here. ElastiCache is just caching in general (Redis OR MemCached).
"long delays and interruptions that are caused by database read performance" will be fixed by caching to reduce read load.
B is for connection pooling which is NOT a problem here.
upvoted 1 times

✉ **awsgeek75** 2 months, 3 weeks ago

Selected Answer: A

C,D are too much architecture work.
B uses RDS Proxy which is mainly for connection pooling and availability issues and rarely helps with read performance issues.
A is caching which is ideal for solving read issues
upvoted 4 times

✉ **saymolet** 3 weeks, 1 day ago

"The company wants to improve the user experience while minimizing changes to the application's architecture." A would require heavy code changes to the application
upvoted 1 times

✉ **farnamjam** 2 months, 3 weeks ago

Selected Answer: A

one ElastiCache usecase is for Gaming Leaderboards which are computationally complex
upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

Selected Answer: A

A will require code changes, but we should 'minimize changes to the architecture', not "the code". We're just introducing ONE additional component, as we would also with B.

B, RDS Proxy would help if there are too many connections (not the issue here), querying multiple databases in parallel (not the issue here as there is only one DB) and failover between instances (not the issue here).

C - Would completely overhaul the architecture

D - From relational database to NoSQL database is bigger "architectural change" than placing cache in front of DB.

upvoted 3 times

Question #269

Topic 1

An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.

What should the solutions architect recommend?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Correct Answer: C

Community vote distribution

C (100%)

✉  **awsgeek75** 2 months, 1 week ago

Selected Answer: C

". A solutions architect needs to solve the problem with minimal changes to the existing web application." ABD all require major changes to the application.
 A: DynamoDB is NoSQL so big change
 B: ElastiCache is a caching layer which require code change normally significant code change
 D: Redshift is analytics so not a solution

upvoted 1 times

✉  **Ruffyit** 4 months, 1 week ago

. While DynamoDB is a scalable NoSQL database, it requires changes to the application's data model and query patterns.
 B. ElastiCache is an in-memory data store that can improve query performance, but it is primarily used for caching rather than running complex queries.
 D. Redshift is a powerful data warehousing solution, but migrating the data and adapting the queries to Redshift's columnar architecture would require significant changes to the application and query logic.

Therefore, option C is the most appropriate recommendation as it leverages read replicas in RDS to offload read-only query traffic from the primary database, allowing the business analysts to run their queries without impacting the performance of the web application. It provides a scalable and efficient solution with minimal changes to the existing web application.

upvoted 1 times

✉  **nileeka97** 6 months ago

Selected Answer: C

C. Create a read replica of the primary database and have the business analysts run their queries

upvoted 1 times

✉  **cookieMr** 9 months ago

Selected Answer: C

A. While DynamoDB is a scalable NoSQL database, it requires changes to the application's data model and query patterns.
 B. ElastiCache is an in-memory data store that can improve query performance, but it is primarily used for caching rather than running complex queries.
 D. Redshift is a powerful data warehousing solution, but migrating the data and adapting the queries to Redshift's columnar architecture would require significant changes to the application and query logic.

Therefore, option C is the most appropriate recommendation as it leverages read replicas in RDS to offload read-only query traffic from the primary database, allowing the business analysts to run their queries without impacting the performance of the web application. It provides a scalable and efficient solution with minimal changes to the existing web application.

upvoted 1 times

✉  **antropaws** 10 months ago

Selected Answer: C

C, no doubt.

upvoted 2 times

✉  **mhmt4438** 1 year, 2 months ago

Selected Answer: C

C is correct answer
upvoted 2 times

 **Aninina** 1 year, 2 months ago

Selected Answer: C

C. Create a read replica of the primary database and have the business analysts run their queries.

Creating a read replica of the primary RDS database will offload the read-only SQL queries from the primary database, which will help to improve the performance of the web application. Read replicas are exact copies of the primary database that can be used to handle read-only traffic, which will reduce the load on the primary database and improve the performance of the web application. This solution can be implemented with minimal changes to the existing web application, as the business analysts can continue to run their queries on the read replica without modifying the code.

upvoted 4 times

 **bamishr** 1 year, 2 months ago

Selected Answer: C

Create a read replica of the primary database and have the business analysts run their queries.

upvoted 1 times

Question #270

Topic 1

A company is using a centralized AWS account to store log data in various Amazon S3 buckets. A solutions architect needs to ensure that the data is encrypted at rest before the data is uploaded to the S3 buckets. The data also must be encrypted in transit.

Which solution meets these requirements?

- A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- C. Create bucket policies that require the use of server-side encryption with S3 managed encryption keys (SSE-S3) for S3 uploads.
- D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.

Correct Answer: A

Community vote distribution



✉️ **techhb** Highly Voted 1 year, 2 months ago

Selected Answer: A

here keyword is "before" "the data is encrypted at rest before the data is uploaded to the S3 buckets."
upvoted 24 times

✉️ **reviewmine** Most Recent 1 month ago

Selected Answer: A

Answer is A. Encrypt it first before uploading to S3.
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

Selected Answer: C

I think the many votes for A are caused by misunderstanding the wording as
"Ensure that
the data is encrypted at rest before the data is uploaded"

But that doesn't make sense, it means

"Ensure that the data is encrypted at rest
before the data is uploaded"

So, before you allow people to upload data, make sure that it gets encrypted.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

On second thought, C would not enforce encryption in transit. Thus must be A indeed.
upvoted 2 times

✉️ **awsgeek75** 2 months, 1 week ago

For a moment I bought into your reasoning for C assuming that maybe the question is missing some grammar construct but realised that C does not really solve the encryption in transit issue like I originally thought. BUT good work!
upvoted 1 times

✉️ **Cyberkayu** 3 months, 1 week ago

BCD, data not yet encrypted before landing on S3 bucket
upvoted 2 times

✉️ **palthainon** 5 months ago

Selected Answer: C

HTTPs would encrypt in transe, SSE3 managed keys fulfills requirement for at rest. This is an aws exam, not a best practices exam.
upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

No. HTTPS is not enough for encryption in transit when it comes to S3.
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingClientSideEncryption.html>

"Client-side encryption is the act of encrypting your data locally to help ensure its security in transit and at rest."
upvoted 2 times

✉️ **peterfang224** 5 months, 1 week ago

Its_SaKar

upvoted 1 times

 **prabhjot** 5 months, 3 weeks ago

Ans is B - Server-Side Encryption (SSE): ensure data is encrypted at rest and also Encryption in Transit: When you upload data to Amazon S3 using standard HTTPS requests.

upvoted 3 times

 **TariqKipkemei** 5 months, 4 weeks ago

Selected Answer: A

Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

Selected Answer: A

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: A

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.

upvoted 1 times

 **Abobaloyi** 9 months, 1 week ago

Selected Answer: A

data must be encrypted before uploaded , which means the client need to do it before uploading the data to S3

upvoted 3 times

 **datz** 11 months, 3 weeks ago

Selected Answer: A

A, would meet requirements.

upvoted 1 times

 **nder** 1 year, 1 month ago

Selected Answer: A

Because the data must be encrypted while in transit

upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: A

A is correct IMO

upvoted 1 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/53840-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 4 times

 **Aninina** 1 year, 2 months ago

Selected Answer: A

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.

upvoted 2 times

 **bamishr** 1 year, 2 months ago

Selected Answer: A

Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets

upvoted 2 times

 **Kesha** 7 months, 3 weeks ago

B. With server-side encryption, it automatically encrypts the data at rest using encryption keys managed by AWS.

upvoted 1 times

Question #271

Topic 1

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the 'same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.

What should the solutions architect do to meet these requirements?

- A. Increase the minimum capacity for the Auto Scaling group.
- B. Increase the maximum capacity for the Auto Scaling group.
- C. Configure scheduled scaling to scale up to the desired compute level.
- D. Change the scaling policy to add more EC2 instances during each scaling operation.

Correct Answer: C

Community vote distribution

C (100%)

 **ManOnTheMoon** Highly Voted  1 year, 1 month ago

GOOD LUCK EVERYONE :) YOU CAN DO THIS

upvoted 27 times

 **david76x** Highly Voted  1 year, 2 months ago

Selected Answer: C

C is correct. Goodluck everybody!

upvoted 13 times

 **Guru4Cloud** Most Recent  6 months, 3 weeks ago

Selected Answer: C

Configuring scheduled scaling actions allows the Auto Scaling group to scale up to the desired capacity at a scheduled time (1 AM in this case) when the batch jobs start. This ensures the desired compute capacity is reached immediately.

The Auto Scaling group can then scale down based on metrics after the batch jobs complete.

upvoted 6 times

 **hsinchang** 8 months ago

Selected Answer: C

The time is given, use scheduled for optimal cost

upvoted 2 times

 **qacollin** 11 months, 1 week ago

just scheduled my exam :)

upvoted 6 times

 **awscerts023** 1 year, 1 month ago

Reached here ! Did anyone schedule the real exam now ? How was it ?

upvoted 5 times

 **pal40sg** 1 year, 1 month ago

Thanks to everyone who contributed with answers :)

upvoted 5 times

 **ProfXsamson** 1 year, 1 month ago

Selected Answer: C

C. I'm here at the end, leaving this here for posterity sake 02/01/2023.

upvoted 4 times

 **dedline** 1 year, 2 months ago

GL ALL!

upvoted 5 times

 **mhmt4438** 1 year, 2 months ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/27868-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Aninina** 1 year, 2 months ago

Selected Answer: C

C. Configure scheduled scaling to scale up to the desired compute level.

By configuring scheduled scaling, the solutions architect can set the Auto Scaling group to automatically scale up to the desired compute level at a specific time (1AM) when the batch job starts and then automatically scale down after the job is complete. This will allow the desired EC2 capacity to be reached quickly and also help in reducing the cost.

upvoted 4 times

 **bamishr** 1 year, 2 months ago

Selected Answer: C

Configure scheduled scaling to scale up to the desired compute level.

upvoted 1 times

 **Morinator** 1 year, 2 months ago

Selected Answer: C

predictable = schedule scaling

upvoted 4 times

Question #272

Topic 1

A company serves a dynamic website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The website needs to support multiple languages to serve customers around the world. The website's architecture is running in the us-west-1 Region and is exhibiting high request latency for users that are located in other parts of the world.

The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.

What should a solutions architect do to meet these requirements?

- A. Replace the existing architecture with a website that is served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.
- B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.
- C. Create an Amazon API Gateway API that is integrated with the ALB. Configure the API to use the HTTP integration type. Set up an API Gateway stage to enable the API cache based on the Accept-Language request header.
- D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the EC2 instances and the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Correct Answer: B

Community vote distribution

B (100%)

 **Yechi**  1 year, 1 month ago

Selected Answer: B

Configuring caching based on the language of the viewer

If you want CloudFront to cache different versions of your objects based on the language specified in the request, configure CloudFront to forward the Accept-Language header to your origin.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html>

upvoted 9 times

 **Trains**  4 months, 1 week ago

Isn't CloudFront for static websites though? Question specifically states the content is dynamic

upvoted 2 times

 **Cloud_A** 2 months ago

Cloudfront serves for both static and dynamic. If it was just static,then you can consider AWS S3.

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: B

By caching content based on the Accept-Language request header, CloudFront can serve the appropriate version of the website to users based on their language preferences. This solution allows the company to improve the website's performance for users around the world without having to recreate the existing architecture in multiple Regions.

upvoted 2 times

 **A1975** 7 months, 3 weeks ago

Selected Answer: B

CloudFront allows you to customize cache behavior based on various request headers. By setting the cache behavior to cache based on the Accept-Language request header, CloudFront can store and serve language-specific versions of the website content, reducing the need to repeatedly fetch the content from the ALB for users with the same language preference.

upvoted 1 times

 **kraken21** 12 months ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html#header-caching-web-language>

upvoted 1 times

 **vherman** 1 year ago

Selected Answer: B

B is correct

upvoted 1 times

✉️  **Steve_4542636** 1 year ago

Selected Answer: B

I think it's b
upvoted 2 times

✉️  **LuckyAro** 1 year, 1 month ago

Selected Answer: B

B is the correct answer
upvoted 1 times

Question #273

Topic 1

A rapidly growing ecommerce company is running its workloads in a single AWS Region. A solutions architect must create a disaster recovery (DR) strategy that includes a different AWS Region. The company wants its database to be up to date in the DR Region with the least possible latency. The remaining infrastructure in the DR Region needs to run at reduced capacity and must be able to scale up if necessary.

Which solution will meet these requirements with the LOWEST recovery time objective (RTO)?

- A. Use an Amazon Aurora global database with a pilot light deployment.
- B. Use an Amazon Aurora global database with a warm standby deployment.
- C. Use an Amazon RDS Multi-AZ DB instance with a pilot light deployment.
- D. Use an Amazon RDS Multi-AZ DB instance with a warm standby deployment.

Correct Answer: B*Community vote distribution*

B (98%)

 **Yechi**  1 year, 1 month ago

Selected Answer: B

Note: The difference between pilot light and warm standby can sometimes be difficult to understand. Both include an environment in your DR Region with copies of your primary Region assets. The distinction is that pilot light cannot process requests without additional action taken first, whereas warm standby can handle traffic (at reduced capacity levels) immediately. The pilot light approach requires you to "turn on" servers, possibly deploy additional (non-core) infrastructure, and scale up, whereas warm standby only requires you to scale up (everything is already deployed and running). Use your RTO and RPO needs to help you choose between these approaches.

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>
upvoted 21 times

 **nickolaj**  1 year, 1 month ago

Selected Answer: B

Option A is incorrect because while Amazon Aurora global database is a good solution for disaster recovery, pilot light deployment provides only a minimalistic setup and would require manual intervention to make the DR Region fully operational, which increases the recovery time.

Option B is a better choice than Option A as it provides a warm standby deployment, which is an automated and more scalable setup than pilot light deployment. In this setup, the database is replicated to the DR Region, and the standby instance can be brought up quickly in case of a disaster.

Option C is incorrect because Multi-AZ DB instances provide high availability, not disaster recovery.

Option D is a good choice for high availability, but it does not meet the requirement for DR in a different region with the least possible latency.
upvoted 18 times

 **awsgEEK75**  2 months, 1 week ago

Selected Answer: B

B: Warm Standby is better when it comes to LOWEST RTO.

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Selected Answer: B

"Different Region" rules out C and D ("Multi-AZ" is within a region)

"Run at reduced capacity" = warm standby (while "pilot light" means that DR resources are shut down and are started manually in case of failover)
upvoted 2 times

 **TariqKipkemei** 5 months, 4 weeks ago

Selected Answer: B

The warm standby approach involves ensuring that there is a scaled down, but fully functional, copy of your production environment in another Region.

With the pilot light approach, you replicate your data from one Region to another and provision a copy of your core workload infrastructure. Resources required to support data replication and backup, such as databases and object storage, are always on. Other elements, such as application servers, are loaded with application code and configurations, but are "switched off".
upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: B

An Amazon Aurora global database with a warm standby deployment provides continuous replication from one AWS Region to another, keeping the DR database up-to-date with minimal latency.

upvoted 1 times

 **A1975** 7 months, 3 weeks ago

Selected Answer: B

In a Pilot Light scenario, only an EC2 Instance and a DB may be running. In Warm Standby, however, everything is running — in a much smaller capacity. This means the load balancer, gateways, databases, all subnets, and everything else are ready to go on a moment's notice.

with reference to below statement Option B is a better choice than Option A.

"The remaining infrastructure in the DR Region needs to run at reduced capacity and must be able to scale up if necessary".

upvoted 1 times

 **krisfromtw** 1 year, 1 month ago

Selected Answer: D

should be D.

upvoted 1 times

 **leoattf** 1 year, 1 month ago

No, my friend. The question asks for deployment in another Region. Hence, it cannot be C or D.

The answer is B because is Global (different regions) and Ward Standby has faster RTO than Pilot Light.

upvoted 8 times

 **pentium75** 2 months, 3 weeks ago

"Multi-AZ" = multiple AZs in same region, but requirement is "a different AWS Region".

upvoted 1 times

Question #274

Topic 1

A company runs an application on Amazon EC2 instances. The company needs to implement a disaster recovery (DR) solution for the application. The DR solution needs to have a recovery time objective (RTO) of less than 4 hours. The DR solution also needs to use the fewest possible AWS resources during normal operations.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS Lambda and custom scripts.
- B. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation.
- C. Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times.
- D. Launch EC2 instances in a secondary Availability Zone. Keep the EC2 instances in the secondary Availability Zone active at all times.

Correct Answer: D

Community vote distribution

B (100%)

✉  **NolaHolla**  1 year, 1 month ago

Guys, sorry but I don't really have time to deepdive as my exam is soon. Based on chatGPT and my previous study the answer should be B "Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation," would likely be the most suitable solution for the given requirements.

This option allows for the creation of Amazon Machine Images (AMIs) to back up the EC2 instances, which can then be copied to a secondary AWS region to provide disaster recovery capabilities. The infrastructure deployment in the secondary region can be automated using AWS CloudFormation, which can help to reduce the amount of time and resources needed for deployment and management.

upvoted 8 times

✉  **NBone** 8 months, 1 week ago

please how do you use chatGPT to study for these questions?

upvoted 4 times

✉  **nickolaj**  1 year, 1 month ago

Selected Answer: B

Option B would be the most operationally efficient solution for implementing a DR solution for the application, meeting the requirement of an RTO of less than 4 hours and using the fewest possible AWS resources during normal operations.

