

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*

A (95%)	5%
---------	----

 **vowaci** Highly Voted 5 days, 22 hours ago

Still valid!! Just passed with total score 824, 90% of the questions are here, I recommend you read all the questions and discussions, if you do, you will have a good chance of passing the exam. <https://t.ly/aUZ5Q>

upvoted 55 times

 **fefef** 2 days, 18 hours ago

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

upvoted 1 times

 **D2w** Highly Voted 1 year, 1 month ago

Selected Answer: A

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

upvoted 48 times

 **Blest012** 4 months, 2 weeks ago

Correct the S3 Transfer Acceleration service is the best for this scenario

upvoted 1 times

 **BoboChow** 1 year, 1 month ago

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

upvoted 1 times

 **sunhat** Most Recent 5 days, 6 hours ago

In case you have pdf version, can you pls send the same to sunhat0115@gmail.com Appreciate your support

upvoted 1 times

 **kam2001** 5 days, 10 hours ago

Please send me pdf dbhblack@proton.com thank you

upvoted 1 times

 **Mohan3516** 5 days, 13 hours ago

Answer is B

upvoted 1 times

 **Genlor** 5 days, 15 hours ago

Selected Answer: A

Enable S3 Transfer Accelerator.

upvoted 1 times

✉️ **bugslife** 1 week ago

Could someone please send me the full pdf version to my email: elvis.ehoro@eatlng.com
Thank you very much.

upvoted 1 times

✉️ **Ruffyit** 1 week, 5 days ago

General line: Collect huge amount of the files across multiple continents
Conditions: High speed Internet connectivity
Task: aggregate the data from all in a single S3 bucket
Requirements: as quick as possible, minimize operational complexity

Correct answer A: S3 Transfer Acceleration because:

- ideally works with objects for long-distance transfer (uses Edge Locations)
- can speed up content transfers to and from S3 as much as 50-500%
- use cases: mobile & web application uploads and downloads, distributed office transfers, data exchange with trusted partners. Generally for sharing of large data sets between companies, customers can set up special access to their S3 buckets with accelerated uploads to speed data exchanges and the pace of innovation.

B - about disaster recovery

C - about transferring data between your local environment and the AWS Cloud

D - about disaster recovery

upvoted 1 times

✉️ **lipi0035** 1 week, 6 days ago

Does anyone have a full pdf version of this exam's questions and answers, could you please send it to lacymaq.0015@yahoo.in?

upvoted 1 times

✉️ **BAPII** 2 weeks ago

In case you have pdf version, can you pls send the same to bhabatosh.555@gmail.com Appreciate your support

upvoted 1 times

✉️ **Sivadocker7** 2 weeks, 3 days ago

Could someone please send me the full pdf version to my email: ssks8p@gmail.com.
I appreciate your help in advance. Thank you very much.

upvoted 1 times

✉️ **anand_here** 3 weeks, 3 days ago

Selected Answer: A

S3 Transfer Acceleration. + multi-part

upvoted 1 times

✉️ **cosmiccliff** 3 weeks, 3 days ago

Thank you ExamTopics! I took SAA exam on 11/03/2023 and passed.

Anyone who's practicing these questions, please go through the discussions you learn and understand a ton!

upvoted 1 times

✉️ **rober_54** 3 weeks, 4 days ago

Can someone please send me the full pdf version? This is my email: maxluki003@gmail.com I appreciate your help in advance. Thank you so much.

upvoted 1 times

✉️ **talia2023** 3 weeks, 4 days ago

Please , Can anyone send me a PDF version at eng.sheroukelarabi@gmail.com

upvoted 1 times

✉️ **Coletas** 3 weeks, 5 days ago

Please ask for free elsewhere. Don't breathe misery in this community!

upvoted 1 times

✉️ **shavit** 1 month ago

if someone can send me the full pdf plus discussion, i'll be gratefull, (im a solider so dont have money to buy this from you), kanadada03@gmail.com

upvoted 1 times

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, 1 month 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 46 times

✉  **BoboChow** 1 year, 1 month ago

I agree C is the answer

upvoted 2 times

✉  **tt79** 1 year, 1 month ago

C is right.

upvoted 1 times

✉  **PhucVuu**  8 months 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 29 times

✉  **Genlor**  5 days, 15 hours ago

Selected Answer: C

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

upvoted 1 times

✉  **Ruffyit** 1 week, 5 days 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** 1 month 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

✉  **AntoMonti** 1 month 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 2 times

 **dumpsfactory_com** 1 month, 1 week ago

Selected Answer: C

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

upvoted 1 times

 **pedrogaf** 1 month, 2 weeks ago

Selected Answer: C

Simple and fast

upvoted 1 times

 **Abitek007** 2 months ago

serverless operation simply

upvoted 1 times

 **thanhnv** 3 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

 **Theocode** 3 months, 3 weeks ago

Selected Answer: C

A no-brainer, Athena can be used to query data directly from s3

upvoted 1 times

 **sandhyaeiji** 3 months, 3 weeks ago

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

 **TariqKipkemei** 4 months ago

Selected Answer: C

Amazon Athena is a serverless, interactive analytics service used to query data in relational, nonrelational, object, and custom data sources running on S3.