By creating Amazon Machine Images (AMIs) to back up the EC2 instances and copying them to a secondary AWS Region, the company can ensure that they have a reliable backup in the event of a disaster. By using AWS CloudFormation to automate infrastructure deployment in the secondary Region, the company can minimize the amount of time and effort required to set up the DR solution.

upvoted 6 times

✉  **djgodzilla**  2 months, 2 weeks ago

OPtion E : Automate infrastructure deployment in the secondary Region by using terraform and ditch AWS CloudFormation 😊😊.

upvoted 3 times

✉  **pentium75** 2 months, 3 weeks ago

Selected Answer: B

A is not "most operationally efficient"

C and D do not meet the "use the fewest possible AWS resources during normal operations" requirement

upvoted 1 times

✉  **vijaykamal** 5 months, 4 weeks ago

Selected Answer: B

Option D suggests launching EC2 instances in a secondary Availability Zone (AZ), but AZs are not separate AWS Regions. While it provides high availability within a Region, it doesn't offer geographic redundancy, which is essential for disaster recovery.

upvoted 2 times

✉  **TariqKipkemei** 5 months, 4 weeks ago

Selected Answer: B

needs to use the fewest possible AWS resources during normal operations = backup & restore

upvoted 1 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: B

Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation

upvoted 1 times

 **AMYMY** 6 months, 3 weeks ago

B SHOULD BE RIGHT

upvoted 1 times

 **A1975** 7 months, 3 weeks ago

Selected Answer: B

Option A: Add complexity and management overhead.

Option B: Creating AMIs for backup and using AWS CloudFormation for infrastructure deployment in the secondary Region is a more streamlined and automated approach. CloudFormation allows you to define and provision resources in a declarative manner, making it easier to maintain and update your infrastructure. This solution is more operationally efficient compared to Option A.

Option C: could be expensive and not fully aligned with the requirement of using the fewest possible AWS resources during normal operations.

Option D: might not be sufficient for meeting the DR requirements, as Availability Zones are still within the same AWS Region and might be subject to the same regional-level failures.

upvoted 1 times

 **NBone** 8 months, 1 week ago

Please I would really appreciate clarification with this question. The community has voted 100% that the right answer is B. However, option D is shown to be the correct answer. So, who sets the correct answer? Which one should new comers like myself believe? the community's or the other (which am guessing is set by the moderators???) Please help.

upvoted 2 times

 **SimiTik** 11 months, 1 week ago

C may satisfy the requirement of using the fewest possible AWS resources during normal operations, it may not be the most operationally efficient or cost-effective solution in the long term.

upvoted 2 times

 **AlmeroSenior** 1 year, 1 month ago

So Weird , they have product for this > Elastic Disaster Recovery , but option is not given .

upvoted 1 times

 **Yechi** 1 year, 1 month ago

Selected Answer: B

https://docs.aws.amazon.com/zh_cn/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore

upvoted 4 times

 **Joan111edu** 1 year, 1 month ago

Selected Answer: B

the answer should be B

--->recovery time objective (RTO) of less than 4 hours.

https://docs.aws.amazon.com/zh_cn/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore

upvoted 3 times

Question #275

Topic 1

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Correct Answer: A

Community vote distribution



✉️ **asoli** 1 year ago

Selected Answer: C

At first, I thought the answer is A. But it is C.

It seems that there is no information in the question about CPU or Memory usage.

So, we might think the answer is A. why? because what we need is to have the required (desired) number of instances. It already has scheduled scaling that works well in this scenario. Scale down after working hours and scale up in working hours. So, it just needs to adjust the desired number to start from 20 instances.

But here is the point it shows A is WRONG!!!

If it started with desired 20 instances, it will keep it for the whole day. What if the load is reduced? We do not need to keep the 20 instances always. That 20 is the MAXIMUM number we need, no the DESIRE number. So it is against COST that is the main objective of this question.

So, the answer is C

upvoted 23 times

✉️ **c10356a** 3 months ago

There is no cooldown period in target tracking, but warm-up time.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

There is a cooldown period in the auto-scaling group, which helps 'keeping costs to a minimum' as instances would be removed sooner.

upvoted 3 times

✉️ **mandragon** 10 months, 3 weeks ago

If it starts with 20 instances it will not keep it all day. It will scale down based on demand. The scheduled action in Option A simply ensures that there are enough instances running to handle the increased traffic when the day begins, while still allowing the Auto Scaling group to scale up or down based on demand during the rest of the day. <https://docs.aws.amazon.com/autoscaling/ec2/userguide/scale-your-group.html>

upvoted 10 times

✉️ **xdkonorek2** 4 months ago

This is right, setting desired capacity doesn't turn off autoscaling policies

upvoted 2 times

✉️ **TheFivePips** 4 weeks ago

From what I can tell, you must specify an end time, or else it will run indefinitely. So I think A would be right, if they specified an end time. Otherwise C is more cost effective

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>

upvoted 1 times

✉️ **foha2012** 2 months ago

Answer is A. Makes more sense to me.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

Selected Answer: C

A is not cost effective, it would set the number of instances to maximum even before the first employee arrives.
 D is not cost effective, it would cause the permanent use of 20 instances

B could almost work, but if you configure small steps then it scales too slowly in the morning; if you configure big steps (like "add 8 instances at a time") it would scale in the morning but not be cost-efficient during the day.

C would address the requirement, it would scale to meet a certain CPU utilization. Decreasing the cooldown period (which is not possible for the scaling policy itself but for the auto-scaling group) would help 'keeping costs to a minimum'.

upvoted 1 times

Mikado211 3 months, 1 week ago

Selected Answer: A

The question 369 is exactly the same problem,
 Since a scheduled scaling doesn't disable the autoscaling later in the day the A works perfectly well.

upvoted 2 times

Cyberkayu 3 months, 1 week ago

A. since only a boot storm issue at 9am and settle down in mid morning, 20 instance is enough to support the workload
 NOT C. Reduce threshold to trigger (lets say 50% from 80% utilization) and lower cool down period, will still take time to ramp up to max 20 instance.

upvoted 1 times

pentium75 2 months, 3 weeks ago

How would scaling up to the maximum number of instances "keep costs to a minimum"?

upvoted 1 times

MoshiurGCP 3 months, 2 weeks ago

Selected Answer: A

I would go with A. Autoscaling is still there and the problem is clearly in morning.
 upvoted 3 times

pentium75 2 months, 3 weeks ago

WOuld not keep costs to a minimum
 upvoted 2 times

meowruki 3 months, 3 weeks ago

Selected Answer: C

C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.

Here's the reasoning:

Target Tracking Scaling Policy: With a target tracking scaling policy, you can set a target value for a specific metric, such as CPU utilization. The Auto Scaling group then adjusts the capacity to maintain that target.

Lower CPU Threshold: By triggering the target tracking action at a lower CPU threshold, the Auto Scaling group can proactively add instances when the workload increases, helping to address the slowness at the beginning of the day.

Decrease Cooldown Period: Reducing the cooldown period allows the Auto Scaling group to scale in and out more rapidly, making adjustments quicker in response to changing demand.

upvoted 4 times

meowruki 3 months, 3 weeks ago

Options A and D involve scheduled actions, which are time-based and may not be as responsive to immediate changes in demand. They also do not dynamically respond to varying workloads.

upvoted 2 times

wearrexdzw3123 4 months, 1 week ago

My mistake, I should have chosen c. A lower threshold can expand in advance, and lowering cooling can increase the expansion frequency.
 upvoted 2 times

wearrexdzw3123 4 months, 2 weeks ago

Selected Answer: A

I choose option A because the root of the problem is the inability of the scaling speed in the morning to meet the demand, rather than what criteria to use for scaling.

upvoted 1 times

pentium75 2 months, 3 weeks ago

How would scaling up to the maximum number of instances "keep costs to a minimum"?

upvoted 1 times

TariqKipkemei 5 months, 4 weeks ago

To keep costs to a minimum target tracking is the best option.

For example the scaling metric is the average CPU utilization of the EC2 auto scaling instances, and their average during the day should always be 80%. When CloudWatch detects that the average CPU utilization is beyond 80% at start of day, it will trigger the target tracking policy to scale out the auto scaling group to meet this target utilization. Once everything is settled and the average CPU utilization has gone below 80% at night, another scale in action will kick in and reduce the number of auto scaling instances in the auto scaling group.

upvoted 3 times

 **TariqKipkemei** 5 months, 4 weeks ago

Option C is best

upvoted 1 times

 **Ramdi1** 6 months ago

Selected Answer: A

I am going A based on it stating upto 20 so you already know what they maximum they use which is n a sense consistent. however i can see why people have put C. I think they need more clarification on the questions.

upvoted 3 times

 **pentium75** 2 months, 3 weeks ago

How would scaling up to the maximum number of instances "keep costs to a minimum"?

upvoted 1 times

 **Uzbekistan** 6 months, 1 week ago

Selected Answer: A

A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

How would scaling up to the maximum number of instances "keep costs to a minimum"?

upvoted 1 times

 **Uzbekistan** 6 months, 1 week ago

CHATGPT says Answers is A

A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.

upvoted 1 times

 **BrijMohan08** 6 months, 3 weeks ago

Selected Answer: A

Scaling Out: In the morning when you schedule the AWS EC2 scaling to have a minimum and maximum of 20 instances, if the load on your application increases beyond the current number of instances, AWS Auto Scaling will automatically launch new instances to meet the demand up to the maximum of 20 instances.

Scaling In: As the load on your application decreases in the afternoon or night, AWS Auto Scaling will continuously monitor the health and load of your instances. If the instances are underutilized and can be terminated without affecting your application's performance, AWS Auto Scaling will automatically scale in by terminating excess instances,

Why not D? If you specify the min instance, AWS will always keep the minimum number of instances (20 in this case) running.

upvoted 2 times

 **LazyTs** 6 months, 3 weeks ago

It's A, C will not be fast enough with the sudden influx of the users, if C is fast enough then the original scenario should already be good enough as the 20 is already the max which set to start at working hours(when CPU starts to spin up)

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

How would A "keep costs to a minimum"?

upvoted 1 times

 **kapalulz** 7 months, 2 weeks ago

Selected Answer: C

C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period

upvoted 1 times

 **Mia2009687** 8 months, 3 weeks ago

Selected Answer: C

I was in team A. But from the definition of desired capacity, it seems once we set it as 20, it will try to keep it as 20 which is not saving cost.

Desired capacity: Represents the initial capacity of the Auto Scaling group at the time of creation. An Auto Scaling group attempts to maintain the desired capacity. It starts by launching the number of instances that are specified for the desired capacity, and maintains this number of instances as long as there are no scaling policies or scheduled actions attached to the Auto Scaling group.

upvoted 2 times

Question #276

Topic 1

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.

What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose two.)

- A. Configure storage Auto Scaling on the RDS for Oracle instance.
- B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
- C. Configure an alarm on the RDS for Oracle instance for low free storage space.
- D. Configure the Auto Scaling group to use the average CPU as the scaling metric.
- E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

Correct Answer: AC

Community vote distribution



✉️ **klayytech** 11 months, 4 weeks ago

Selected Answer: AD

- A) Configure storage Auto Scaling on the RDS for Oracle instance.
 = Makes sense. With RDS Storage Auto Scaling, you simply set your desired maximum storage limit, and Auto Scaling takes care of the rest.
- B) Migrate the database to Amazon Aurora to use Auto Scaling storage.
 = Scenario specifies application's data layer uses Oracle-specific PL/SQL functions. This rules out migration to Aurora.
- C) Configure an alarm on the RDS for Oracle instance for low free storage space.
 = You could do this but what does it fix? Nothing. The CW notification isn't going to trigger anything.
- D) Configure the Auto Scaling group to use the average CPU as the scaling metric.
 = Makes sense. The CPU utilization is the precursor to the storage outage. When the ec2 instances are overloaded, the RDS instance storage hits its limits, too.
- upvoted 20 times

✉️ **MoshiurGCP** 4 weeks, 1 day ago

Nicely Explained.

upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

Selected Answer: AD

- B is not possible because the application "uses Oracle-specific PL/SQL functions"
 C does not meet the "automatically scale" requirement
 E would require an agent on the hosts which we might not have, plus CPU is a better indicator than memory
- upvoted 1 times

✉️ **meowruki** 3 months, 3 weeks ago

Selected Answer: AD

- A. Configure storage Auto Scaling on the RDS for Oracle instance.

This option allows the RDS instance to automatically scale its storage based on the actual storage usage, ensuring that you don't run out of storage.

- D. Configure the Auto Scaling group to use the average CPU as the scaling metric.

By using CPU utilization as a scaling metric, the Auto Scaling group can dynamically adjust the number of EC2 instances based on the application's demand. This helps in handling increased traffic and preventing overload on existing instances.

upvoted 1 times

✉️ **meowruki** 3 months, 3 weeks ago

Option B (Migrate the database to Amazon Aurora): While Amazon Aurora provides benefits such as auto-scaling storage and high performance, it involves migrating from Oracle to Aurora, which might require application changes and data migration efforts.

Option C (Configure an alarm on the RDS for Oracle instance for low free storage space): While it's good to have an alarm for low storage space, configuring storage Auto Scaling (Option A) is a more proactive solution that automatically adjusts storage before reaching a critical point.

Option E (Configure the Auto Scaling group to use the average free memory as the scaling metric): While monitoring memory is important for application performance, CPU utilization is often a more direct and responsive metric for auto-scaling in many scenarios.

upvoted 2 times

 **TariqKipkemei** 5 months, 3 weeks ago

Selected Answer: AD

Configure storage Auto Scaling on the RDS for Oracle instance and Configure the Auto Scaling group to use the average CPU as the scaling metric to accommodate the increased traffic automatically.

upvoted 1 times

 **vijaykamal** 5 months, 4 weeks ago

Selected Answer: AD

Option B (Migrate the database to Amazon Aurora) may be a good long-term solution, but it involves database migration, which can be complex and time-consuming. For immediate scalability and to address the storage issue, configuring storage Auto Scaling on the existing RDS instance is a more immediate and straightforward solution.

Option C (Configure an alarm on the RDS for Oracle instance for low free storage space) is useful for monitoring, but it doesn't proactively address the storage issue by automatically expanding storage as needed.

Option E (Configure the Auto Scaling group to use the average free memory as the scaling metric) is less common as a scaling metric for EC2 instances compared to CPU utilization. While memory can be an important factor for application performance, CPU utilization is typically a more commonly used metric for scaling decisions. It also doesn't directly address the RDS storage issue.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: AD

A. By enabling storage Auto Scaling on the RDS for Oracle instance, it will automatically add more storage when the existing storage is running out, ensuring the application's data layer can handle the increased data storage requirements.

D. By configuring the Auto Scaling group to use the average CPU utilization as the scaling metric, it can automatically add more EC2 instances to the Auto Scaling group when the CPU utilization exceeds a certain threshold. This will help handle the increased traffic and workload on the EC2 instances in the multi-tier application.

upvoted 1 times

 **A1975** 7 months, 3 weeks ago

Selected Answer: AD

A. By enabling storage Auto Scaling on the RDS for Oracle instance, it will automatically add more storage when the existing storage is running out, ensuring the application's data layer can handle the increased data storage requirements.

D. By configuring the Auto Scaling group to use the average CPU utilization as the scaling metric, it can automatically add more EC2 instances to the Auto Scaling group when the CPU utilization exceeds a certain threshold. This will help handle the increased traffic and workload on the EC2 instances in the multi-tier application.

upvoted 1 times

 **kruasan** 11 months ago

Selected Answer: AD

These options will allow the system to scale both the compute tier (EC2 instances) and the data tier (RDS storage) automatically as traffic increases:

A. Storage Auto Scaling will allow the RDS for Oracle instance to automatically increase its allocated storage when free storage space gets low. This ensures the database does not run out of capacity and can continue serving data to the application.

D. Configuring the EC2 Auto Scaling group to scale based on average CPU utilization will allow it to launch additional instances automatically as traffic causes higher CPU levels across the instances. This scales the compute tier to handle increased demand.

upvoted 2 times

 **kraken21** 12 months ago

Selected Answer: AD

Auto scaling storage RDS will ease storage issues and migrating Oracle PI/Sql to Aurora is cumbersome. Also Aurora has auto storage scaling by default.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PIOPS.Autoscaling

upvoted 2 times

 **Nel8** 1 year ago

Selected Answer: BD

My answer is B & D...

B. Migrate the database to Amazon Aurora to use Auto Scaling Storage. --- Aurora storage is also self-healing. Data blocks and disks are continuously scanned for errors and repaired automatically.

D. Configure the Auto Scaling group to use the average CPU as the scaling metric. -- Good choice.

I believe either A & C or B & D options will work.

upvoted 3 times

 **FourOfAKind** 1 year ago

In this question, you have Oracle DB, and Amazon Aurora is for MySQL/PostgreSQL. A and D are the correct choices.

upvoted 5 times

 **[Removed]** 1 year ago

You can migrate Oracle PL/SQL to Aurora:

<https://docs.aws.amazon.com/dms/latest/oracle-to-aurora-mysql-migration-playbook/chap-oracle-aurora-mysql.sql.html>

upvoted 1 times

 **[Removed]** 1 year ago

I still think A is the answer, because RDS for Oracle auto scaling once enabled it will automatically adjust the storage capacity.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

But the application "uses Oracle-specific PL/SQL functions".

upvoted 1 times

 **Ja13** 1 year, 1 month ago

Selected Answer: AD

a and d

upvoted 3 times

 **KZM** 1 year, 1 month ago

A and D.

upvoted 3 times

 **GwonLEE** 1 year, 1 month ago

Selected Answer: AD

a and d

upvoted 3 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: AD

A and D

upvoted 2 times

 **Joan111edu** 1 year, 1 month ago

Selected Answer: AD

<https://www.examtopics.com/discussions/amazon/view/46534-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **ChrisG1454** 1 year, 1 month ago

answer is A and D

upvoted 1 times

 **ChrisG1454** 1 year, 1 month ago

<https://www.examtopics.com/discussions/amazon/view/46534-exam-aws-certified-solutions-architect-associate-saa-c02/#:~:text=%22This%20overloads%20the%20EC2%20instances%20and%20causes%20the,RDS%20for%20Oracle%20instance%20upvo>

ted%202%20times

upvoted 1 times

 **rrharris** 1 year, 1 month ago

A and D are the Answers

upvoted 1 times

Question #277

Topic 1

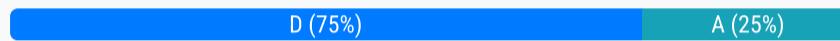
A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

- A. Use AWS Storage Gateway for files to store and process the video content.
- B. Use AWS Storage Gateway for volumes to store and process the video content.
- C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
- D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing.