upvoted 1 times

 **Guru4Cloud** 4 months, 2 weeks ago

Selected Answer: C

Explanation:

Option C is the most suitable choice for this scenario. Amazon Athena is a serverless query service that allows you to analyze data directly from Amazon S3 using standard SQL queries. Since the log files are already stored in JSON format in an S3 bucket, there is no need for data transformation or loading into another service. Athena can directly query the JSON logs without the need for any additional infrastructure.

upvoted 3 times

 **james2033** 4 months, 2 weeks ago

Selected Answer: C

I remember question and answer in an easy way with case study <https://www.youtube.com/watch?v=Dmw7HOOmJQ>

upvoted 1 times

 **miki111** 4 months, 2 weeks ago

Best option is CCCC

upvoted 1 times

 **animefan1** 4 months, 4 weeks ago

Selected Answer: C

athena is great for querying data in s3

upvoted 1 times

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*

A (95%)	5%
---------	----

 ude Highly Voted 1 year, 1 month 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 46 times

 BoboChow 1 year, 1 month ago

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

upvoted 14 times

 Naneyerocky Highly Voted 1 year 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 15 times

 Sleepy_Lazy_Coder 3 months, 2 weeks ago

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

upvoted 2 times

 BlackMamba_4 3 months ago

Exactly

upvoted 1 times

 Ruffyit Most Recent 1 week, 5 days 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 1 times

 Ruffyit 1 month ago

Answer: A

upvoted 1 times

 dumpsfactory_com 1 month, 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** 4 months, 2 weeks 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 2 times

 **james2033** 4 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/cWW0xAiWwc?t=677> at 11:17 use "aws:PrincipalOrgId": "o-fr75jjs531".

upvoted 3 times

 **miki111** 4 months, 2 weeks ago

Option A MET THE REQUIREMENT

upvoted 1 times

 **cookieMr** 5 months, 2 weeks 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** 5 months, 2 weeks ago

A is the correct answer.

upvoted 1 times

 **Musti35** 7 months, 3 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** 7 months, 4 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 8 times

 **linux_admin** 8 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** 8 months, 1 week 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

 **iamRohanKaushik** 8 months, 1 week ago

Selected Answer: A

Answer is A.

upvoted 1 times

 **buiducvu** 9 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **SilentMilli** 10 months, 3 weeks ago

Selected Answer: A

This is the least operationally overhead solution because it requires only a single configuration change to the S3 bucket policy, which will allow access to the bucket for all users within the organization. The other options require ongoing management and maintenance. Option B requires the creation and maintenance of organizational units for each department. Option C requires monitoring of specific CloudTrail events and updates to the S3 bucket policy based on those events. Option D requires the creation and maintenance of tags for each user that needs access to the bucket.

upvoted 1 times

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%)

 **D2w** Highly Voted 1 year, 1 month ago

Selected Answer: A

VPC endpoint allows you to connect to AWS services using a private network instead of using the public Internet
upvoted 29 times

 **PhucVuu** Highly Voted 7 months, 4 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 27 times

 **Ruffyit** Most Recent 1 week, 5 days ago

VPC endpoint allows you to connect to AWS services using a private network instead of using the public Internet
upvoted 1 times

 **Ruffyit** 1 month 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 1 times

 **dumpsfactory_com** 1 month, 1 week ago

Selected Answer: A

Create a gateway VPC endpoint to the S3 bucket
upvoted 1 times

 **namtp** 1 month, 2 weeks ago

Selected Answer: A

Create VPC endpoint is a private way to connect to AWS services without internet.
upvoted 1 times

 **RNess** 2 months, 3 weeks ago

Selected Answer: A

VPC endpoint is the best way to connect in private
upvoted 1 times

 **Bmarodi** 3 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** 4 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** 4 months, 2 weeks 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

 **james2033** 4 months, 2 weeks ago

Selected Answer: A

Keyword (1) EC2 in a VPC. (2)EC2 instance need access S3 bucket WITHOUT internet. Therefore, A is correct answer: Create a gateway VPC endpoint to S3 bucket.

upvoted 1 times

 **miki111** 4 months, 2 weeks ago

Option A MET THE REQUIREMENT

upvoted 1 times

 **cookieMr** 5 months, 2 weeks ago

Selected Answer: A

Here's why Option A is the correct choice:

Gateway VPC Endpoint: A gateway VPC endpoint allows you to privately connect your VPC to supported AWS services. By creating a gateway VPC endpoint for S3, you can establish a private connection between your VPC and the S3 service without requiring internet connectivity.

Private network connectivity: The gateway VPC endpoint for S3 enables your EC2 instance within the VPC to access the S3 bucket over the private network, ensuring secure and direct communication between the EC2 instance and S3.