Correct Answer: A

Community vote distribution



✉️ **bdp123** 1 year, 1 month ago

Selected Answer: D

Storage gateway is not used for storing content - only to transfer to the Cloud
upvoted 24 times

✉️ **pentium75** 2 months, 3 weeks ago

A doesn't say "store content ON the gateway", it says "use AWS Storage Gateway for files" (which is the product) "to store the video content" [on S3].
upvoted 2 times

✉️ **jaswantn** 1 month, 2 weeks ago

Creating storage gateway for Files will mount S3 bucket as an NFS volume that can be shared among EC2 Instances in the same manner as EFS but more cost effectively.
upvoted 1 times

✉️ **kraken21** 12 months ago

Selected Answer: D

There is no on-prem/non Aws infrastructure to create a gateway. Also, EFS+EBS is more expensive than EFS and S3. So D is the best option.
upvoted 9 times

✉️ **pentium75** 2 months, 3 weeks ago

But how do you attach "an EBS volume" to all the servers, and how will you use the files on it then to serve customers.
upvoted 1 times

✉️ **bujuman** 2 weeks, 6 days ago

Selected Answer: A

Answer is closer to the following principle and D is near impossible to implement:

"Amazon S3 File Gateway – Amazon S3 File Gateway supports a file interface into Amazon Simple Storage Service (Amazon S3) and combines a service and a virtual software appliance. By using this combination, you can store and retrieve objects in Amazon S3 using industry-standard file protocols such as Network File System (NFS) and Server Message Block (SMB). You deploy the gateway into your on-premises environment as a virtual machine (VM) running on VMware ESXi, Microsoft Hyper-V, or Linux Kernel-based Virtual Machine (KVM), or as a hardware appliance that you order from your preferred reseller. You can also deploy the Storage Gateway VM in VMware Cloud on AWS, or as an AMI in Amazon EC2. The gateway provides access to objects in S3 as files or file share mount points. With a S3 File Gateway, you can do the following"

upvoted 1 times

✉️ **vip2** 1 month, 1 week ago

Selected Answer: A

A is correct
For D, how to move file from S3 to EBS temporarily????
upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

Selected Answer: A

I was initially going for D but EBS part makes no sense as it is not possible. Closest explanation of A is in this article:
<https://aws.amazon.com/blogs/storage/mounting-amazon-s3-to-an-amazon-ec2-instance-using-a-private-connection-to-s3-file-gateway/>

A is missing a lot of key steps but D is just impossible. Maybe it's just the wording?

upvoted 1 times

 **AzExam2020** 2 months, 2 weeks ago

EFS is already used, why EBS is an option in the answer?

upvoted 1 times

 **anikolov** 2 months, 2 weeks ago

Selected Answer: A

AWS Storage Gateway S3 file gateway can be setup on EC2 (<https://repost.aws/knowledge-center/file-gateway-ec2>). It use local disks/EBS for caching data.

D: Can be used too, using attached EBS volume to each EC2 instance to process files. If require single EBS volume to be attached to multiple EC2, then it is possible too if they are in the same Availability Zone -> <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html>. For me A and D both are possible, but expect AWS would like to select Storage GW

upvoted 2 times

 **SVDK** 2 months, 1 week ago

I agree. This documentation has convinced me. <https://docs.aws.amazon.com/filegateway/latest/files3/what-is-file-s3.html>

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Selected Answer: A

A would work, "Storage Gateway for files" can provide access to S3 (cheap) via NFS (what the clients are using now). It has some additional cost in addition to the S3 charges, but would still be way cheaper than EFS.

B would work for a single server, but as it provides a volume via iSCSI, it could be mounted only to a single server - does not meet the 'multiple instances can access' requirement.

C and D do not meet the 'multiple instances can access' requirement because EBS can't be easily attached to all servers at the same time.

upvoted 2 times

 **pentium75** 2 months, 2 weeks ago

And even if ignoring the 'multiple instances can access' requirement, D would be against WAF; for temporary storage you'd use instance storage, not EBS.

upvoted 1 times

 **liux99** 4 months, 2 weeks ago

Storage gateway is intended for on-premises applications to access cloud storage, so A, B is out. The question explicitly states that the files are uploaded and stored in EFS, not S3, so D is not correct. The answer is C. The EFS storage costs 10 times more than EBS, so moving files to EBS after processing is the solution.

upvoted 1 times

 **beginnercloud** 4 months, 4 weeks ago

Selected Answer: D

Answer D is correct.

Storage gateway is not used for storing content - only to transfer to the Cloud

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

But how do you attach "an EBS volume" to all the servers, and how will you use the files on it then to serve customers?

A doesn't say "store content ON the gateway", it says "use AWS Storage Gateway for files" (which is the product) "to store the video content" [on S3]. And to be exact, Storage Gateway is not "to transfer to the cloud" but to provide access to S3 storage via SMB or NFS.

upvoted 1 times

 **TariqKipkemei** 5 months, 3 weeks ago

Selected Answer: D

Cost effective = Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: D

Amazon S3 provides low-cost object storage for storing large amounts of unstructured data like videos. The videos can be stored in S3 durably and reliably.

For processing, the video files can be temporarily copied from S3 to an EBS volume attached to the EC2 instance. EBS provides low latency block storage for high performance video processing.

Once processing is complete, the output can be stored back in S3.

upvoted 3 times

 **bjexamprep** 7 months, 2 weeks ago

Selected Answer: D

The question doesn't give enough information. Well, quite a few AWS exam questions don't provide enough info. Ideally, A could be the best answer if it mentions S3 as the backend of storage gateway. Because if it doesn't mention S3 as the backend, that implies either Storage gateway as the storage(which is impossible) or continue using EFS(also impossible). D is not ideal, because it will introduce video download cost for downloading files from S3 to EBS temporary storage. But it is the best option we have.

upvoted 1 times

 **pentium75** 2 months, 2 weeks ago

A mentions "AWS Storage Gateway for files" which implies S3 as the backend storage. D does not meet the 'multiple instances can access for processing' requirement.

upvoted 1 times

 **foha2012** 2 months ago

We are ditching EFS in favor of S3. So there is no longer simultaneous access happening. Whoever needs the file, downloads it from S3, process it on their EC2 instance and save it back to S3.

upvoted 1 times

 **Undisputed** 7 months, 3 weeks ago

Selected Answer: D

A more cost-effective storage solution for this scenario would be Amazon Simple Storage Service (Amazon S3). Amazon S3 is an object storage service that offers high scalability, durability, and availability at a lower cost compared to Amazon EFS. By using Amazon S3, you only pay for the storage you use, and it is typically more cost-efficient for scenarios where data is accessed less frequently, such as video storage for processing.

upvoted 2 times

 **smartegnine** 9 months, 1 week ago

Selected Answer: A

The result should be A.

Amazon storage gateway has 4 types, S3 File Gateway, FSx file gateway, Type Gateway and Volume Gateway.

If not specific reference file gateway should be default as S3 gateway, which sent file over to S3 the most cost effective storage in AWS.

Why not D, the reason is last sentence, there are multiple EC2 servers for processing the video and EBS can only attach to 1 EC2 instance at a time, so if you use EBS, which mean for each EC2 instance you will have 1 EBS. This rule out D.

upvoted 1 times

 **argl1995** 8 months, 4 weeks ago

We can use multi-attach feature of EBS to attach one EBS volume to multiple Ec2 instances

upvoted 2 times

 **[Removed]** 9 months ago

AWS Storage Gateway = extend storage to onprem

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Storage Gateway is a GATEWAY, it does not store anything. You could use the gateway as a cache for content actually in S3. Btw, A and B even say that Storage Gateway would "process the video content" ...

upvoted 1 times

 **MostafaWardany** 9 months, 3 weeks ago

Selected Answer: D

D: MOST cost-effective of these options = S3

upvoted 1 times

 **omoakin** 10 months ago

CCCCCCCCCC

upvoted 1 times

Question #278

Topic 1

A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must protect any sensitive data. The company also needs to receive monthly email messages if any financial information is present in the employee data.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Use Amazon Redshift to store the employee data in hierarchies. Unload the data to Amazon S3 every month.
- B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.
- C. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.
- D. Use Amazon Athena to analyze the employee data in Amazon S3. Integrate Athena with Amazon QuickSight to publish analysis dashboards and share the dashboards with users.
- E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

Correct Answer: CD

Community vote distribution

BE (100%)

 **Bhawesh**  1 year, 1 month ago

Selected Answer: BE

Data in hierarchies : Amazon DynamoDB

B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.

Sensitive Info: Amazon Macie

E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

upvoted 11 times

 **gold4otas** 12 months ago

Can someone please provide explanation why options "B" & "C" are the correct options?

upvoted 1 times

 **smartegnive** 9 months, 1 week ago

C is half statement once event sent to Lambda what is next? Should send email right, but it does not say it.

upvoted 1 times

 **hro**  1 week, 3 days ago

B - because to store employee data in a hierarchical structured relationship. AmazonDB "...Schema flexibility lets DynamoDB store complex hierarchical data within a single item."

E - because C omits the monthly email notifications resolved by using Amazon SNS.

Just my take.

upvoted 1 times

 **MoshirGCP** 4 weeks, 1 day ago

Why not C and D? Can anyone explain please.

upvoted 1 times

 **Cyberkayu** 3 months, 1 week ago

A. Unload the data to Amazon S3 every month.

doesnt make sense to empty the employee data from redshift monthly

upvoted 1 times

 **beginnercloud** 4 months, 4 weeks ago

Selected Answer: BE

B and E are the steps to meet all of the requirements.

upvoted 1 times

 **TariqKipkemei** 5 months, 3 weeks ago

Selected Answer: BE

Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: BE

B and E are the steps to meet all of the requirements.

B meets the need to store hierarchical employee data in DynamoDB for low latency queries at high traffic. DynamoDB can handle the access patterns for hierarchical data. Exporting to S3 monthly provides an audit trail.

E sets up Macie to analyze sensitive data and integrate with EventBridge to trigger monthly SNS notifications when financial data is present.
upvoted 2 times

✉ **A1975** 7 months, 3 weeks ago

Selected Answer: BE

]B. Amazon DynamoDB is a fully managed NoSQL database service that provides low-latency, high-performance storage for hierarchical data. It handles high-traffic queries and delivering fast responses to retrieve employee data efficiently.

E. Amazon Macie is a service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Integrating Macie with Amazon EventBridge allows you to receive events whenever any financial information is identified in the employee data. By using Amazon SNS, you can receive these notifications via email.

upvoted 2 times

✉ **cesargalindo123** 9 months, 1 week ago

AE

<https://aws.amazon.com/es/blogs/big-data/query-hierarchical-data-models-within-amazon-redshift/>

upvoted 2 times

✉ **kruasan** 11 months ago

Selected Answer: BE

, the combination of DynamoDB for fast data queries, S3 for durable storage and backups, Macie for sensitive data monitoring, and EventBridge + SNS for email notifications satisfies all needs: fast query response, sensitive data protection, and monthly alerts. The solutions architect should implement DynamoDB with export to S3, and configure Macie with integration to send SNS email notifications.

upvoted 1 times

✉ **kruasan** 11 months ago

Generally, for building a hierarchical relationship model, a graph database such as Amazon Neptune is a better choice. In some cases, however, DynamoDB is a better choice for hierarchical data modeling because of its flexibility, security, performance, and scale.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/dynamodb-hierarchical-data-model/introduction.html>

upvoted 3 times

✉ **darn** 11 months ago

why Dynamo and not Redshift?

upvoted 2 times

✉ **kruasan** 11 months ago

1. Low latency - DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with single-digit millisecond latency. Redshift is a data warehouse solution optimized for complex analytical queries, so query latency would typically be higher. Since the requirements specify minimum latency for high-traffic queries, DynamoDB is better suited.

2. Scalability - DynamoDB is highly scalable, able to handle very high read and write throughput with no downtime. Redshift also scales, but may experience some downtime during rescale operations. For a high-traffic application, DynamoDB's scalability and availability are better matched.

upvoted 3 times

✉ **kruasan** 11 months ago

3. Hierarchical data - DynamoDB supports hierarchical (nested) data structures well in a NoSQL data model. Defining hierarchical employee data may be more complex in Redshift's columnar SQL data warehouse structure. DynamoDB is built around flexible data schemas that can represent complex relationships.

4. Data export - Both DynamoDB and Redshift allow exporting data to S3, so that requirement could be met with either service. However, overall DynamoDB is the better fit based on the points above regarding latency, scalability, and support for hierarchical data.

upvoted 5 times

✉ **PRASAD180** 1 year, 1 month ago

BE is crt 100%

upvoted 1 times

✉ **KZM** 1 year, 1 month ago

B and E

To send monthly email messages, an SNS service is required.

upvoted 2 times

✉ **skiwili** 1 year, 1 month ago

Selected Answer: BE

B and E

upvoted 3 times

Question #279

Topic 1

A company has an application that is backed by an Amazon DynamoDB table. The company's compliance requirements specify that database backups must be taken every month, must be available for 6 months, and must be retained for 7 years.

Which solution will meet these requirements?

- A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.
- B. Create a DynamoDB on-demand backup of the DynamoDB table on the first day of each month. Transition the backup to Amazon S3 Glacier Flexible Retrieval after 6 months. Create an S3 Lifecycle policy to delete backups that are older than 7 years.
- C. Use the AWS SDK to develop a script that creates an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the script on the first day of each month. Create a second script that will run on the second day of each month to transition DynamoDB backups that are older than 6 months to cold storage and to delete backups that are older than 7 years.
- D. Use the AWS CLI to create an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the command on the first day of each month with a cron expression. Specify in the command to transition the backups to cold storage after 6 months and to delete the backups after 7 years.

Correct Answer: B

Community vote distribution



vijaykamal 5 months, 4 weeks ago

Selected Answer: A

Option B mentions using Amazon S3 Glacier Flexible Retrieval, but DynamoDB doesn't natively support transitioning backups to Amazon S3 Glacier. Options C and D involve custom scripts and EventBridge rules, which add complexity and may not be as reliable or efficient as using AWS Backup for this purpose.

upvoted 6 times

Sadiya_Javid_Abbasi 2 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/aws-backup/latest/devguide/creating-a-backup-plan.html>

upvoted 1 times

mwwt2022 2 months, 3 weeks ago

Why B is wrong?

upvoted 1 times

Cyberkayu 3 months, 1 week ago

BCD, on-demand backup, manual work

upvoted 3 times

beginnercloud 4 months, 4 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/database/set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/>

upvoted 2 times

chanchal133 7 months ago

Selected Answer: A

A is right ans

upvoted 1 times

MNotABot 8 months, 2 weeks ago

All except A are "On-demand"

upvoted 3 times

narddrer 8 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/BackupRestore.html>

Using DynamoDB with AWS Backup, you can copy your on-demand backups across AWS accounts and Regions, add cost allocation tags to on-demand backups, and transition on-demand backups to cold storage for lower costs. To use these advanced features, you must opt in to AWS Backup.

upvoted 4 times

👤 **pentium75** 2 months, 3 weeks ago

"on demand" (manual) backup -> hell no
upvoted 2 times

👤 **kruasan** 11 months ago

Selected Answer: A

This solution satisfies the requirements in the following ways:

- AWS Backup will automatically take full backups of the DynamoDB table on the schedule defined in the backup plan (the first of each month).
- The lifecycle policy can transition backups to cold storage after 6 months, meeting that requirement.
- Setting a 7-year retention period in the backup plan will ensure each backup is retained for 7 years as required.
- AWS Backup manages the backup jobs and lifecycle policies, requiring no custom scripting or management.

upvoted 2 times

👤 **TariqKipkemei** 12 months ago

Answer is A

upvoted 1 times

👤 **TariqKipkemei** 5 months, 3 weeks ago

Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years

upvoted 1 times

👤 **mmustafa4455** 1 year ago

Selected Answer: A

The correct Answer is A

<https://aws.amazon.com/blogs/database/set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/>

upvoted 1 times

👤 **mmustafa4455** 1 year ago

Its B.

<https://aws.amazon.com/blogs/database/set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/>

upvoted 2 times

👤 **Wael216** 1 year, 1 month ago

Selected Answer: A

A is the answer

upvoted 1 times

👤 **LuckyAro** 1 year, 1 month ago

Selected Answer: A

A is the answer.

upvoted 1 times

👤 **skiwili** 1 year, 1 month ago

Selected Answer: A

A is the correct answe

upvoted 1 times

👤 **rrharris** 1 year, 1 month ago

A is the Answer

can be used to create backup schedules and retention policies for DynamoDB tables

upvoted 2 times

👤 **kpato87** 1 year, 1 month ago

Selected Answer: A

A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.

upvoted 3 times

Question #280

Topic 1

A company is using Amazon CloudFront with its website. The company has enabled logging on the CloudFront distribution, and logs are saved in one of the company's Amazon S3 buckets. The company needs to perform advanced analyses on the logs and build visualizations.

What should a solutions architect do to meet these requirements?

- A. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
- B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.
- C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
- D. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.

Correct Answer: A

Community vote distribution



✉ **rrharris** Highly Voted 1 year, 1 month ago

Answer is B - Quicksite creating data visualizations

<https://docs.aws.amazon.com/quicksight/latest/user/welcome.html>
upvoted 6 times

✉ **LoXoL** Most Recent 1 month, 3 weeks ago

Selected Answer: B

Glue is meant to prepare and transform data for analytics, not to build visualizations. Hence A and C are out.
Athena is used to analyze data stored in S3 and it is commonly used with QuickSight, thus B is the answer
upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

Selected Answer: B

Data is in S3 -> Athena, not DynamoDB (thus A or B)
Visualize -> QuickSight, not Glue (thus B or D)
upvoted 3 times

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

Admin please remove my comment. That answer was for another question.
upvoted 1 times

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

A & C combined make sense isn't it?
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Why 'use queries in DynamoDB' when the data is in S3? And why Glue?
upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: B

OptionB: Amazon Athena allows you to run standard SQL queries directly on the data stored in the S3 bucket.
Amazon QuickSight is a business intelligence (BI) service that allows you to create interactive and visual dashboards to analyze data. You can connect Amazon QuickSight to Amazon Athena to visualize the results of your SQL queries from the CloudFront logs.
upvoted 2 times

✉ **A1975** 7 months, 3 weeks ago

Selected Answer: B

OptionB: Amazon Athena allows you to run standard SQL queries directly on the data stored in the S3 bucket.
Amazon QuickSight is a business intelligence (BI) service that allows you to create interactive and visual dashboards to analyze data. You can connect Amazon QuickSight to Amazon Athena to visualize the results of your SQL queries from the CloudFront logs.
upvoted 1 times

✉ **ajay258** 10 months, 1 week ago

Answer is B
upvoted 1 times

✉ **FF0** 11 months, 2 weeks ago

Selected Answer: B

Athena and Quicksight. Glue is for ETL transformation

upvoted 1 times

✉ **TariqKipkemei** 12 months ago

Answer is B

Analysis on S3 = Athena

Visualizations = Quicksight

upvoted 1 times

✉ **GalileoEC2** 1 year ago

Why the Hell A?

upvoted 1 times

✉ **GalileoEC2** 1 year ago

Why A! as far as I know Glue is not used for visualization

upvoted 1 times

✉ **Bhrino** 1 year, 1 month ago

Selected Answer: B

B because athena can be used to analyse data in s3 buckets and AWS quicksight is literally used to create visual representation of data

upvoted 1 times

✉ **LuckyAro** 1 year, 1 month ago

Selected Answer: B

Using Athena to query the CloudFront logs in the S3 bucket and QuickSight to visualize the results is the best solution because it is cost-effective, scalable, and requires no infrastructure setup. It also provides a robust solution that enables the company to perform advanced analysis and build interactive visualizations without the need for a dedicated team of developers.

upvoted 1 times

✉ **skiwili** 1 year, 1 month ago

Selected Answer: B

Yes B is the answer

upvoted 1 times

✉ **obatunde** 1 year, 1 month ago

Selected Answer: B

Correct answer should be B.

upvoted 1 times

✉ **Namrash** 1 year, 1 month ago

B is correct

upvoted 1 times

Question #281

Topic 1

A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.

Which solution meets these requirements?

- A. Enable a Multi-AZ deployment for the DB instance.
- B. Enable auto scaling for the DB instance in one Availability Zone.
- C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.
- D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Correct Answer: D*Community vote distribution*

KZM Highly Voted 1 year, 1 month ago

A:

By using Multi-AZ deployment, the company can achieve an RPO of less than 1 second because the standby instance is always in sync with the primary instance, ensuring that data changes are continuously replicated.

upvoted 16 times

rrharris Highly Voted 1 year, 1 month ago

Correct Answer is A

upvoted 7 times

pentium75 Most Recent 2 months, 3 weeks ago

I'm unsure with A, because the term RPO is not only applied to datacenter outages. Say, an application error corrupts the database, or an administrator accidentally overwrites all records. With answer A, Multi-AZ, these changes would be instantly copied to the replica.

Only reason why A might still be correct is that the other answers don't make much more sense.

B has nothing to do with RPO at all

C could lose more than 1 second since read replicas are asynchronous

D could be part of a solution but the CDC task alone won't help

upvoted 3 times

A1975 7 months, 3 weeks ago

Selected Answer: A

Read Replicas:

Read Replicas are asynchronous and support read scalability.

It is used to improve performance.

Read Replicas can be in the same region or in a different region for disaster recovery purposes, but this involves manual intervention, which means Read Replicas do not provide automatic failover and requires DNS updates and application changes

Multi-AZ:

Multi-AZ maintains a synchronous standby replica of the primary instance in a different Availability Zone within the same region.

Multi-AZ deployments provide high availability and automatic failover.

Option A is better choice with respect to below statement,

"the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases."

upvoted 7 times

narddrer 8 months, 3 weeks ago

Selected Answer: D

option A doesn't provide Data integrity only achieved in Option D using CDC.

upvoted 1 times

FFO 11 months, 2 weeks ago

Selected Answer: A

Used for DR. Every single change is replicated in a standby AZ. If we lose the main AZ, (uses the same DNS name) standby becomes automatic failover and the new main DB.

upvoted 3 times

TariqKipkemei 12 months ago

Answer is A
High availability = Multi AZ
upvoted 1 times

 **Steve_4542636** 1 year ago

Selected Answer: A

My vote is A
upvoted 1 times

 **ManOnTheMoon** 1 year, 1 month ago

Agree with A
upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: A

Multi-AZ is a synchronous communication with the Master in "real time" and fail over will be almost instant.
upvoted 3 times

 **GwonLEE** 1 year, 1 month ago

Selected Answer: A

correct is A
upvoted 1 times

 **Namrash** 1 year, 1 month ago

A should be correct
upvoted 2 times

 **Joan111edu** 1 year, 1 month ago

Selected Answer: A

should be A
upvoted 2 times

Question #282

Topic 1

A company runs a web application that is deployed on Amazon EC2 instances in the private subnet of a VPC. An Application Load Balancer (ALB) that extends across the public subnets directs web traffic to the EC2 instances. The company wants to implement new security measures to restrict inbound traffic from the ALB to the EC2 instances while preventing access from any other source inside or outside the private subnet of the EC2 instances.

Which solution will meet these requirements?

- A. Configure a route in a route table to direct traffic from the internet to the private IP addresses of the EC2 instances.
- B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.
- C. Move the EC2 instances into the public subnet. Give the EC2 instances a set of Elastic IP addresses.
- D. Configure the security group for the ALB to allow any TCP traffic on any port.

Correct Answer: C

Community vote distribution

B (100%)

 **Abrar2022** Highly Voted 9 months, 3 weeks ago

Read the discussion, that's the whole point why examtopics picks the wrong answer. Follow most voted answer not examtopics answer
upvoted 8 times

 **Guru4Cloud** Most Recent 6 months, 3 weeks ago

Selected Answer: B

Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB
upvoted 3 times

 **awslearner7** 8 months, 1 week ago

can anybody explains the question?
upvoted 2 times

 **theochan** 2 months, 1 week ago

i don't even understand what the question is trying to ask
upvoted 1 times

 **David_Ang** 4 months, 3 weeks ago

is just admins fault dont worry, he just made a mistake, because "C" doesnt make any sence
upvoted 1 times

 **antropaws** 10 months ago

Selected Answer: B

It's very confusing that the system marks C as correct.
upvoted 1 times

 **FFO** 11 months, 2 weeks ago

Selected Answer: B

This is B. Question already tells us they only want ONLY traffic from the ALB.
upvoted 1 times

 **TariqKipkemei** 12 months ago

Answer is B
upvoted 1 times

 **TariqKipkemei** 5 months, 3 weeks ago

A security group acts as a firewall that controls the traffic allowed to and from the resources in your virtual private cloud (VPC).
upvoted 1 times

 **GalileoEC2** 1 year ago

Why C! another crazy answer , If i am concern about security why I would want to expose my EC2 to the public internet,not make sense at all, am I correct with this? I also go with B
upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: B

B is the correct answer.

upvoted 2 times

 **kpato87** 1 year, 1 month ago

Selected Answer: B

configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB. This ensures that only the traffic originating from the ALB is allowed access to the EC2 instances in the private subnet, while denying any other traffic from other sources. The other options do not provide a suitable solution to meet the stated requirements.

upvoted 3 times

 **Bhawesh** 1 year, 1 month ago

Selected Answer: B

B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.

upvoted 3 times

Question #283

Topic 1

A research company runs experiments that are powered by a simulation application and a visualization application. The simulation application runs on Linux and outputs intermediate data to an NFS share every 5 minutes. The visualization application is a Windows desktop application that displays the simulation output and requires an SMB file system.

The company maintains two synchronized file systems. This strategy is causing data duplication and inefficient resource usage. The company needs to migrate the applications to AWS without making code changes to either application.

Which solution will meet these requirements?

- A. Migrate both applications to AWS Lambda. Create an Amazon S3 bucket to exchange data between the applications.
- B. Migrate both applications to Amazon Elastic Container Service (Amazon ECS). Configure Amazon FSx File Gateway for storage.
- C. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon Simple Queue Service (Amazon SQS) to exchange data between the applications.
- D. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon FSx for NetApp ONTAP for storage.

Correct Answer: D

Community vote distribution

D (98%)

LuckyAro 1 year, 1 month ago

Selected Answer: D

Amazon FSx for NetApp ONTAP provides shared storage between Linux and Windows file systems.

upvoted 22 times

rrharris 1 year, 1 month ago

Answer is D

upvoted 7 times

awsgeek75 2 months, 1 week ago

Selected Answer: D

It is D but I think NetApp ONTAP is an oversell in this context. They just needed a FSx solution not a whole expensive managed service...

ABC are a lot of change to the code so D is the only choice here anyway

upvoted 1 times

djgodzilla 2 months, 2 weeks ago

Selected Answer: D

Amazon FSx for NetApp ONTAP

Fully managed service offering shared storage between Linux and Windows file systems (Multi & Single-AZ) up to petabytes datasets and 10+Gbps.

- Allows Multi-protocol access to data using the (NFS), Server Message Block (SMB), and Internet Small Computer Systems Interface (iSCSI) protocols
- Integrated with other AWS services (KMS, IAM, CloudTrail, amazon workspace)
- ideal solution to migrate, back up, or burst your file-based applications from on-prem to AWS without application code change.

upvoted 1 times

pentium75 2 months, 3 weeks ago

Selected Answer: D

A would require code changes

B might also require code changes, and "FSx File Gateway" provides SMB access (not NFS)

C uses SQS which has no place here

D can provide same storage via SMB and NFS

upvoted 1 times

osmk 3 months, 1 week ago

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html>

upvoted 1 times

TariqKipkemei 5 months, 3 weeks ago

Selected Answer: D

One of the use cases for Amazon FSx for NetApp ONTAP is when you need to move workloads running on NetApp or other NFS/SMB/iSCSI servers to AWS without modifying application code or how you manage data.

upvoted 3 times

Guru4Cloud 6 months, 3 weeks ago

Selected Answer: D

The key requirements are:

- Simulation app runs on Linux, outputs data to NFS
- Visualization app runs on Windows, requires SMB file system
- Migrate apps to AWS without code changes
- Eliminate data duplication and inefficient resource usage

upvoted 2 times

Abrar2022 9 months, 3 weeks ago

For shared storage between Linux and windows you need to implement Amazon FSx for NetApp ONTAP

upvoted 2 times

kruasan 11 months ago

Selected Answer: D

This solution satisfies the needs in the following ways:

- Amazon EC2 provides a seamless migration path for the existing server-based applications without code changes. The simulation app can run on Linux EC2 instances and the visualization app on Windows EC2 instances.
- Amazon FSx for NetApp ONTAP provides highly performant file storage that is accessible via both NFS and SMB. This allows the simulation app to write to NFS shares as currently designed, and the visualization app to access the same data via SMB.
- FSx for NetApp ONTAP ensures the data is synchronized and up to date across the file systems. This addresses the data duplication issues of the current setup.
- Resources can be scaled efficiently since EC2 and FSx provide scalable compute and storage on demand.

upvoted 6 times

kruasan 11 months ago

The other options would require more significant changes:

- A. Migrating to Lambda would require re-architecting both applications and not meet the requirement to avoid code changes. S3 does not provide file system access.
- B. While ECS could run the apps without code changes, FSx File Gateway only provides S3 or EFS storage, neither of which offer both NFS and SMB access. Data exchange would still be an issue.
- C. Using SQS for data exchange between EC2 instances would require code changes to implement a messaging system rather than a shared file system.

upvoted 1 times

mr_kanchan 7 months, 3 weeks ago

How does the data duplication issue get addressed on selecting D ?

upvoted 1 times

Reckless_Jas 7 months ago

Maybe I'm wrong, but I feel like the data is duplicated between the two types of EC2 instances. By using the FSX ONTAP will address this issue.

upvoted 1 times

pentium75 2 months, 3 weeks ago

Because FSx for ONTAP provides THE SAME STORAGE via NFS and SMB. Duplication issue occurred because Linux saved the files via NFS to one storage, then the data was copied to ANOTHER storage that shared it via SMB.

upvoted 1 times

Wael216 1 year ago

Selected Answer: D

windows => FSX

we didn't mention containers => can't be ECS

upvoted 1 times

everfly 1 year, 1 month ago

Selected Answer: D

Amazon FSx for NetApp ONTAP is a fully managed service that provides shared file storage built on NetApp's popular ONTAP file system. It supports NFS, SMB, and iSCSI protocols2 and also allows multi-protocol access to the same data

upvoted 1 times

Yechi 1 year, 1 month ago

Selected Answer: D

Amazon FSx for NetApp ONTAP is a fully-managed shared storage service built on NetApp's popular ONTAP file system. Amazon FSx for NetApp ONTAP provides the popular features, performance, and APIs of ONTAP file systems with the agility, scalability, and simplicity of a fully managed AWS service, making it easier for customers to migrate on-premises applications that rely on NAS appliances to AWS. FSx for ONTAP file systems are similar to on-premises NetApp clusters. Within each file system that you create, you also create one or more storage virtual machines (SVMs). These are isolated file servers each with their own endpoints for NFS, SMB, and management access, as well as authentication (for both administration and end-user data access). In turn, each SVM has one or more volumes which store your data.

<https://aws.amazon.com/de/blogs/storage/getting-started-cloud-file-storage-with-amazon-fsx-for-netapp-ontap-using-netapp-management-tools/>

upvoted 3 times

 **zTopic** 1 year, 1 month ago

Selected Answer: B

B is correct I believe

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

"FSx File Gateway" is a gateway, and ECS would require code changes.

upvoted 1 times

Question #284

Topic 1

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.

Which solution meets these requirements?

- A. Run a query with Amazon Athena to generate the report.
- B. Create a report in Cost Explorer and download the report.
- C. Access the bill details from the billing dashboard and download the bill.
- D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Correct Answer: B

Community vote distribution

B (100%)

✉️  **DagsH**  1 year ago

Selected Answer: B

Cost Explorer looks at the usage pattern or history
upvoted 6 times

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

Selected Answer: B

Create a report in Cost Explorer and download the report
upvoted 1 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: B

- ° Cost Explorer is a AWS service that allows you to view, analyze, and manage your AWS costs and usage. It provides a variety of reports that you can use to track your costs, including a report of AWS billed items listed by user.
- ° Creating a report in Cost Explorer is a quick and easy way to get the information you need. You can customize the report to include the specific data you want, and you can download the report in a variety of formats, including CSV, Excel, and PDF.

upvoted 2 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

This is trick question -

You need to know the differences between the billing services.

upvoted 1 times

✉️  **Wheretostart** 1 year ago

Selected Answer: B

Cost Explorer
upvoted 1 times

✉️  **pcops** 1 year, 1 month ago

Answer is B
upvoted 2 times

✉️  **fulingyu288** 1 year, 1 month ago

Selected Answer: B

Answer is B
upvoted 3 times

✉️  **rrharris** 1 year, 1 month ago

Answer is B
upvoted 2 times

Question #285

A company hosts its static website by using Amazon S3. The company wants to add a contact form to its webpage. The contact form will have dynamic server-side components for users to input their name, email address, phone number, and user message. The company anticipates that there will be fewer than 100 site visits each month.

Which solution will meet these requirements MOST cost-effectively?

- A. Host a dynamic contact form page in Amazon Elastic Container Service (Amazon ECS). Set up Amazon Simple Email Service (Amazon SES) to connect to any third-party email provider.
- B. Create an Amazon API Gateway endpoint with an AWS Lambda backend that makes a call to Amazon Simple Email Service (Amazon SES).
- C. Convert the static webpage to dynamic by deploying Amazon Lightsail. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.
- D. Create a t2.micro Amazon EC2 instance. Deploy a LAMP (Linux, Apache, MySQL, PHP/Perl/Python) stack to host the webpage. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.

Correct Answer: B

Community vote distribution

B (91%) 9%

obatunde **Highly Voted** 1 year, 1 month ago

Selected Answer: B

Correct answer is B. <https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/>

upvoted 8 times

kruasan **Highly Voted** 11 months ago

Selected Answer: B

This solution is the most cost-efficient for the anticipated 100 monthly visits because:

- API Gateway charges are based on API calls. With only 100 visits, charges would be minimal.
- AWS Lambda provides compute time for the backend code in increments of 100ms, so charges would also be negligible for this workload.
- Amazon SES is used only for sending emails from the submitted contact forms. SES has a generous free tier of 62,000 emails per month, so there would be no charges for sending the contact emails.
- No EC2 instances or other infrastructure needs to be run and paid for.

upvoted 5 times

awsgeek75 **Most Recent** 2 months, 1 week ago

Option D just made me laugh!

upvoted 2 times

Guru4Cloud 6 months, 3 weeks ago

Selected Answer: B

B is the most cost-effective solution for this use case.