No internet connectivity required: Since the requirement is to access the S3 bucket without internet connectivity, the gateway VPC endpoint provides a private and direct connection to S3 without needing to route traffic through the internet.

Minimal operational complexity: Setting up a gateway VPC endpoint is a straightforward process. It involves creating the endpoint and configuring the appropriate routing in the VPC. This solution minimizes operational complexity while providing the required private network connectivity.

upvoted 2 times

 **Bmarodi** 6 months ago

Selected Answer: A

A is right answer.

upvoted 1 times

 **cheese929** 6 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **channn** 8 months ago

Selected Answer: A

Option B) not provide private network connectivity to S3.

Option C) not provide private network connectivity to S3.

Option D) API Gateway with a private link provide private network connectivity between a VPC and an HTTP(S) endpoint, not S3.

upvoted 2 times

 **linux_admin** 8 months ago

Selected Answer: A

Option A proposes creating a VPC endpoint for Amazon S3. A VPC endpoint enables private connectivity between the VPC and S3 without using an internet gateway or NAT device. This would provide the EC2 instance with private network connectivity to the S3 bucket.

upvoted 2 times

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** Highly Voted 1 year, 1 month ago

Selected Answer: C

Concurrent or at the same time key word for EFS
upvoted 32 times

 **mikey2000** Highly Voted 1 year ago

Ebs doesnt support cross az only reside in one Az but Efs does, that why it's c
upvoted 21 times

 **pbpally** 6 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 5 times

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

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#efs-regional-ec2>
upvoted 1 times

 **Hayden001** 3 weeks, 1 day ago

Proposed = new service = EFS
upvoted 1 times

 **Ruffyit** 1 month 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

 **dumpsfactory_com** 1 month, 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** 1 month, 2 weeks ago

C is correct
upvoted 1 times

 **mattuyghur** 1 month, 3 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** 1 day, 17 hours 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** 2 months, 3 weeks ago

Selected Answer: C

EFS is to muliple AZ

upvoted 1 times

✉ **TariqKipkemei** 4 months ago

Selected Answer: C

Shared file storage = EFS

upvoted 1 times

✉ **Guru4Cloud** 4 months, 2 weeks ago

Selected Answer: C

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

The current architecture is using two separate EBS volumes, one for each EC2 instance. This means that each instance only has a subset of the documents. When a user refreshes the website, the Application Load Balancer will randomly direct them to one of the two instances. If the user's documents are not on the instance that they are directed to, they will not be able to see them.

upvoted 2 times

✉ **james2033** 4 months, 2 weeks ago

Selected Answer: C

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.

Solution: Amazon Elastic File System, see <https://aws.amazon.com/efs/> . "Amazon EFS file system creation, mounting, and settings" <https://www.youtube.com/watch?v=Aux37Nwe5nc> . "Amazon EFS overview" <https://www.youtube.com/watch?v=vAV4ASDnbN0> .

upvoted 1 times

✉ **miki111** 4 months, 2 weeks ago

Option C MET THE REQUIREMENT

upvoted 1 times

✉ **FroZor** 4 months, 3 weeks ago

They could use Sicky sessions with EBS, if they don't want to use EFS

upvoted 1 times

✉ **datmd77** 2 months, 3 weeks ago

no, they want to see both documents so must be EFS, not sticky sessions.

upvoted 1 times

✉ **capino** 4 months, 4 weeks ago

EFS Reduces latency and all user can see all files at once

upvoted 1 times

✉ **cookieMr** 5 months, 2 weeks ago

Selected Answer: C

To ensure users can see all their documents at once in the duplicated architecture with multiple EC2 instances and EBS volumes behind an Application Load Balancer, the most appropriate solution is Option C: Copy the data from both EBS volumes to Amazon EFS (Elastic File System) and modify the application to save new documents to Amazon EFS.

In summary, Option C, which involves copying the data to Amazon EFS and modifying the application to use Amazon EFS for document storage, is the most appropriate solution to ensure users can see all their documents at once in the duplicated architecture. Amazon EFS provides scalability, availability, and shared access, allowing both EC2 instances to access and synchronize the documents seamlessly.

upvoted 4 times

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

fffkfkffkfkf

upvoted 1 times

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 (82%)

Other

 **Gatt** Highly Voted 1 year, 1 month 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 specific 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 64 times

 **th3cookie** 1 year, 1 month ago

The company must transfer the data asap. Direct connect takes a month to setup doesn't it?

upvoted 5 times

 **Gatt** 1 year ago

That's a good point, indeed, DA might take weeks to establish (depending on your local ISP). And the question does not state that DA has already been established for this company. If they are starting fresh, then certainly DA would be taking too long.

upvoted 2 times

 **LuckyAro** 10 months, 3 weeks ago

But it said "as soon as possible" It takes about 4-6 weeks to provision a direct connect.

upvoted 12 times

 **Uncolored8034** 7 months, 4 weeks ago

This calculation is out of the scope.