The key requirements are:

Static website hosted on S3

Add a contact form with server-side processing

Low traffic website (<100 visits per month)

upvoted 2 times

rogerHS 8 months, 3 weeks ago

why not C

upvoted 2 times

Guru4Cloud 6 months, 3 weeks ago

Option C uses Lightsail which incurs charges even at low usage. Not cost effective for low traffic sites.

upvoted 2 times

pentium75 2 months, 3 weeks ago

Also it has been decided that "the contact form will have dynamic server-side components ", thus "use client-side scripting to build the contact form" is not what has been asked for.

upvoted 2 times

datz 11 months, 3 weeks ago

Selected Answer: B

B would be cheaper than option D,

Member only 100 site visits per month, so you are comparing API GW used 100 times a month with constantly running EC2...
upvoted 1 times

Steve_4542636 1 year ago

Selected Answer: B

Both api gateway and lambda are serverless so charges apply only on the 100 form submissions per month
upvoted 1 times

bdp123 1 year, 1 month ago

Selected Answer: B

After looking at cost of Workmail compared to SES - probably 'B' is better
upvoted 2 times

bdp123 1 year, 1 month ago

Selected Answer: D

Create a t2 micro Amazon EC2 instance. Deploy a LAMP (Linux Apache MySQL, PHP/Perl/Python) stack to host the webpage (free open-source). Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail. This solution will provide the company with the necessary components to host the contact form page and integrate it with Amazon WorkMail at the lowest cost. Option A requires the use of Amazon ECS, which is more expensive than EC2, and Option B requires the use of Amazon API Gateway, which is also more expensive than EC2. Option C requires the use of Amazon Lightsail, which is more expensive than EC2.
<https://aws.amazon.com/what-is/lamp-stack/>

upvoted 1 times

Guru4Cloud 6 months, 3 weeks ago

Option D uses EC2 which has a higher monthly cost than serverless options. LAMP stack adds complexity for a simple contact form.
upvoted 1 times

SkyZeroZx 10 months, 4 weeks ago

3 million API Gateway == 3,50 USD (EE.UU. Este (Ohio))

Is more cheaper letter B

<https://aws.amazon.com/es/api-gateway/pricing/>

<https://aws.amazon.com/es/lambda/pricing/>

upvoted 1 times

Palanda 1 year, 1 month ago

Selected Answer: B

It's B

upvoted 1 times

LuckyAro 1 year, 1 month ago

Selected Answer: B

B allows the company to create an API endpoint using AWS Lambda, which is a cost-effective and scalable solution for a contact form with low traffic. The backend can make a call to Amazon SES to send email notifications, which simplifies the process and reduces complexity.
upvoted 1 times

cloudbusting 1 year, 1 month ago

it is B : <https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/>
upvoted 3 times

bdp123 1 year, 1 month ago

Selected Answer: D

<https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html>
Using AWS Lambda with Amazon API Gateway - AWS Lambda
<https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html>
<https://aws.amazon.com/lambda/faqs/>
AWS Lambda FAQs
<https://aws.amazon.com/lambda/faqs/>
upvoted 1 times

Guru4Cloud 6 months, 3 weeks ago

Option D uses EC2 which has a higher monthly cost than serverless options. LAMP stack adds complexity for a simple contact form.
upvoted 1 times

Question #286

Topic 1

A company has a static website that is hosted on Amazon CloudFront in front of Amazon S3. The static website uses a database backend. The company notices that the website does not reflect updates that have been made in the website's Git repository. The company checks the continuous integration and continuous delivery (CI/CD) pipeline between the Git repository and Amazon S3. The company verifies that the webhooks are configured properly and that the CI/CD pipeline is sending messages that indicate successful deployments.

A solutions architect needs to implement a solution that displays the updates on the website.

Which solution will meet these requirements?

- A. Add an Application Load Balancer.
- B. Add Amazon ElastiCache for Redis or Memcached to the database layer of the web application.
- C. Invalidate the CloudFront cache.
- D. Use AWS Certificate Manager (ACM) to validate the website's SSL certificate.

Correct Answer: B

Community vote distribution

C (95%) 5%

✉️ **fulingyu288** 1 year, 1 month ago

Selected Answer: C

Invalidate the CloudFront cache: The solutions architect should invalidate the CloudFront cache to ensure that the latest version of the website is being served to users.

upvoted 9 times

✉️ **jayantp04** 3 months, 1 week ago

Correct C, because Invalidating the CloudFront cache will force CloudFront to fetch the latest content from Amazon S3.

Not B because not related to clear cache

upvoted 3 times

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

Selected Answer: C

Invalidate the CloudFront cache so that it can read the updated static page from S3.

upvoted 1 times

✉️ **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: C

C. Invalidate the CloudFront cache

upvoted 1 times

✉️ **Damdom** 7 months, 1 week ago

C. Invalidate the CloudFront cache.

Explanation:

Invalidate the CloudFront cache to ensure that the latest updates from the Git repository are reflected on the static website. When updates are made to the website's Git repository and deployed to Amazon S3, the CloudFront cache may still be serving the old cached content to users. By invalidating the CloudFront cache, you're instructing CloudFront to fetch fresh content from the origin (Amazon S3) and serve it to users.

upvoted 4 times

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

Selected Answer: C

C is the most reasonable cause, though the question is not well-written - "The static website uses a database backend." does not make a lot of sense to me.

upvoted 2 times

✉️ **kruasan** 11 months ago

Selected Answer: B

Since the static website is hosted behind CloudFront, updates made to the S3 bucket will not be visible on the site until the CloudFront cache expires or is invalidated. By invalidating the CloudFront cache after deploying updates, the latest version in S3 will be pulled and the updates will then appear on the live site.

upvoted 1 times

✉️  **RoroJ** 10 months, 1 week ago

Isn't that C?
upvoted 4 times

✉️  **Namrash** 1 year, 1 month ago

B should be the right one
upvoted 1 times

✉️  **Neorem** 1 year, 1 month ago

Selected Answer: C

We need to create an Cloudfront invalidation
upvoted 2 times

✉️  **Bhawesh** 1 year, 1 month ago

Selected Answer: C

C. Invalidate the CloudFront cache.
Problem is the CF cache. After invalidating the CloudFront cache, CF will be forced to read the updated static page from the S3 and the S3 changes will start being visible.
upvoted 3 times

Question #287

Topic 1

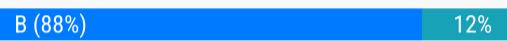
A company wants to migrate a Windows-based application from on premises to the AWS Cloud. The application has three tiers: an application tier, a business tier, and a database tier with Microsoft SQL Server. The company wants to use specific features of SQL Server such as native backups and Data Quality Services. The company also needs to share files for processing between the tiers.

How should a solutions architect design the architecture to meet these requirements?

- A. Host all three tiers on Amazon EC2 instances. Use Amazon FSx File Gateway for file sharing between the tiers.
- B. Host all three tiers on Amazon EC2 instances. Use Amazon FSx for Windows File Server for file sharing between the tiers.
- C. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.
- D. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume for file sharing between the tiers.

Correct Answer: B

Community vote distribution



✉️ **KZM** Highly Voted 1 year, 1 month ago

It is B:

A: Incorrect > FSx file Gateway designed for low latency and efficient access to in-cloud FSx for Windows File Server file shares from your on-premises facility.

B: Correct > This solution will allow the company to host all three tiers on Amazon EC2 instances while using Amazon FSx for Windows File Server to provide Windows-based file sharing between the tiers. This will allow the company to use specific features of SQL Server, such as native backups and Data Quality Services, while sharing files for processing between the tiers.

C: Incorrect > Currently, Amazon EFS supports the NFSv4.1 protocol and does not natively support the SMB protocol, and can't be used in Windows instances yet.

D: Incorrect > Amazon EBS is a block-level storage solution that is typically used to store data at the operating system level, rather than for file sharing between servers.

upvoted 15 times

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

Selected Answer: B

RDS for SQL Backups: aren't Native MSSQL backups Instead RDS creates a storage volume snapshot of the instance, backing up the entire instance not just individual databases.

upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

Selected Answer: B

Not A - File Gateway is just a gateway, needs S3 too

B - Yes

Not C - RDS does not support the required features, and EFS does not provide SMB

Not D - RDS does not support the required features, and EBS volume shared between tiers doesn't make sense

upvoted 3 times

✉️ **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: B

B. Host all three tiers on Amazon EC2 instances. Use Amazon FSx for Windows File Server for file sharing between the tiers.

upvoted 1 times

✉️ **Abrar2022** 9 months, 3 weeks ago

The question mentions Microsoft = windows

EFS is Linux

upvoted 1 times

✉️ **kruasan** 11 months ago

Selected Answer: B

This design satisfies the needs in the following ways:

- Running all tiers on EC2 allows using SQL Server on EC2 with its native features like backups and Data Quality Services. SQL Server cannot be run directly on RDS.
- Amazon FSx for Windows File Server provides fully managed Windows file storage with SMB access. This allows sharing files between the

Windows EC2 instances for all three tiers.

- FSx for Windows File Server has high performance, so it can handle file sharing needs between the tiers.

upvoted 1 times

 **kruasan** 11 months ago

The other options would not meet requirements:

- A. FSx File Gateway only provides access to S3 or EFS storage. It cannot be used directly for Windows file sharing.
- C. RDS cannot run SQL Server or its native tools. The database tier needs to run on EC2.
- D. EBS volumes can only be attached to a single EC2 instance. They cannot be shared between tiers for file exchanges.

upvoted 1 times

 **Netgear** 6 months, 1 week ago

No, there is RDS for SQL Server.

<https://aws.amazon.com/rds/sqlserver/>

upvoted 2 times

 **fageroff** 5 months, 2 weeks ago

IO2 support multi-attach

upvoted 1 times

 **ManOnTheMoon** 1 year, 1 month ago

Why not C?

upvoted 1 times

 **KZM** 1 year, 1 month ago

Currently, Amazon EFS supports the NFSv4.1 protocol and does not natively support the SMB protocol, and can't be used in Windows instances yet.

upvoted 3 times

 **AlmeroSenior** 1 year, 1 month ago

Selected Answer: B

Yup B . RDS will not work , Native Backup only to S3 , and Data Quality is not supported , so all EC2 .

<https://aws.amazon.com/premiumsupport/knowledge-center/native-backup-rds-sql-server/> and <https://www.sqlserver-dba.com/2021/07/aws-rds-sql-server-limitations.html>

upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

After further research, I concur that the correct answer is B. Native Back up and Data Quality not supported on RDS for Ms SQL

upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: C

C.

Host the application tier and the business tier on Amazon EC2 instances.

Host the database tier on Amazon RDS.

Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.

This solution allows the company to use specific features of SQL Server such as native backups and Data Quality Services, by hosting the database tier on Amazon RDS. It also enables file sharing between the tiers using Amazon EFS, which is a fully managed, highly available, and scalable file system. Amazon EFS provides shared access to files across multiple instances, which is important for processing files between the tiers. Additionally, hosting the application and business tiers on Amazon EC2 instances provides the company with the flexibility to configure and manage the environment according to their requirements.

upvoted 2 times

 **rushi0611** 10 months, 3 weeks ago

How are you gonna connect the EFS to windows based ??

upvoted 2 times

 **Yechi** 1 year, 1 month ago

Selected Answer: B

Data Quality Services: If this feature is critical to your workload, consider choosing Amazon RDS Custom or Amazon EC2.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-sql-server/comparison.html>

upvoted 3 times

 **Bhawesh** 1 year, 1 month ago

Selected Answer: B

Correct Answer: B

upvoted 3 times

Question #288

Topic 1

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. The company must not make any changes to the application.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 Standard bucket with access to the web servers.
- B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
- C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.
- D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Correct Answer: A

Community vote distribution

C (100%)

✉  **Bhawesh**  1 year, 1 month ago

Selected Answer: C

Since no code change is permitted, below choice makes sense for the unix server's file sharing:

C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.

upvoted 14 times

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

Selected Answer: C

Rehost the application webservers on EC2 and Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.

upvoted 1 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: C

Since no code change is permitted, below choice makes sense for the unix server's file sharing:

upvoted 1 times

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

Selected Answer: C

Since no code change is permitted, below choice makes sense for the unix server's file sharing:

upvoted 1 times

✉  **antropaws** 10 months ago

Selected Answer: C

C is correct.

upvoted 1 times

✉  **kruasan** 11 months ago

Selected Answer: C

This solution satisfies the needs in the following ways:

- EFS provides a fully managed elastic network file system that can be mounted on multiple EC2 instances concurrently.
- The EFS file system appears as a standard file system mount on the Linux web servers, requiring no application changes. The servers can access shared files as if they were on local storage.
- EFS is highly available, durable, and scalable, providing a robust shared storage solution.

upvoted 2 times

✉  **kruasan** 11 months ago

The other options would require modifying the application or do not provide a standard file system:

- A. S3 does not provide a standard file system mount or share. The application would need to be changed to access S3 storage.
- B. CloudFront is a content delivery network and caching service. It does not provide a file system mount or share and would require application changes.
- D. EBS volumes can only attach to a single EC2 instance. They cannot be mounted by multiple servers concurrently and do not provide a shared file system.

upvoted 2 times

✉  **Steve_4542636** 1 year ago

Selected Answer: C

No application changes are allowed and EFS is compatible with Linux

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: C

C is the answer:

Create an Amazon Elastic File System (Amazon EFS) file system.

Mount the EFS file system on all web servers.

To meet the requirements of providing a shared file store for Linux-based web servers without making changes to the application, using an Amazon EFS file system is the best solution.

Amazon EFS is a managed NFS file system service that provides shared access to files across multiple Linux-based instances, which makes it suitable for this use case.

Amazon S3 is not ideal for this scenario since it is an object storage service and not a file system, and it requires additional tools or libraries to mount the S3 bucket as a file system.

Amazon CloudFront can be used to improve content delivery performance but is not necessary for this requirement.

Additionally, Amazon EBS volumes can only be mounted to one instance at a time, so it is not suitable for sharing files across multiple instances.
upvoted 2 times

 **Karlos99** 1 year ago

But what about aws ebs multi attach?

upvoted 2 times

 **elearningtakai** 12 months ago

Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple instances. EBS General Purpose SSD (gp3) doesn't support Multi-Attach

upvoted 1 times

Question #289

Topic 1

A company has an AWS Lambda function that needs read access to an Amazon S3 bucket that is located in the same AWS account.

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

- A. Apply an S3 bucket policy that grants read access to the S3 bucket.
- B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket.
- C. Embed an access key and a secret key in the Lambda function's code to grant the required IAM permissions for read access to the S3 bucket.
- D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets in the account.

Correct Answer: D

Community vote distribution

B (100%)

 **Rido4good** 2 months ago

Has anyone passed this exam, choosing the wrong answers from ExamTopics? or what's the reason for the confusion???
upvoted 1 times

 **bbgun891404021** 2 months, 2 weeks ago

Selected Answer: B

B is correct.
upvoted 1 times

 **TMabs** 5 months, 2 weeks ago

Answer=B
upvoted 1 times

 **antropaws** 10 months ago

Selected Answer: B

B is correct.
upvoted 1 times

 **kruasan** 11 months ago

Selected Answer: B

This solution satisfies the needs in the most secure manner:

- An IAM role provides temporary credentials to the Lambda function to access AWS resources. The function does not have persistent credentials.
- The IAM policy grants least privilege access by specifying read access only to the specific S3 bucket needed. Access is not granted to all S3 buckets.
- If the Lambda function is compromised, the attacker would only gain access to the one specified S3 bucket. They would not receive broad access to resources.

upvoted 4 times

 **kruasan** 11 months ago

The other options are less secure:

- A. A bucket policy grants open access to a resource. It is a less granular way to provide access and grants more privilege than needed.
- C. Embedding access keys in code is extremely insecure and against best practices. The keys provide full access and are at major risk of compromise if the code leaks.
- D. Granting access to all S3 buckets provides far too much privilege if only one bucket needs access. It greatly expands the impact if compromised.

upvoted 3 times

 **Dr_Chomp** 11 months, 2 weeks ago

Selected Answer: B

you dont want to grant access to all S3 buckets (which is answer D) - only the one identified (so answer A)

upvoted 2 times

 **Steve_4542636** 1 year ago

Selected Answer: B

B is only for one bucket and you want to use Role based security here.

upvoted 1 times

 **Ja13** 1 year, 1 month ago

Selected Answer: B

C, it says MOST secure manner, so only to one bucket

upvoted 1 times

Joxtat 1 year, 1 month ago

Selected Answer: B

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

upvoted 1 times

kpato87 1 year, 1 month ago

Selected Answer: B

This is the most secure and recommended way to provide an AWS Lambda function with access to an S3 bucket. It involves creating an IAM role that the Lambda function assumes, and attaching an IAM policy to the role that grants the necessary permissions to read from the S3 bucket.

upvoted 3 times

Joan111edu 1 year, 1 month ago

Selected Answer: B

B. Least of privilege

upvoted 2 times

Question #290

Topic 1

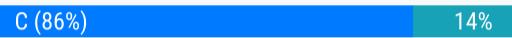
A company hosts a web application on multiple Amazon EC2 instances. The EC2 instances are in an Auto Scaling group that scales in response to user demand. The company wants to optimize cost savings without making a long-term commitment.

Which EC2 instance purchasing option should a solutions architect recommend to meet these requirements?

- A. Dedicated Instances only
- B. On-Demand Instances only
- C. A mix of On-Demand Instances and Spot Instances
- D. A mix of On-Demand Instances and Reserved Instances

Correct Answer: B

Community vote distribution



✉️ **ExamGuru727** 2 days, 7 hours ago

Selected Answer: C

On-demand + spot for additional capacity will save costs.

upvoted 1 times

✉️ **thewalker** 1 month, 3 weeks ago

Selected Answer: B

On-Demand.

upvoted 1 times

✉️ **Krishhhh** 3 months, 2 weeks ago

Any one have dumps

upvoted 1 times

✉️ **Burrito69** 1 day, 11 hours ago

After seeing this website answers I wouldn't trust dumps. I rather go on each question through discussion, chatgpt and aws account for any practical to see whats right and whats wrong. I have been through dumps and those are fed with wrong answers too. Its not worth it there. just get through each question here and you'll get it for sure. Im doing it and i am getting it.

upvoted 1 times

✉️ **Mikado211** 3 months, 2 weeks ago

Selected Answer: C

There is a little trap here, because in the way this question is asked, both B and C are true since we don't know if it's production or not.

In a production environment C is absolutely forbidden and B is the good solution, we even have questions in this dump about this case.

In a dev environment spot instances are good if you don't care about stability so C can be a good answer.

Since this question is all about cost, let's go for the stingy rat solution, spot instances are cheaper, so C is correct.

upvoted 4 times

✉️ **beginnercloud** 4 months, 4 weeks ago

Selected Answer: C

It's about COST, not operational efficiency for this question :) C is correct

upvoted 3 times

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

Selected Answer: C

A mix of On-Demand Instances to handle baseline workload and Spot Instances to handle excess workload.

upvoted 3 times

✉️ **Kt** 6 months, 1 week ago

Exam topic is not free anymore. Anyone has free access ?

upvoted 1 times

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

for now though, I have still access.

upvoted 2 times

 **Damdom** 7 months, 1 week ago

Selected Answer: C

By combining On-Demand Instances for steady-state workloads or critical components and Spot Instances for less critical or burstable workloads, you can achieve a balance between cost savings and performance. This strategy allows you to optimize costs without making a long-term commitment, as Spot Instances provide cost savings without the need for upfront payments or long-term contracts.

upvoted 3 times

 **Abrar2022** 9 months, 3 weeks ago

Selected Answer: C

It's about COST, not operational efficiency for this question.

upvoted 3 times

 **kraken21** 12 months ago

Selected Answer: C

Autoscaling with ALB / scale up on demand using on demand and spot instance combination makes sense. Reserved will not fit the no-long term commitment clause.

upvoted 1 times

 **Whericanstart** 1 year ago

Selected Answer: C

Without commitment....Spot instances

upvoted 1 times

 **cegama543** 1 year ago

Selected Answer: B

If the company wants to optimize cost savings without making a long-term commitment, then using only On-Demand Instances may not be the most cost-effective option. Spot Instances can be significantly cheaper than On-Demand Instances, but they come with the risk of being interrupted if the Spot price increases above your bid price. If the company is willing to accept this risk, a mix of On-Demand Instances and Spot Instances may be the best option to optimize cost savings while maintaining the desired level of scalability.

However, if the company wants the most predictable pricing and does not want to risk instance interruption, then using only On-Demand Instances is a good choice. It ultimately depends on the company's priorities and risk tolerance.

upvoted 3 times

 **pentium75** 2 months, 3 weeks ago

First, the question is about cost, cost, cost. Second, answer C is "a mix of on-demand and spot instances"; they could still use on-demand if spot is not available.

upvoted 2 times

 **Steve_4542636** 1 year ago

Selected Answer: C

It's about COST, not operational efficiency for this question.

upvoted 1 times

 **Samuel03** 1 year, 1 month ago

Selected Answer: C

Should be C

upvoted 1 times

 **bdp123** 1 year, 1 month ago

Selected Answer: C

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-mixed-instances-groups.html>

upvoted 1 times

 **AlmeroSenior** 1 year, 1 month ago

Selected Answer: C

C - WEB apps , mostly Stateless , and ASG support OnDemand and Spot mix , in fact , you can prioritize to have Ondemand , before it uses Spot > <https://docs.aws.amazon.com/autoscaling/ec2/userguide/launch-template-spot-instances.html>

upvoted 1 times

 **designmood22** 1 year, 1 month ago

Selected Answer: C

Answer : C. A mix of On-Demand Instances and Spot Instances

upvoted 1 times

Question #291

Topic 1

A media company uses Amazon CloudFront for its publicly available streaming video content. The company wants to secure the video content that is hosted in Amazon S3 by controlling who has access. Some of the company's users are using a custom HTTP client that does not support cookies. Some of the company's users are unable to change the hardcoded URLs that they are using for access.

Which services or methods will meet these requirements with the LEAST impact to the users? (Choose two.)

- A. Signed cookies
- B. Signed URLs
- C. AWS AppSync
- D. JSON Web Token (JWT)
- E. AWS Secrets Manager

Correct Answer: CE

Community vote distribution

AB (86%)

11%

✉  **leoatff**  1 year, 1 month ago

Selected Answer: AB

I thought that option A was totally wrong, because the question mentions "HTTP client does not support cookies". However it is right, along with option B. Check the link below, first paragraph.

<https://aws.amazon.com/blogs/media/secure-content-using-cloudfront-functions/>

upvoted 22 times

✉  **bujuman** 2 weeks, 6 days ago

Plus, Customers can choose to use either one or both, depending on the use case.

Thanks for this share !

upvoted 1 times

✉  **Steve_4542636** 1 year ago

Thanks for this! What a tricky question. If the client doesn't support cookies, THEN they use the signed S3 URLs.

upvoted 9 times

✉  **AAAWrekng** 5 months ago

LOL, like the old question, in my hand I have 2 coins, and they equal 15 cents, one of them is not a nickel. What are the coins

upvoted 4 times

✉  **johnmcclane78**  1 year ago

B. Signed URLs - This method allows the media company to control who can access the video content by creating a time-limited URL with a cryptographic signature. This URL can be distributed to the users who are unable to change the hardcoded URLs they are using for access, and they can access the content without needing to support cookies.

D. JSON Web Token (JWT) - This method allows the media company to control who can access the video content by creating a secure token that contains user authentication and authorization information. This token can be distributed to the users who are using a custom HTTP client that does not support cookies. The users can include this token in their requests to access the content without needing to support cookies.

Therefore, options B and D are the correct answers.

Option A (Signed cookies) would not work for users who are using a custom HTTP client that does not support cookies. Option C (AWS AppSync) is not relevant to the requirement of securing video content. Option E (AWS Secrets Manager) is a service used for storing and retrieving secrets, which is not relevant to the requirement of securing video content.

upvoted 18 times

✉  **ONS_KH** 5 months, 1 week ago

This is the response of chatgpt isn't it ? Pay attention ! it doesn't always give the right answer

upvoted 4 times

✉  **pentium75** 2 months, 3 weeks ago

So you want to 'distribute the signed URL to the users who are unable to change the hardcoded URL'?

upvoted 1 times

✉  **lostmagnet001**  1 month, 2 weeks ago

Selected Answer: AB

a little tricky but you have to "control" access, ok dont support cookies, so put signed cookies.

upvoted 1 times

✉ ray320x 1 month, 2 weeks ago

so how many marks do you get if you get 1 wrong

upvoted 2 times

✉ awsgeek75 2 months, 1 week ago

Selected Answer: AB

If you have gotten this far and got THIS trick question right then you are going to make it! Good Luck!

upvoted 3 times

✉ pentium75 2 months, 3 weeks ago

Selected Answer: AB

'SOME are using a client that does not support cookies' -> use signed URLs

'SOME are unable to change the hardcoded URLs' -> used signed cookies

upvoted 8 times

✉ ale_brd_ 3 months ago

Selected Answer: AB

Signed URLs and signed cookies are the most suitable options. They can effectively address the requirements of both users with custom HTTP clients and those with hardcoded URLs.

upvoted 1 times

✉ prabhjot 5 months, 3 weeks ago

B & E - B. Signed URLs: This allows you to generate time-limited URLs with a signature that grants temporary access to specific resources in your S3 bucket. It doesn't rely on cookies and can be generated for users without requiring any changes to their HTTP client or hardcoded URLs. This method provides fine-grained control over access to your content.

E. AWS Secrets Manager: While AWS Secrets Manager can be useful for managing and rotating secrets, it is not directly related to securing S3 content in the context of the question. It's not one of the primary methods for securing access to S3 objects.

upvoted 1 times

✉ TariqKipkemei 5 months, 3 weeks ago

Selected Answer: AB

To secure streaming video content from Amazon CloudFront, two methods are available: signed cookies or signed URLs. Customers can choose to use either one or both, depending on the use case.

upvoted 3 times

✉ tabbyDolly 6 months, 1 week ago

AB - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

upvoted 1 times

✉ Guru4Cloud 6 months, 3 weeks ago

Selected Answer: BD

B and D are the correct options for meeting the requirements with the least impact to users.

Signed URLs allow access to individual objects in Amazon S3 for a specified time period without requiring cookies. This allows the custom HTTP client users to access content.

JSON Web Tokens (JWT) allow users to get temporary access tokens that can be passed in requests. This allows users with hardcoded URLs to access content without updating URLs.

upvoted 2 times

✉ Guru4Cloud 6 months, 3 weeks ago

No good

Signed cookies require client support and may impact users.

AWS AppSync and Secrets Manager do not help address the specific access requirements.

Good

So Signed URLs and JWTs allow securing access to S3 content with minimal impact to users, meeting the requirements.

upvoted 1 times

✉ riccardoto 7 months, 3 weeks ago

Selected Answer: BD

I understand why many users here are voting AB, but in my opinion BD is more correct.

Using JWT or signed urls will work both for users that cannot use cookies or cannot change the url.

upvoted 2 times

✉ katedel 8 months, 1 week ago

Selected Answer: AB

it's correct

upvoted 1 times

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

Selected Answer: CE

These are the right answers!

upvoted 2 times

✉  **DrWatson** 9 months, 3 weeks ago

Selected Answer: AB

"Some of the company's users" does not support cookies, then they'll use Signed URLs.

"Some of the company's users" are unable to change the hardcoded URLs, then they'll use Signed cookies.

upvoted 4 times

✉  **kruasan** 11 months ago

Selected Answer: AB

Signed cookies would allow the media company to authorize access to related content (like HLS video segments) with a single signature, minimizing implementation overhead. This works for users that can support cookies.

Signed URLs would allow the media company to sign each URL individually to control access, supporting users that cannot use cookies. By embedding the signature in the URL, existing hardcoded URLs would not need to change.

upvoted 3 times

✉  **kruasan** 11 months ago

C. AWS AppSync - This is for building data-driven apps with real-time and offline capabilities. It does not directly help with securing streaming content.

D. JSON Web Token (JWT) - Although JWTs can be used for authorization, they would require the client to get a token and validate/check access on the server for each request. This does not work for hardcoded URLs and minimizes impact.

E. AWS Secrets Manager - This service is for managing secrets, not for controlling access to resources. It would not meet the requirements.

upvoted 2 times

✉  **ale_brd_** 3 months ago

Nicely put

upvoted 1 times

✉  **Shrestwt** 11 months, 1 week ago

A. Signed cookies: CloudFront signed cookies allow you to control who can access your content when you don't want to change your current URLs.
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html>

B. Signed URLs: This method allows the media company to control who can access the video content by creating a time-limited URL with a cryptographic signature.

upvoted 1 times

Question #292

Topic 1

A company is preparing a new data platform that will ingest real-time streaming data from multiple sources. The company needs to transform the data before writing the data to Amazon S3. The company needs the ability to use SQL to query the transformed data.

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

- A. Use Amazon Kinesis Data Streams to stream the data. Use Amazon Kinesis Data Analytics to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
- B. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use AWS Glue to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
- C. Use AWS Database Migration Service (AWS DMS) to ingest the data. Use Amazon EMR to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
- D. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use Amazon Kinesis Data Analytics to transform the data and to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.
- E. Use Amazon Kinesis Data Streams to stream the data. Use AWS Glue to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.

Correct Answer: AB

Community vote distribution



✉ **Steve_4542636** 1 year ago

Selected Answer: AB

OK, for B I did some research, <https://docs.aws.amazon.com/glue/latest/dg/add-job-streaming.html>

"You can create streaming extract, transform, and load (ETL) jobs that run continuously, consume data from streaming sources like Amazon Kinesis Data Streams, Apache Kafka, and Amazon Managed Streaming for Apache Kafka (Amazon MSK). The jobs cleanse and transform the data, and then load the results into Amazon S3 data lakes or JDBC data stores."

upvoted 12 times

✉ **Paras043** 11 months, 3 weeks ago

But how can you transform data using kinesis data analytics ??

upvoted 5 times

✉ **luisgu** 10 months, 3 weeks ago

See <https://aws.amazon.com/kinesis/data-analytics/faqs/?nc=sn&loc=6>

upvoted 2 times

✉ **awsgeek75** 2 months, 1 week ago

Selected Answer: AB

Just because C is not going to work a DE use RDS so totally illogical

A & B seem to have redundant streaming, transformation and query steps so not sure if these are the right choices but CDE are completely wrong anyway!

upvoted 2 times

✉ **farnamjam** 2 months, 3 weeks ago

For A didn't know that Kinesis Analytics can transform the data as well:

Amazon Kinesis Data Analytics provides built-in functions to filter, aggregate, and transform streaming data for advanced analytics. It processes streaming data with sub-second latencies, enabling you to analyze and respond to incoming data and streaming events in real time.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Selected Answer: AB

"Use SQL to query the transformed data" [which is in S3] requires Athena, thus D and E are out. DMS is nonsense here thus C is out.

upvoted 2 times

✉ **MiniYang** 3 months, 3 weeks ago

why E is not right choise?

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Because you can't "use the Amazon RDS query editor to query .. data from S3"

upvoted 1 times

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

Selected Answer: AB

options A and B will meet these requirements.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: AB

A and B are correct.

A uses Kinesis Data Streams for streaming, Kinesis Data Analytics for transformation, Kinesis Data Firehose for writing to S3, and Athena for SQL queries on S3 data.

B uses Amazon MSK for streaming, AWS Glue for transformation and writing to S3, and Athena for SQL queries on S3 data.

upvoted 2 times

✉ **Diqian** 7 months, 1 week ago

Why E is incorrect?

upvoted 3 times

✉ **awsgeek75** 2 months, 1 week ago

"Use the Amazon RDS query editor to query the transformed data from Amazon S3." is not possible as RDS query editor is for RDS and not for S3

upvoted 2 times

✉ **MrCloudy** 11 months, 1 week ago

Selected Answer: AE

To transform real-time streaming data from multiple sources, write it to Amazon S3, and query the transformed data using SQL, the company can use the following solutions: Amazon Kinesis Data Streams, Amazon Kinesis Data Analytics, and Amazon Kinesis Data Firehose. The transformed data can be queried using Amazon Athena. Therefore, options A and E are the correct answers.

Option A is correct because it uses Amazon Kinesis Data Streams to stream data from multiple sources, Amazon Kinesis Data Analytics to transform the data, and Amazon Kinesis Data Firehose to write the data to Amazon S3. Amazon Athena can be used to query the transformed data in Amazon S3.

Option E is also correct because it uses Amazon Kinesis Data Streams to stream data from multiple sources, AWS Glue to transform the data, and Amazon Kinesis Data Firehose to write the data to Amazon S3. Amazon Athena can be used to query the transformed data in Amazon S3.

upvoted 3 times

✉ **sand444** 6 months ago

Amazon Athena is not in option E

upvoted 7 times

✉ **kraken21** 12 months ago

Selected Answer: AB

DMS can move data from DBs to streaming services and cannot natively handle streaming data. Hence A.B makes sense. Also AWS Glue/ETL can handle MSK streaming <https://docs.aws.amazon.com/glue/latest/dg/add-job-streaming.html>.

upvoted 2 times

✉ **elearningtakai** 12 months ago

Selected Answer: AB

The solutions that meet the requirements of streaming real-time data, transforming the data before writing to S3, and querying the transformed data using SQL are A and B.

Option C: This option is not ideal for streaming real-time data as AWS DMS is not optimized for real-time data ingestion.

Option D & E: These options are not recommended as the Amazon RDS query editor is not designed for querying data in S3, and it is not efficient for running complex queries.

upvoted 4 times

✉ **gold4otas** 12 months ago

Selected Answer: AB

The correct answers are options A & B

upvoted 1 times

✉ **TungPham** 1 year ago

may Amazon RDS query editor to query the transformed data from Amazon S3 ?

i don't think so, plz get link docs to that

upvoted 1 times

✉ **ManOnTheMoon** 1 year, 1 month ago

Why not A & D?

upvoted 1 times

✉ **TungPham** 1 year ago

may Amazon RDS query editor to query the transformed data from Amazon S3 ?

i don't think so, plz get link docs to that

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: AB

A and B

upvoted 1 times

 **designmood22** 1 year, 1 month ago

Answer is : A & B

upvoted 1 times

Question #293

Topic 1

A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.

Which solution meets these requirements?

- A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
- B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
- C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.
- D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Correct Answer: D*Community vote distribution*

D (100%)

Steve_4542636 Highly Voted 1 year ago

Selected Answer: D

The question states, "wants to maintain local access to all the data" This is storage gateway. Cached gateway stores only the frequently accessed data locally which is not what the problem statement asks for.

upvoted 11 times

kruasan Highly Voted 11 months ago

Selected Answer: D

1. The company wants to maintain local access to all the data. Only stored volumes keep the complete dataset on-premises, providing low-latency access. Cached volumes only cache a subset locally.
2. The company wants the data backed up on AWS. With stored volumes, periodic backups (snapshots) of the on-premises data are sent to S3, providing durable and scalable backup storage.
3. The company wants the data transfer to AWS to be automatic and secure. Storage Gateway provides an encrypted connection between the on-premises gateway and AWS storage. Backups to S3 are sent asynchronously and automatically based on the backup schedule configured.

upvoted 8 times

TariqKipkemei Most Recent 5 months, 3 weeks ago

Selected Answer: D

The Volume Gateway runs in either a cached or stored mode.

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access.

In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

<https://aws.amazon.com/storagegateway/faqs/#:~:text=What%20is%20Volume%20Gateway%3F>

upvoted 6 times

Guru4Cloud 6 months, 3 weeks ago

Selected Answer: D

@kruasan well explained

upvoted 1 times

ChrisG1454 1 year, 1 month ago

Ans = D

<https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html>

upvoted 3 times

Neha999 1 year, 1 month ago

D

<https://www.examtopics.com/discussions/amazon/view/43725-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

bdp123 1 year, 1 month ago

Selected Answer: D

<https://aws.amazon.com/storagegateway/faqs/#:~:text=In%20the%20cached%20mode%2C%20your,asynchronously%20backed%20up%20to%20AWS>.

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access. In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

upvoted 2 times

Question #294**Topic 1**

An application that is hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Traffic must not traverse the internet.

How should a solutions architect configure access to meet these requirements?

- A. Create a private hosted zone by using Amazon Route 53.
- B. Set up a gateway VPC endpoint for Amazon S3 in the VPC.
- C. Configure the EC2 instances to use a NAT gateway to access the S3 bucket.
- D. Establish an AWS Site-to-Site VPN connection between the VPC and the S3 bucket.

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

 **TariqKipkemei** 5 months, 3 weeks ago

Selected Answer: B

Set up a gateway VPC endpoint for Amazon S3 in the VPC.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: B

The correct answer is B. Set up a gateway VPC endpoint for Amazon S3 in the VPC.