C is right because the company wants to use the LEAST POSSIBLE NETWORK BANDWIDTH. Therefore they don't want or can't use the snowball capabilities of having a such fast connection because it draws too much bandwidth within their company.

upvoted 9 times

 **[Removed]** 6 months ago

NFS is using bandwidth within their company, so that logic does not apply.

upvoted 2 times

 **tribagus6** 5 months, 4 weeks ago

yeah first company use NFS file to store the data right then the company want to move to S3. with endpoint we dont need public connectivity
upvoted 2 times

✉ **darn** 7 months, 1 week ago

you are out of scope
upvoted 6 times

✉ **Help2023** 9 months, 2 weeks ago

D is a viable solution but to setup D it can take weeks or months and the question does say as soon as possible.
upvoted 4 times

✉ **debolek** 2 weeks, 6 days ago

but they said as soon as possible
upvoted 1 times

✉ **tuloveu** Highly Voted 1 year, 1 month ago

Selected Answer: B

As using the least possible network bandwidth.
upvoted 31 times

✉ **ssz123** Most Recent 1 week, 3 days ago

Selected Answer: B

It's a one-time migration so setting up direct connect doesn't make sense. I think it's B - the Snowball Edge device.
upvoted 1 times

✉ **lorenziello15** 2 weeks, 3 days ago

Selected Answer: B

"as soon as possible" + "least possible network bandwidth" = Snowball Edge
upvoted 1 times

✉ **brk_ravi** 3 weeks, 5 days ago

question contains "while using the least possible network bandwidth" so answer B is right
upvoted 1 times

✉ **Rsmastermind** 1 month ago

Selected Answer: D

From architecture point of view, I would recommend option D. The main reason is architecture is not about whether ISP can establish the connection in a day or months. But, if there is a connectivity that can be provided by a an ISP then that is the fastest option. If the answer is ISP will take greater than a week then yes the option C is second best option.

This question to me is not architecture oriented rather procurement and sourcing.
upvoted 2 times

✉ **Ruffyit** 1 month ago

Correct answer is C. The key words are NFS, S3 and low bandwidth. S3 File Gateway retains access through NFS protocol so that existing users don't have to change anything while being able to use S3 to store the files. The question also gives a clue that we only need to upload existing 70TB and no new data is added. This gives a clue that users only need to read data via NFS and don't need to write to S3 bucket. The existing data can be quickly uploaded (via endpoint) to S3 bucket by admin.
upvoted 2 times

✉ **dumpsfactory_com** 1 month, 1 week ago

Selected Answer: 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
upvoted 1 times

✉ **jasm33t** 1 month, 1 week ago

Selected Answer: B

It's a one-time transfer where data is no longer growing. Since internet bandwidth cannot be used, using Snowball device is the best way.
upvoted 1 times

✉ **Wayne23Fang** 1 month, 3 weeks ago

Selected Answer: C

Gatt's calculation below seems not right. 70TB = 70000 GB. Assume 1gbps, then it would need 70000 seconds, convert to day: $70000/60/60/24 = 0.81$ day.
upvoted 1 times

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

Actually Gatt's calculation is right. This is 1gbps (bits per second) not 1GBps (bytes per second), hence it'll be $70*1000*8/60/60/24 = 6.5$ days. So B.
upvoted 1 times

✉ **vbalakumar** 1 month, 3 weeks ago

Selected Answer: 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.

upvoted 1 times

 **Zelda28** 1 month, 3 weeks ago

B. Snowball edge would use 0 bandwidth in my opinion, you simply install the snowball client/AWS OpsHub on the servers and copy the files into the device. Then, its shipped back to AWS facility and placed into S3. So I don't get it why people are choosing option C.

upvoted 1 times

 **zk1200** 1 month, 3 weeks ago

Selected Answer: B

A snowball edge device will use no bandwidth at all.

upvoted 1 times

 **Abitek007** 1 month, 4 weeks ago

Selected Answer: C

because that is the fastest way to achieve this

upvoted 1 times

 **awashenko** 1 month, 4 weeks ago

Selected Answer: B

B is the easiest and least resource intensive

upvoted 1 times

 **debolek** 2 months ago

Selected Answer: B

option B is the most efficient and least resource-intensive solution for migrating large video files to Amazon S3 in a timely manner

upvoted 1 times

 **Yonimoni** 2 months, 3 weeks ago

Selected Answer: C

while using the least possible network bandwidth
they want to do it over the internet

upvoted 4 times

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

D (79%)	A (17%)	3%
---------	---------	----

 **rein_chau**  1 year, 1 month ago

Selected Answer: D

D makes more sense to me.
upvoted 41 times

 **SilentMilli** 10 months, 3 weeks 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 8 times

 **Abdel42** 10 months, 3 weeks 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 14 times

 **daizy** 10 months 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 8 times

 **9014** 12 months ago

of course, the answer is D
upvoted 3 times

 **Bevemo**  1 year 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 18 times

 **Rsmastermind**  1 month ago

The right answer to me is D as the SNS and SQS usage to decouple and set the scaling policy based on the messages in SQS will deal with the type of problem mentioned.