A gateway VPC endpoint is a private way for Amazon EC2 instances in a VPC to access AWS services, such as Amazon S3, without having to go through the internet. This can help to improve security and performance.

upvoted 3 times

 **Steve_4542636** 1 year ago

Selected Answer: B

S3 and DynamoDB are the only services with Gateway endpoint options

upvoted 3 times

 **ManOnTheMoon** 1 year, 1 month ago

Agree with B

upvoted 1 times

 **jennyka76** 1 year, 1 month ago

ANSWER - B

<https://docs.aws.amazon.com/vpc/latest/privateLink/gateway-endpoints.html> B

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

 **skiwili** 1 year, 1 month ago

Selected Answer: B

Bbbbbbbb

upvoted 3 times

Question #295

Topic 1

An ecommerce company stores terabytes of customer data in the AWS Cloud. The data contains personally identifiable information (PII). The company wants to use the data in three applications. Only one of the applications needs to process the PII. The PII must be removed before the other two applications process the data.

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

- A. Store the data in an Amazon DynamoDB table. Create a proxy application layer to intercept and process the data that each application requests.
- B. Store the data in an Amazon S3 bucket. Process and transform the data by using S3 Object Lambda before returning the data to the requesting application.
- C. Process the data and store the transformed data in three separate Amazon S3 buckets so that each application has its own custom dataset. Point each application to its respective S3 bucket.
- D. Process the data and store the transformed data in three separate Amazon DynamoDB tables so that each application has its own custom dataset. Point each application to its respective DynamoDB table.

Correct Answer: B

Community vote distribution



✉ **Steve_4542636** 1 year ago

Selected Answer: B

Actually this is what Macie is best used for.
upvoted 13 times

✉ **Mikado211** 3 months, 3 weeks ago

Yes. That's the problem here, Macie is the recommended tool in such case, but you do not have it in the answers.
upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Macie is for identifying the PII data. Here it's much simpler because one of the apps need the PII data and other apps don't so you don't need to identify the PII data as you know it is already there. You just need to identify the app that needs the data which is not the best use case for Macie
upvoted 1 times

✉ **fruto123** 1 year, 1 month ago

Selected Answer: B

B is the right answer and the proof is in this link.

<https://aws.amazon.com/blogs/aws/introducing-amazon-s3-object-lambda-use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/>
upvoted 10 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

This is so wrong
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

But it matches the exact use case here.
upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Why do you think this is wrong?
upvoted 1 times

✉ **MikeJANG** 1 month, 1 week ago

Selected Answer: C

[GPT4] while S3 Object Lambda is a powerful tool for real-time data transformation, it is not the best fit for processing very large datasets due to Lambda's execution limits(15 min). Instead, preprocessing the data and storing it in separate S3 buckets for each application's needs is a more operationally efficient solution for the scenario described.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Selected Answer: B

Because this is exactly what the AWS blog says.

"When you store data in Amazon Simple Storage Service (Amazon S3), you can easily share it for use by multiple applications. However, each application has its own requirements and may need a different view of the data. For example, a dataset created by an e-commerce application may include personally identifiable information (PII) that is not needed when the same data is processed for analytics and should be redacted."

upvoted 4 times

 **pentium75** 2 months, 3 weeks ago

"Today, I'm very happy to announce the availability of S3 Object Lambda, a new capability that allows you to add your own code to process data retrieved from S3 before returning it to an application. S3 Object Lambda works with your existing applications and uses AWS Lambda functions to automatically process and transform your data as it is being retrieved from S3. The Lambda function is invoked inline with a standard S3 GET request, so you don't need to change your application code."

<https://aws.amazon.com/de/blogs/aws/introducing-amazon-s3-object-lambda-use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/>

upvoted 5 times

 **meowruki** 3 months, 3 weeks ago

B. Store the data in an Amazon S3 bucket. Process and transform the data by using S3 Object Lambda before returning the data to the requesting application.

This solution allows you to use S3 Object Lambda to process and transform the data on-the-fly as it is requested by each application. S3 Object Lambda enables you to apply custom code to your data retrieval requests, allowing you to remove PII before returning the data to the requesting application. This eliminates the need to create and manage separate storage locations for each application, reducing operational overhead.

upvoted 1 times

 **rvca231** 5 months ago

Selected Answer: C

Why would you reprocess the data every time you request it when you can just filter it once and be done?

Because of this I think A and B are highly inefficient, leaving us with C and D as options.

Since S3 is better suited for Data Lakes, I think C is the answer.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

Because this is exactly what the AWS blog says.

"When you store data in Amazon Simple Storage Service (Amazon S3), you can easily share it for use by multiple applications. However, each application has its own requirements and may need a different view of the data. For example, a dataset created by an e-commerce application may include personally identifiable information (PII) that is not needed when the same data is processed for analytics and should be redacted. ... Today, I'm very happy to announce the availability of S3 Object Lambda, a new capability that allows you to add your own code to process data retrieved from S3 before returning it to an application. S3 Object Lambda works with your existing applications and uses AWS Lambda functions to automatically process and transform your data as it is being retrieved from S3."

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Least operational overhead. The DevOps team is throwing this problem to the developers which is why C is not best.

upvoted 1 times

 **Abrar2022** 9 months, 3 weeks ago

Selected Answer: B

Store the data in an Amazon S3 bucket and using S3 Object Lambda to process and transform the data before returning it to the requesting application. This approach allows the PII to be removed in real-time and without the need to create separate datasets or tables for each application.

upvoted 1 times

 **antropaws** 10 months ago

Selected Answer: A

@fruto123 and everyone that upvoted:

Is it plausible that S3 Object Lambda can process terabytes of data in 60 seconds? The same link you shared states that the maximum duration for a Lambda function used by S3 Object Lambda is 60 seconds.

Answer is A.

upvoted 2 times

 **antropaws** 10 months ago

Chat GPT:

Isn't just 60 seconds the maximum duration for a Lambda function used by S3 Object Lambda? How can it process terabytes of data in 60 seconds?

You are correct that the maximum duration for a Lambda function used by S3 Object Lambda is 60 seconds.

Given the time constraint, it is not feasible to process terabytes of data within a single Lambda function execution.

S3 Object Lambda is designed for lightweight and real-time transformations rather than extensive processing of large datasets.

To handle terabytes of data, you would typically need to implement a distributed processing solution using services like Amazon EMR, AWS Glue, or AWS Batch. These services are specifically designed to handle big data workloads and provide scalability and distributed processing capabilities.

So, while S3 Object Lambda can be useful for lightweight processing tasks, it is not the appropriate tool for processing terabytes of data within the execution time limits of a Lambda function.

upvoted 2 times

 **Kp88** 8 months ago

Terabyte is just the storage. Lambda only need to process which application request. Think like removing/scratching off your social security number before sharing your doc to a third party.

upvoted 2 times

 **kruasan** 11 months ago

Selected Answer: B

- Storing the raw data in S3 provides a durable, scalable data lake. S3 requires little ongoing management overhead.
- S3 Object Lambda can be used to filter and process the data on retrieval transparently. This minimizes operational overhead by avoiding the need to preprocess and store multiple transformed copies of the data.
- Only one copy of the data needs to be stored and maintained in S3. S3 Object Lambda will transform the data on read based on the requesting application.
- No additional applications or proxies need to be developed and managed to handle the data transformation. S3 Object Lambda provides this functionality.

upvoted 2 times

 **kruasan** 11 months ago

Option A requires developing and managing a proxy app layer to handle data transformation, adding overhead.

Options C and D require preprocessing and storing multiple copies of the transformed data, adding storage and management overhead.

Option B using S3 Object Lambda minimizes operational overhead by handling data transformation on read transparently using the native S3 functionality. Only one raw data copy is stored in S3, with no additional applications required.

upvoted 1 times

 **pagom** 1 year, 1 month ago

Selected Answer: B

<https://aws.amazon.com/ko/blogs/korea/introducing-amazon-s3-object-lambda-use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/>

upvoted 4 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: B

B is the correct answer.

Amazon S3 Object Lambda allows you to add custom code to S3 GET requests, which means that you can modify the data before it is returned to the requesting application. In this case, you can use S3 Object Lambda to remove the PII before the data is returned to the two applications that do not need to process PII. This approach has the least operational overhead because it does not require creating separate datasets or proxy application layers, and it allows you to maintain a single copy of the data in an S3 bucket.

upvoted 4 times

 **NolaHolla** 1 year, 1 month ago

To meet the requirement of removing the PII before processing by two of the applications, it would be most efficient to use option B, which involves storing the data in an Amazon S3 bucket and using S3 Object Lambda to process and transform the data before returning it to the requesting application. This approach allows the PII to be removed in real-time and without the need to create separate datasets or tables for each application. S3 Object Lambda can be configured to automatically remove PII from the data before it is sent to the non-PII processing applications. This solution provides a cost-effective and scalable way to meet the requirement with the least operational overhead.

upvoted 2 times

 **minglu** 1 year, 1 month ago

Selected Answer: B

I think it is B.

upvoted 1 times

 **skiwili** 1 year, 1 month ago

Selected Answer: C

Looks like C is the correct answer

upvoted 2 times

Question #296

Topic 1

A development team has launched a new application that is hosted on Amazon EC2 instances inside a development VPC. A solutions architect needs to create a new VPC in the same account. The new VPC will be peered with the development VPC. The VPC CIDR block for the development VPC is 192.168.0.0/24. The solutions architect needs to create a CIDR block for the new VPC. The CIDR block must be valid for a VPC peering connection to the development VPC.

What is the SMALLEST CIDR block that meets these requirements?

- A. 10.0.1.0/32
- B. 192.168.0.0/24
- C. 192.168.1.0/32
- D. 10.0.1.0/24

Correct Answer: B

Community vote distribution

D (98%)

✉️  **BrainOBrain**  1 year, 1 month ago

Selected Answer: D

10.0.1.0/32 and 192.168.1.0/32 are too small for VPC, and /32 network is only 1 host
192.168.0.0/24 is overlapping with existing VPC
upvoted 23 times

✉️  **kruasan**  11 months ago

Selected Answer: D

- Option A (10.0.1.0/32) is invalid - a /32 CIDR prefix is a host route, not a VPC range.
 - Option B (192.168.0.0/24) overlaps the development VPC and so cannot be used.
 - Option C (192.168.1.0/32) is invalid - a /32 CIDR prefix is a host route, not a VPC range.
 - Option D (10.0.1.0/24) satisfies the non-overlapping CIDR requirement but is a larger block than needed. Since only two VPCs need to be peered, a /24 block provides more addresses than necessary.
- upvoted 8 times

✉️  **TheFivePips**  4 weeks ago

Selected Answer: D

In an Amazon VPC, the first four and the last IP address in each subnet are reserved for specific purposes, and they cannot be used for customer instances. Here's how the reserved addresses are typically allocated:

Network Address (First IP):

The first IP address (all zeros in the host portion) in a subnet is reserved as the network address. For example, if you have a subnet with a CIDR notation of 10.0.0.0/24, the network address would be 10.0.0.0.

VPC Router (Second IP):

The second IP address in the subnet is reserved for the VPC router.

DNS Server (Third IP):

The third IP address is reserved for the DNS server.

Reserved for Future Use (Fourth IP):

The fourth IP address is reserved for future use.

Customer Instances (Fifth to Second-to-Last IP):

The IP addresses from the fifth to the second-to-last IP address in the subnet are available for customer instances.

Broadcast Address (Last IP):

The last IP address (all ones in the host portion) in a subnet is reserved as the broadcast address, even though AWS does not support broadcast.

upvoted 2 times

✉️  **walter9660** 1 month ago

Selected Answer: C

10.0.0.0 - 10.255.255.255 (10/8 prefix): Example CIDR block: 10.0.0.0/16

172.16.0.0 - 172.31.255.255 (172.16/12 prefix): Example CIDR block: 172.31.0.0/16

192.168.0.0 - 192.168.255.255 (192.168/16 prefix): Example CIDR block: 192.168.0.0/20

Given that the development VPC already uses 192.168.0.0/24, we need to choose a non-overlapping CIDR block. The smallest valid CIDR block that meets the requirements is 192.168.1.0/24 (Option C).

upvoted 1 times

✉ **Murtadhaceit** 3 months, 3 weeks ago

Selected Answer: D

A and C are host IP addresses.
B is not possible because it's using the same subnet for the other team/department.
We are left with D, which is the right answer.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: D

10.0.1.0/32 and 192.168.1.0/32 are too small for VPC, and /32 network is only 1 host
192.168.0.0/24 is overlapping with existing VPC

upvoted 1 times

✉ **Abrar2022** 9 months, 3 weeks ago

Definitely D. The only valid VPC CIDR block that does not overlap with the development VPC CIDR block among the options. The other 2 CIDR block options are too small.

upvoted 1 times

✉ **antropaws** 10 months ago

Selected Answer: D

D is correct.
upvoted 1 times

✉ **channn** 11 months, 4 weeks ago

Selected Answer: D

D is the only correct answer
upvoted 1 times

✉ **r04dB10ck** 1 year ago

Selected Answer: D

only one valid with no overlap
upvoted 1 times

✉ **Steve_4542636** 1 year ago

Selected Answer: D

A process by elimination solution here. a CIDR value is the number of bits that are locked so 10.0.0.0/32 means no range.
upvoted 3 times

✉ **LuckyAro** 1 year, 1 month ago

Selected Answer: D

Answer is D, 10.0.1.0/24.
upvoted 1 times

✉ **skiwili** 1 year, 1 month ago

Selected Answer: D

Yes D is the answer
upvoted 1 times

✉ **obatunde** 1 year, 1 month ago

Selected Answer: D

Definitely D. It is the only valid VPC CIDR block that does not overlap with the development VPC CIDR block among the options.
upvoted 1 times

✉ **bdp123** 1 year, 1 month ago

Selected Answer: D

The allowed block size is between a /28 netmask and /16 netmask.
The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
<https://docs.aws.amazon.com/vpc/latest/userguide/configure-your-vpc.html>
upvoted 4 times

Question #297

Topic 1

A company deploys an application on five Amazon EC2 instances. An Application Load Balancer (ALB) distributes traffic to the instances by using a target group. The average CPU usage on each of the instances is below 10% most of the time, with occasional surges to 65%.

A solutions architect needs to implement a solution to automate the scalability of the application. The solution must optimize the cost of the architecture and must ensure that the application has enough CPU resources when surges occur.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm that enters the ALARM state when the CPUUtilization metric is less than 20%. Create an AWS Lambda function that the CloudWatch alarm invokes to terminate one of the EC2 instances in the ALB target group.
- B. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set a target tracking scaling policy that is based on the ASGAverageCPUUtilization metric. Set the minimum instances to 2, the desired capacity to 3, the maximum instances to 6, and the target value to 50%. Add the EC2 instances to the Auto Scaling group.
- C. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set the minimum instances to 2, the desired capacity to 3, and the maximum instances to 6. Add the EC2 instances to the Auto Scaling group.
- D. Create two Amazon CloudWatch alarms. Configure the first CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is below 20%. Configure the second CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is above 50%. Configure the alarms to publish to an Amazon Simple Notification Service (Amazon SNS) topic to send an email message. After receiving the message, log in to decrease or increase the number of EC2 instances that are running.

Correct Answer: D

Community vote distribution

B (95%)

5%

 **bdp123**  1 year, 1 month ago

Selected Answer: B

Just create an auto scaling policy
upvoted 13 times

 **vilagiri**  5 months, 4 weeks ago

I picked B.. I am not 100% sure..The application is deployed in 5 instances initially. What is the logic behind 2/3/6 ASG. Because utilization is 10%, we can set min 2? I know for sure I am not going to get this ASG question correct in the exam.
upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: B

The correct answer is B.

This solution will meet the requirements because it will:

Automate the scalability of the application by using EC2 Auto Scaling.

Optimize the cost of the architecture by only scaling the number of EC2 instances up when needed.

Ensure that the application has enough CPU resources when surges occur by setting the target value of the target tracking scaling policy to 50%.
upvoted 1 times

 **ajchi1980** 8 months, 4 weeks ago

Wrong answers: Options A, C, and D are not the most appropriate solutions:

Option A suggests creating a CloudWatch alarm to terminate an EC2 instance when CPU utilization is less than 20%. However, this approach does not ensure that the application will have enough CPU resources during surges, as it only terminates instances when CPU utilization is low, which may not meet the requirements.

Option C suggests creating an Auto Scaling group without any specific scaling policies or configurations. This approach does not address the need for automated scaling based on CPU utilization, making it insufficient for the given requirements.

Option D suggests using CloudWatch alarms to send notifications via Amazon SNS and manually adjusting the number of instances based on the received messages. This approach lacks automation and requires manual intervention, which does not optimize cost or meet the requirement of automated scalability.

Therefore, Option B is the most appropriate solution in this case.

upvoted 2 times

 **ajchi1980** 8 months, 4 weeks ago

Selected Answer: B

Explanation:

Option B leverages EC2 Auto Scaling, which is designed to automatically adjust the number of instances based on specified metrics. By setting a target tracking scaling policy based on average CPU utilization, the Auto Scaling group can dynamically scale the number of instances to maintain the desired level of CPU resources. The minimum instances of 2 ensure a minimum baseline capacity, while the desired capacity of 3 ensures at least three instances are running even during normal traffic. The maximum instances of 6 cap the upper limit to control costs.

upvoted 2 times

 **RoroJ** 10 months, 1 week ago

Selected Answer: D

Auto Scaling group must have an AMI for it.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

"After receiving the message, log in to decrease or increase the number of EC2 instances that are running" does surely not "automate the scalability".

upvoted 2 times

 **th3k33n** 10 months, 2 weeks ago

how can we set max to 6 since the company is using 5 ec2 instance

upvoted 1 times

 **examtopicstempacc** 10 months, 1 week ago

In the scenario you provided, you're setting up an Auto Scaling group to manage the instances for you, and the settings (min 2, desired 3, max 6) are for the Auto Scaling group, not for your existing instances. When you integrate the instances into the Auto Scaling group, you are effectively moving from a fixed instance count to a dynamic one that can range from 2 to 6 based on the demand.