The answer cannot be A as Kinesis service is for real time data streaming and specially the kinesis data analytics is used for below cases and the problem is unrelated to any of the below used case.

Generate time-series analytics
Feed real-time dashboards
Create real-time metrics

upvoted 1 times

 **Ruffyit** 1 month ago

D. Here's why option D is the correct choice:

Amazon SNS: Amazon SNS is a fully managed pub/sub messaging service that enables message publishing and subscription to topics. It provides fast and flexible communication between publishers and subscribers.

Amazon SQS: Amazon SQS is a fully managed message queuing service that decouples the components of a distributed application. It offers reliable and scalable queues for storing messages and enables applications to process them asynchronously.

By publishing the messages to an Amazon SNS topic and using Amazon SQS subscriptions, the solution achieves decoupling and scalability. Multiple applications and microservices can subscribe to the topic and receive messages through their individual SQS queues. This allows for parallel processing and enables the system to handle varying message volumes, including spikes of up to 100,000 messages per second.

upvoted 2 times

 **dumpsfactory_com** 1 month, 1 week ago

Selected Answer: 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

upvoted 4 times

 **rosstaylor** 1 month, 1 week ago

Selected Answer: D

d is proper answer

<https://www.pass4surexams.com/amazon/saa-c03-dumps.html>

upvoted 1 times

 **IdanAWS** 1 month, 2 weeks ago

Selected Answer: D

D. Here's why option D is the correct choice:

Amazon SNS: Amazon SNS is a fully managed pub/sub messaging service that enables message publishing and subscription to topics. It provides fast and flexible communication between publishers and subscribers.

Amazon SQS: Amazon SQS is a fully managed message queuing service that decouples the components of a distributed application. It offers reliable and scalable queues for storing messages and enables applications to process them asynchronously.

By publishing the messages to an Amazon SNS topic and using Amazon SQS subscriptions, the solution achieves decoupling and scalability. Multiple applications and microservices can subscribe to the topic and receive messages through their individual SQS queues. This allows for parallel processing and enables the system to handle varying message volumes, including spikes of up to 100,000 messages per second.

upvoted 2 times

 **Tralfalgarlaw** 1 month, 3 weeks ago

The correct is D

upvoted 1 times

 **Zelda28** 1 month, 3 weeks ago

Selected Answer: B

B aligns with the simpler approach and more dynamic as well which is suitable for longer run.

upvoted 1 times

 **Zelda28** 1 month, 3 weeks ago

Selected Answer: D

Allows multiple consumers to process the messages independently.

upvoted 1 times

 **hrushikeshrelekar** 2 months ago

Option D

Amazon SNS allows you to publish messages to a topic, which can then fan out those messages to multiple subscribers.

By using Amazon SQS as a subscriber to the SNS topic, you can handle the message load in a decoupled and scalable way. SQS can store messages until the consuming application is ready to process them, helping to smooth out the variance in message load.

This approach allows the company to effectively decouple the message producing applications from the consuming applications, and it can easily scale to handle the high load of messages.

The number of messages (100,000 each second) might require careful configuration and sharding of SQS queues or use of FIFO queues to ensure that they can handle the load.

Options A, B, and C have their own limitations:

upvoted 2 times

 **MOSHE** 2 months ago

Selected Answer: D

D is the right answer

upvoted 1 times

 **AshokBabu** 2 months, 2 weeks ago

My choice is D

The only reason A is chosen because of incoming message rate, which is 100000. I was referring the document. If it is standard topic or standard queue, they support unlimited throughput. So, incoming message rate can't be the criteria for choosing option A

upvoted 1 times

 **Chiquitabandita** 2 months, 4 weeks ago

the wording in the question leads me to think it is D.
upvoted 1 times

 **Syruis** 3 months, 1 week ago

Selected Answer: D
"(Amazon SOS)" should be "(Amazon SQS)" it blow my mind :/
upvoted 2 times

 **BillyBlunts** 3 months, 1 week ago

How are we to go into the test with such confusing answers....I agree as well that it should be D. However, I want to select the answer they say is right so I can pass the test. Everywhere I have looked including Quizlet who I think is pretty reliable, the answer is A. Would you guys say it is better to go with the answer they select, even though we majority agree it is a different answer?
upvoted 1 times

 **Stevey** 3 months, 4 weeks ago

D. is the answer.
The question states that there are dozens of other applications and microservices that consume these messages and that the volume of messages can vary drastically and increase suddenly. Therefore, you need a solution that can handle a high volume of messages, distribute them to multiple consumers, and scale quickly. SNS with SQS provides these capabilities.

Publishing messages to an SNS topic with multiple SQS subscriptions is a common AWS pattern for achieving both decoupling and scalability in message-driven systems. SNS allows messages to be fanned out to multiple subscribers, which in this case would be SQS queues. Each consumer application could then process messages from its SQS queue at its own pace, providing scalability and ensuring that all messages are processed by all consumer applications.

A. Amazon Kinesis Data Analytics is primarily used for real-time analysis of streaming data. It's not designed to distribute messages to multiple consumers.

upvoted 3 times

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%) 2%

✉  **rein_chau** Highly Voted 1 year, 1 month 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 68 times

✉  **Wilson_S** 1 year ago

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

✉  **Sinaneos** Highly Voted 1 year, 1 month 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

✉  **achechen** Most Recent 3 days, 14 hours ago

Selected Answer: B

B of course
upvoted 1 times

✉  **ssz123** 1 week, 3 days 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** 2 weeks, 6 days ago

Selected Answer: B

B is the right answer here.
upvoted 1 times

✉  **furkanx** 3 weeks, 2 days ago

Selected Answer: B

The answer seems to be B for me
upvoted 1 times

✉  **chrisExam** 4 weeks, 1 day ago

C. L'utilisation de AWS CloudTrail comme destination pour les tâches n'est pas adaptée à ce scénario. CloudTrail est conçu pour la surveillance et la journalisation des appels d'API dans un environnement AWS, et non comme un mécanisme de gestion de file d'attente.

B .L'utilisation d'Amazon SQS pour gérer les tâches est une bonne idée car elle découpe le producteur de tâches du consommateur, améliorant ainsi la résilience. Utiliser des instances Amazon EC2 dans un groupe Auto Scaling permet de gérer l'évolutivité des noeuds de calcul. non planifiée c.a.d elle ajuste le nombre d'instances EC2 en fonction de la taille de la file d'attente SQS maximisant ainsi l'évolutivité.

upvoted 1 times

✉ **dumpsfactory_com** 1 month, 1 week ago

Selected Answer: 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

✉ **rosstaylor** 1 month, 1 week ago

Selected Answer: B

B BECAUSE B is valid answer

<https://www.pass4surexams.com/amazon/saa-c03-dumps.html>

upvoted 1 times

✉ **debolek** 2 months ago

Option B provides the required scalability, resiliency, and dynamic workload handling that the company needs for its distributed application while maximizing efficiency and minimizing operational overhead

upvoted 1 times

✉ **MOSHE** 2 months ago

Selected Answer: B

Option B: This option provides a decoupled architecture where the jobs are sent to an SQS queue. The compute nodes (EC2 instances in an Auto Scaling group) can then process these jobs. Scaling based on the size of the SQS queue (the number of messages) allows the architecture to adapt to variable workloads, scaling out when the queue depth increases and scaling in when the depth decreases.

upvoted 1 times

✉ **joyce66** 2 months, 2 weeks ago

A and B are not correct. The question is about multiple nodes / distributed system. A and B use SQS which is a message driven solution. You don't know the system from the question is message driven or not. The answer is either C or D. I selected D. But after reading CloudTrail doc, C is correct. CloudTrail monitors actions, and CloudWatch monitoring resources. The system composes of multiple nodes which perform actions. From actions monitored/recorded, CloudTrail can trigger/notify next workload to action...

upvoted 4 times

✉ **krozmok** 2 months, 3 weeks ago

I think that B is correct, but considering that the questions mentions that they are only migrating but no redesigning its architecture, that could be a key word to go for C as correct. It does not scales like SQS, but it fullfill the requirements. And it is well known that no one should modify Legacy Code :v

upvoted 1 times

✉ **BillyBlunts** 3 months ago

Can anyone tell me what answers we are to pick on the test. This site is driving me crazy with not having matching answers, especially with ones like this where the answer they have really doesn't seem like the right one. I am hesitant to pick the actual correct answer because the dumps have wrong answers. Any help is appreciated.

upvoted 8 times

✉ **dwx101** 1 month, 3 weeks ago

learn AWS not just Q&A's.

upvoted 1 times

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

Using CloudTrail as a "target for jobs" doesn't make sense, as CloudTrail is designed to audit and log API events in an AWS environment, not to manage jobs in a distributed application.

upvoted 5 times

✉ **Teruteru** 3 months, 2 weeks ago

<Correct Answer> is saying the option C is the correct answer. But in the <Community vote distribution>, the option B(97%) is most voted. So, do I still need to consider the C is the correct answer? or should I consider the most voted is the correct one?
Sorry but I just confused.

upvoted 2 times

✉ **pKap1812** 3 months ago

I've gone through the first 290 questions, which are accessible for free, and I'm just doing a revision run. Trust me when I say that about 98% of the time, I have found no dissonance between the most voted answer and what answer I could derive from a few simple google searches, and the remaining 2% was because of ambiguity. So stick to the most voted ones, there's a much higher relative probability of them being accurate.

upvoted 8 times

✉ **niltriv98** 3 months, 2 weeks ago

I always consider the most voted answer to be correct and most of the time they explain as well why that option is correct.