The existing 5 instances can be included in the Auto Scaling group, but the group can reduce the number of instances if the load is low (to the minimum specified, which is 2 in this case) and can also add more instances (up to a maximum of 6) if the load increases.

upvoted 2 times

 **kruasan** 11 months ago

Selected Answer: B

Reasons:

- An Auto Scaling group will automatically scale the EC2 instances to match changes in demand. This optimizes cost by only running as many instances as needed.
- A target tracking scaling policy monitors the ASGAverageCPUUtilization metric and scales to keep the average CPU around the 50% target value. This ensures there are enough resources during CPU surges.
- The ALB and target group are reused, so the application architecture does not change. The Auto Scaling group is associated to the existing load balancer setup.
- A minimum of 2 and maximum of 6 instances provides the ability to scale between 3 and 6 instances as needed based on demand.
- Costs are optimized by starting with only 3 instances (the desired capacity) and scaling up as needed. When CPU usage drops, instances are terminated to match the desired capacity.

upvoted 2 times

 **kruasan** 11 months ago

Option A - terminates instances reactively based on low CPU and may not provide enough capacity during surges. Does not optimize cost.
Option C - lacks a scaling policy so will not automatically adjust capacity based on changes in demand. Does not ensure enough resources during surges.

Option D - requires manual intervention to scale capacity. Does not optimize cost or provide an automated solution.

upvoted 1 times

 **darn** 11 months ago

as you dig down the question, they get more and more bogus with less and less votes

upvoted 1 times

 **Steve_4542636** 1 year ago

Selected Answer: B

B is my vote

upvoted 1 times

 **KZM** 1 year, 1 month ago

Based on the information given, the best solution is option "B".

Autoscaling group with target tracking scaling policy with min 2 instances, desired capacity to 3, and the maximum instances to 6.

upvoted 1 times

 **Shrestwt** 11 months, 1 week ago

But the company is using only 5 EC2 Instances so how can we set maximum instance to 6.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

"Create an EC2 Auto Scaling group" includes replacing your existing EC2 instances with a launch configuration that starts and stops instances automatically.

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

Selected Answer: B

B is the correct solution because it allows for automatic scaling based on the average CPU utilization of the EC2 instances in the target group. With the use of a target tracking scaling policy based on the ASGAverageCPUUtilization metric, the EC2 Auto Scaling group can ensure that the target value of 50% is maintained while scaling the number of instances in the group up or down as needed. This will help ensure that the application has enough CPU resources during surges without overprovisioning, thus optimizing the cost of the architecture.

upvoted 1 times

 **Babba** 1 year, 1 month ago

Selected Answer: B

Should be B

upvoted 1 times

Question #298

Topic 1

A company is running a critical business application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances run in an Auto Scaling group and access an Amazon RDS DB instance.

The design did not pass an operational review because the EC2 instances and the DB instance are all located in a single Availability Zone. A solutions architect must update the design to use a second Availability Zone.

Which solution will make the application highly available?

- A. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
- B. Provision two subnets that extend across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
- C. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.
- D. Provision a subnet that extends across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.

Correct Answer: D

Community vote distribution

C (100%)

✉  bdp123  1 year, 1 month ago

Selected Answer: C

A subnet must reside within a single Availability Zone.

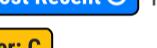
<https://aws.amazon.com/vpc/faqs/#:~:text=Can%20a%20subnet%20span%20Availability,within%20a%20single%20Availability%20Zone>.

upvoted 15 times

✉  zjcorpuz  7 months, 4 weeks ago

a subnet only resides on a one AZ, it does not span to another AZ.

upvoted 5 times

✉  LoXoL  1 month, 2 weeks ago

Selected Answer: C

A subnet can't "Extend" across multiple AZs: B,D out

HA = RDS Multi-AZ: A out

C

upvoted 2 times

✉  thewalker 1 month, 3 weeks ago

Selected Answer: C

An Auto Scaling group can span across two Availability Zones, where one subnet is created in each AZ.

When creating an Auto Scaling group, you need to specify at least one subnet. You can add additional subnets later on, including subnets across multiple AZs.

Auto Scaling will distribute instances evenly across the specified subnets to maintain availability and optimize performance. If one AZ becomes unavailable, instances can be launched in the other AZ.

The associated load balancer should also span the same subnets/AZs as the Auto Scaling group. This allows traffic to be routed to instances in different subnets and AZs, increasing fault tolerance of the application.

upvoted 1 times

✉  TariqKipkemei 5 months, 3 weeks ago

Selected Answer: C

Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment

upvoted 1 times

✉  Guru4Cloud 6 months, 3 weeks ago

Selected Answer: C

This solution will ensure that the EC2 instances and the DB instance are not located in the same Availability Zone, which will improve the availability of the application.

upvoted 2 times

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

Selected Answer: C

D is completely wrong, because each subnet must reside entirely within one Availability Zone and cannot span zones. By launching AWS resources in separate Availability Zones, you can protect your applications from the failure of a single Availability Zone.

upvoted 2 times

✉ **Anmol_1010** 9 months, 2 weeks ago

The key word here was extend.

upvoted 1 times

✉ **GalileoEC2** 1 year ago

This discards B and D: Subnet basics. Each subnet must reside entirely within one Availability Zone and cannot span zones. By launching AWS resources in separate Availability Zones, you can protect your applications from the failure of a single Availability Zone

upvoted 2 times

✉ **Steve_4542636** 1 year ago

Selected Answer: C

a subnet is per AZ. a scaling group can span multiple AZs. <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

upvoted 1 times

✉ **KZM** 1 year, 1 month ago

I think D.

Span the single subnet in both Availability Zones can access the DB instances in either zone without going over the public internet.

upvoted 3 times

✉ **KZM** 1 year, 1 month ago

Can span like that?

upvoted 1 times

✉ **KZM** 1 year, 1 month ago

Sorry I think C is correct.

upvoted 1 times

✉ **leoatf** 1 year, 1 month ago

Nope. The answer is indeed C.

You cannot span like that. Check the link below:

"Each subnet must reside entirely within one Availability Zone and cannot span zones."

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

upvoted 3 times

✉ **KZM** 1 year ago

Thanks, Leoatf for the link you shared.

upvoted 2 times

✉ **Babba** 1 year, 1 month ago

Selected Answer: C

it's C

upvoted 1 times

Question #299

Topic 1

A research laboratory needs to process approximately 8 TB of data. The laboratory requires sub-millisecond latencies and a minimum throughput of 6 GBps for the storage subsystem. Hundreds of Amazon EC2 instances that run Amazon Linux will distribute and process the data.

Which solution will meet the performance requirements?

- A. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to ALL. Import the raw data into the file system. Mount the file system on the EC2 instances.
- B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
- C. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent HDD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
- D. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to NONE. Import the raw data into the file system. Mount the file system on the EC2 instances.

Correct Answer: D

Community vote distribution

B (100%)

 **Bhawesh**  1 year, 1 month ago

Selected Answer: B

Keyword here is a minimum throughput of 6 GBps. Only the FSx for Lustre with SSD option gives the sub-milli response and throughput of 6 GBps or more.

B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.

References:

<https://aws.amazon.com/fsx/when-to-choose-fsx/>

upvoted 13 times

 **bdp123**  1 year, 1 month ago

Selected Answer: B

Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances. Amazon FSx for Lustre uses SSD storage for submillisecond latencies and up to 6 GBps throughput, and can import data from and export data to Amazon S3. Additionally, the option to select persistent SSD storage will ensure that the data is stored on the disk and not lost if the file system is stopped.

upvoted 6 times

 **MrPCarrot**  3 weeks, 6 days ago

Answer is B : FSx for Lustre with SSD option gives the sub-milli response and throughput of 6 GBps or more

upvoted 2 times

 **Pangian** 1 month, 1 week ago

I dont even think that NetApp comes for Linux

upvoted 1 times

 **djgodzilla** 2 months, 2 weeks ago

Selected Answer: B

Amazon FSx for Lustre for compute-intensive workloads.

- allows file-based applications to access data with hundreds of gigabytes per second of data, millions of IOPS, and sub millisecond latencies.
- supports file access to thousands of EC2 instances

and well SSD always wins ;)

upvoted 1 times

 **Mikado211** 3 months, 2 weeks ago

Selected Answer: B

sub-millisecondes == Lustre

HDD vs SSD == for performance use SSD

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: B

Amazon FSx for Lustre with SSD: Amazon FSx for Lustre is designed for high-performance, parallel file processing workloads. Choosing SSD storage ensures fast I/O and meets the sub-millisecond latency requirement.

upvoted 2 times

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

Voto por la B

upvoted 1 times

✉ **Gooniegoogoo** 9 months ago

So many of these are wrong, its good we have people that vote so we can get to the right answer!!

upvoted 1 times

✉ **kruasan** 11 months ago

Selected Answer: B

- Amazon FSx for Lustre with SSD storage can provide up to 260 GB/s of aggregate throughput and sub-millisecond latencies needed for this workload.
- Persistent SSD storage ensures data durability in the file system. Data is also exported to S3 for backup storage.
- The file system will import the initial 8 TB of raw data from S3, providing a fast storage tier for processing while retaining the data in S3.
- The file system is mounted to the EC2 compute instances to distribute processing.
- FSx for Lustre is optimized for high-performance computing workloads running on Linux, matching the EC2 environment.

upvoted 1 times

✉ **kruasan** 11 months ago

Option A - FSx for NetApp ONTAP with ALL tiering policy would not provide fast enough storage tier for sub-millisecond latency. HDD tiers have higher latency.

Option C - FSx for Lustre with HDD storage would not provide the throughput, IOPS or low latency needed.

Option D - FSx for NetApp ONTAP with NONE tiering policy would require much more expensive SSD storage to meet requirements, increasing cost.

upvoted 1 times

✉ **Steve_4542636** 1 year ago

Selected Answer: B

I vote B

upvoted 1 times

✉ **AlmeroSenior** 1 year, 1 month ago

Selected Answer: B

FSX Lustre is 1000mbps per TB provisioned and we have 8TBs so gives us 8GBs . The netapp FSX appears a hard limit of 4gbps .

<https://aws.amazon.com/fsx/lustre/faqs/?nc=sn&loc=5>

<https://aws.amazon.com/fsx/netapp-ontap/faqs/>

upvoted 5 times

✉ **LuckyAro** 1 year, 1 month ago

Selected Answer: B

B is the best choice as it utilizes Amazon S3 for data storage, which is cost-effective and durable, and Amazon FSx for Lustre for high-performance file storage, which provides the required sub-millisecond latencies and minimum throughput of 6 Gbps. Additionally, the option to import and export data to and from Amazon S3 makes it easier to manage and move data between the two services.

B is the best option as it meets the performance requirements for sub-millisecond latencies and a minimum throughput of 6 Gbps.

upvoted 1 times

✉ **everfly** 1 year, 1 month ago

Selected Answer: B

Amazon FSx for Lustre provides fully managed shared storage with the scalability and performance of the popular Lustre file system. It can deliver sub-millisecond latencies and hundreds of gigabytes per second of throughput.

upvoted 3 times

Question #300

Topic 1

A company needs to migrate a legacy application from an on-premises data center to the AWS Cloud because of hardware capacity constraints. The application runs 24 hours a day, 7 days a week. The application's database storage continues to grow over time.

What should a solutions architect do to meet these requirements MOST cost-effectively?

- A. Migrate the application layer to Amazon EC2 Spot Instances. Migrate the data storage layer to Amazon S3.
- B. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon RDS On-Demand Instances.
- C. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon Aurora Reserved Instances.
- D. Migrate the application layer to Amazon EC2 On-Demand Instances. Migrate the data storage layer to Amazon RDS Reserved Instances.

Correct Answer: C

Community vote distribution

C (84%)	B (16%)
---------	---------

✉️  **LuckyAro**  1 year, 1 month ago

Selected Answer: C

Amazon EC2 Reserved Instances allow for significant cost savings compared to On-Demand instances for long-running, steady-state workloads like this one. Reserved Instances provide a capacity reservation, so the instances are guaranteed to be available for the duration of the reservation period.

Amazon Aurora is a highly scalable, cloud-native relational database service that is designed to be compatible with MySQL and PostgreSQL. It can automatically scale up to meet growing storage requirements, so it can accommodate the application's database storage needs over time. By using Reserved Instances for Aurora, the cost savings will be significant over the long term.

upvoted 16 times

✉️  **NolaHolla**  1 year, 1 month ago

Option B based on the fact that the DB storage will continue to grow, so on-demand will be a more suitable solution

upvoted 13 times

✉️  **pentium75** 2 months, 3 weeks ago

Database STORAGE will grow, not performance need (and required instance size).

upvoted 2 times

✉️  **NolaHolla** 1 year, 1 month ago

Since the application's database storage is continuously growing over time, it may be difficult to estimate the appropriate size of the Aurora cluster in advance, which is required when reserving Aurora.

In this case, it may be more cost-effective to use Amazon RDS On-Demand Instances for the data storage layer. With RDS On-Demand Instances, you pay only for the capacity you use and you can easily scale up or down the storage as needed.

upvoted 5 times

✉️  **Joxtat** 1 year, 1 month ago

The Answer is C.

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

upvoted 1 times

✉️  **hristni0** 9 months, 4 weeks ago

Answer is C. From Aurora Reserved Instances documentation:

If you have a DB instance, and you need to scale it to larger capacity, your reserved DB instance is automatically applied to your scaled DB instance. That is, your reserved DB instances are automatically applied across all DB instance class sizes. Size-flexible reserved DB instances are available for DB instances with the same AWS Region and database engine.

upvoted 1 times

✉️  **MrPCarrot**  3 weeks, 6 days ago

Answer is C: Amazon EC2 Reserved Instances and Amazon Aurora Reserved Instances = less expensive than RDS.

upvoted 2 times

✉️  **andyngkh86** 1 month, 3 weeks ago

Amazon Aurora reserved instances is used for the work load on predictable, so answer should be B

upvoted 1 times

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

Selected Answer: B

I think it's B as database storage will grow

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Application runs 24x7 which means database is also used 24x7. The storage will grow and RDS On-Demand does not have auto-grow storage. You have to configure a storage size for RDS which means it will eventually run out of space. RDS On-Demand just scales CPU, not storage.

Aurora has no storage limitation and can scale storage according to need which is what is required here

upvoted 2 times

✉ **Mikado211** 3 months, 3 weeks ago

Selected Answer: C

24/7 forbids spot instances , so A is excluded

Cost efficiency require reserved instances , so D is excluded

Between RDS and Aurora, Aurora is less expensive thanks to the reserved instance, so B is finally excluded

Answer is C

upvoted 1 times

✉ **cciesam** 4 months, 3 weeks ago

Selected Answer: B

I hope it should be B considering Database growth

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Reserved instance applies to the DB instance size (CPU, RAM etc.), not storage.

upvoted 1 times

✉ **Wayne23Fang** 6 months ago

My research concludes that From pure price point of view Aurora Reserved might/ usually be slightly more expensive than On-demand RDS. But RDS has less Operation overhead. For the 24x7 nature, I would vote C. But for pure cost-effective, B is less costly.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: C

This option involves migrating the application layer to Amazon EC2 Reserved Instances and migrating the data storage layer to Amazon Aurora Reserved Instances. Amazon EC2 Reserved Instances provide a significant discount (up to 75%) compared to On-Demand Instance pricing, making them a cost-effective choice for applications that have steady state or predictable usage. Similarly, Amazon Aurora Reserved Instances provide a significant discount (up to 69%) compared to On-Demand Instance pricing.

upvoted 1 times

✉ **ajchi1980** 9 months ago

Selected Answer: C

To meet the requirements of migrating a legacy application from an on-premises data center to the AWS Cloud in a cost-effective manner, the most suitable option would be:

C. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon Aurora Reserved Instances.

Explanation:

Migrating the application layer to Amazon EC2 Reserved Instances allows you to reserve EC2 capacity in advance, providing cost savings compared to On-Demand Instances. This is especially beneficial if the application runs 24/7.

Migrating the data storage layer to Amazon Aurora Reserved Instances provides cost optimization for the growing database storage needs. Amazon Aurora is a fully managed relational database service that offers high performance, scalability, and cost efficiency.

upvoted 1 times

✉ **cpen** 10 months ago

nnascncnscnkknkckl

upvoted 1 times

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

Answer is C

upvoted 1 times

✉ **QuangPham810** 11 months, 1 week ago

Answer is C. Refer https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_WorkingWithReservedDBInstances.html => Size-flexible reserved DB instances

upvoted 1 times

✉ **Abhineet9148232** 1 year ago

Selected Answer: C

C: With Aurora Serverless v2, each writer and reader has its own current capacity value, measured in ACUs. Aurora Serverless v2 scales a writer or reader up to a higher capacity when its current capacity is too low to handle the load. It scales the writer or reader down to a lower capacity when its current capacity is higher than needed.

This is sufficient to accommodate the growing data changes.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html#aurora-serverless-v2.how-it-works.scaling>

upvoted 1 times

✉ **Steve_4542636** 1 year ago

Selected Answer: C

Typically Amazon RDS cost less than Aurora. But here, it's Aurora reserved.

upvoted 1 times

✉ **djgodzilla** 2 months, 2 weeks ago

although agree and AWS wants you to choose Answer C. You can't convince a cloud accounting analyst that Aurora is cheaper than RDS. no matter what

upvoted 1 times

✉ **ACasper** 1 year ago

Answer C

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_WorkingWithReservedDBInstances.html

Discounts for reserved DB instances are tied to instance type and AWS Region.

upvoted 1 times

✉ **AlmeroSenior** 1 year ago

Selected Answer: C

Both RDS and RDS aurora support Storage Auto scale .

Aurora is more expensive than base RDS , But between B and C , the Aurora is reserved instance and base RDS is on demand . Also it states the DB strorage will grow , so no concern about a bigger DB instance (server) , only the actual storage

upvoted 2 times