upvoted 3 times

 **Jenny9063** 3 months, 2 weeks ago

I am new to this and I am confused. why is the voted answer different from the correct answer? what is the accuracy of the correct answer?
upvoted 1 times

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

B (84%) Other

 **Sinaneos** Highly Voted 1 year, 1 month 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 41 times

 **Udoyen** 12 months ago

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

upvoted 2 times

 **SuperDuperPooperScooper** 3 months, 2 weeks 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 1 times

 **Nava702** 3 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

 **javitech83** Highly Voted 11 months, 4 weeks 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

 **nathanss** Most Recent 2 weeks, 6 days ago

Selected Answer: B

B is the correct answer again here. Why dont the moderator give some reasoning for the community's Most Voted answer a proper review and correct themselves or provide better reasoning ? Whoever agrees please upvote this.Thanks

upvoted 5 times

 **pabloveintimilla** 3 weeks, 3 days ago

Selected Answer: B

With File gateway can apply lifecycles

upvoted 1 times

 **chrisExam** 4 weeks, 1 day ago

Selected Answer: B

D. Installer un utilitaire sur chaque ordinateur de l'utilisateur n'est pas une solution évolutive et peut entraîner des problèmes de gestion et de compatibilité.bien que S3 Glacier Flexible Retrieval puisse être une option valable pour le stockage à long terme, cette solution ne prend pas en compte l'accès à faible latence aux fichiers les plus récents ou la gestion automatique du cycle de vie.

Parmi ces options, la meilleure solution qui répond aux exigences est :

B.

upvoted 1 times

✉️ **dumpsfactory_com** 1 month, 1 week ago

Selected Answer: D

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

upvoted 1 times

✉️ **Emanv** 1 month, 3 weeks ago

why the website always choose the wrong answer -__-

upvoted 2 times

✉️ **dadymanu** 1 day, 23 hours ago

I have seen a lot, I am not sure if their dumps are not choosing the wrong answer also

upvoted 1 times

✉️ **lowkey07** 2 months ago

Installing a utility on each user computer is a MANUAL process. AWS will always favor an AUTOMATED process over a manual process. the correct answer is B.

upvoted 1 times

✉️ **cris93** 23 hours, 34 minutes ago

about automated processes you are right, but filegateway is used for migrations! there is no reference or keyword here that refers to a migration

upvoted 1 times

✉️ **MOSHE** 2 months ago

Selected Answer: B

option B: Amazon S3 File Gateway provides a hybrid cloud storage solution, integrating on-premises environments with cloud storage. Files written to the file share are automatically saved as S3 objects. With S3 Lifecycle policies, you can transition objects between storage classes. Transitioning to Glacier Deep Archive is suitable for rarely accessed files. This solution addresses both the storage capacity and lifecycle management requirements.

upvoted 3 times

✉️ **pakut2** 2 months, 1 week ago

Selected Answer: A

A is the only answer meeting the requirements. B and D are incorrect, since minimum storage duration needed for an object to be moved into Glacier is 90 days, not 7 <https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html#sc-compare>. C does not provide lifecycle management, which is a part of the requirements

upvoted 2 times

✉️ **pakut2** 2 months, 1 week ago

I was wrong. Turns out you are able to transition from standard to Glacier after just 7 days. I can't find it explicitly stated anywhere, but it works in the console. My confusion is from the `minimum storage duration` metric. As I understand it now, you are able to delete/move objects before minimum storage duration is exceeded, but you pay for the entire period nonetheless. So it's doable, but not cost effective. Anyway, it does not apply here since S3 Standard storage class does not have a minimum storage duration constraint. So, I would go with B. Both B and D achieve the same thing, but B is way simpler to setup and maintain

upvoted 4 times

✉️ **LR2023** 2 months, 1 week ago

Selected Answer: A

<https://aws.amazon.com/about-aws/whats-new/2019/08/aws-datasync-can-now-transfer-data-to-and-from-smb-files-shares/>

we cannot move objects to S3 glacier within 7 days

upvoted 2 times

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

D Correct answer.

keywords->low-latency is required for the most recently accessed files which will be from glacier having low latency utility will run as from multiple systems connected to SMB server to do the transfer.

upvoted 1 times

✉️ **dbs6339** 2 months, 2 weeks ago

Selected Answer: D

Exactly, what we need to focus on that is increase the company's available storage space not total storage space with not losing the low-latency access.

Answer D is the more exact.

B/D both answers can be made more available storage space after 7 days sent to the S3 glacier but B will lose access about most recently accessed files with the low-latency access.

upvoted 1 times

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

Selected Answer: B

B answer is correct

upvoted 1 times

 **BillyBlunts** 3 months, 1 week ago

Can anyone tell me what the test is going to use as the correct answer? I don't want to go into the test and just answer the ones that majority voted for but really they don't have it as the right answer. BTW the discussions are awesome and helps you learn a lot from other peoples intellect.

upvoted 3 times

 **Fresbie99** 3 months, 2 weeks ago

Acc to the question we need lifecycle policy and file gateway - Also the S3 flexible retrieval is not required here, Deep archive is the solution. hence B is correct

upvoted 1 times

 **McLobster** 4 months ago

Selected Answer: A

according to documentation the minimum storage timeframe for an object inside S3 before being able to transition using lifecycle policy is 30 days , so those 7 days policies kinda seem wrong to me

Transition actions – These actions define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after creating them, or archive objects to the S3 Glacier Flexible Retrieval storage class one year after creating them. For more information, see Using Amazon S3 storage classes.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html>

I was thinking of option A using DataSync as a scheduled task? am i wrong here?

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

upvoted 1 times

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** Highly Voted 1 year, 1 month ago**Selected Answer: B**

B because FIFO is made for that specific purpose
upvoted 50 times

  **rein_chau** Highly Voted 1 year, 1 month ago**Selected Answer: B**

Should be B because SQS FIFO queue guarantees message order.
upvoted 23 times

  **achechen** Most Recent 3 days, 14 hours ago**Selected Answer: B**

B because of FIFO.
upvoted 1 times

  **nathanss** 2 weeks, 6 days ago**Selected Answer: B**

B again
upvoted 1 times

  **ifaby** 3 weeks, 1 day ago**Selected Answer: A**

It's A because the option B is wrong, SQS never invoke nothing, it's Lambda who reads the messages.
upvoted 1 times

  **dodino** 1 week, 5 days ago

wrong:

https://docs.aws.amazon.com/lambda/latest/dg/example_serverless_SQS_Lambda_section.html
upvoted 1 times

  **jors1116** 3 weeks, 2 days ago**Selected Answer: B**

Keyword is FIFO
upvoted 1 times

  **chry900** 3 weeks, 5 days ago**Selected Answer: B**

b. SQS fifo
upvoted 1 times

  **Ruffyit** 1 month ago

b. SQS fifo is made for first in first out
upvoted 1 times

  **lorrangarcia** 1 month ago

Selected Answer: B

B, devido ao uso do SQS
upvoted 1 times

 **dumpsfactory_com** 1 month, 1 week ago

Selected Answer: 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.
upvoted 1 times

 **jasm33t** 1 month, 1 week ago

Selected Answer: B

in order = SQS FIFO
upvoted 1 times

 **vishal08** 1 month, 1 week ago

Selected Answer: B

can any1 say what is right answer? and how its A?
upvoted 1 times

 **bhavin042** 1 month, 3 weeks ago

Selected Answer: B

I think B is the correct answer, keyword FIFO to process orders in correct order.
upvoted 1 times

 **avrk** 1 month, 3 weeks ago

For most of the questions there is correct answer and votes given by group. Which one is the correct answer to consider as i am getting confused.
who has given correct answer?
upvoted 2 times

 **dhax12** 1 month, 2 weeks ago

It's literally B if you have studied AWS
upvoted 1 times

 **bhavin042** 1 month, 3 weeks ago

Yes, this is very confusing. What is the correct answer ?
upvoted 1 times

 **Zelda28** 1 month, 3 weeks ago

Selected Answer: B

Invoking lambda function is the right way, if we use standard, the orders would not be processed in the correct order. FIFO would give the correct order...
upvoted 1 times

 **AWSGuru123** 2 months ago

Selected Answer: B

FIFO queue suits best
upvoted 1 times

 **praveenkumar2** 2 months, 1 week ago

I vote for Option B, When the question says about orderblindly go for SQS FIFO
upvoted 1 times

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

A (95%)	4%
---------	----

 **Sinaneos** Highly Voted 1 year, 1 month 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 72 times

 **17Master** 1 year, 1 month 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/blogs/security/how-to-connect-to-aws-secrets-manager-service-within-a-virtual-private-cloud/>
https://aws.amazon.com/secrets-manager/?nc1=h_ls
upvoted 20 times

 **HarishArul** 6 months, 1 week ago

Read this - https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_parameterstore.html
It says SSM Parameter store cant rotate automatically.
upvoted 4 times

 **kewl** 12 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 14 times

 **mrbottomwood** 11 months, 3 weeks ago

That was a fantastic link. This part of their site "comparison of AWS services" is superb. Thanks.
upvoted 5 times

 **iCcma** 1 year, 1 month ago

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

 **leeyoung** Highly Voted 11 months ago

Admin is trying to fail everybody in the exam.
upvoted 56 times

 **perception** 7 months ago

He wants you to read discussion part as well for better understanding
upvoted 2 times

 **acuaws** 8 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

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

Selected Answer: B

B becasue the user wants reduce costs and SSM Parameter Store layer Standard is free and the type SecureString uses KMS
upvoted 2 times

 **Ruffyit** 1 month 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/> y
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 1 times

 **AbirAbu** 1 month, 2 weeks ago

It should be "A."

upvoted 2 times

 **santbot** 1 month, 4 weeks ago

Selected Answer: A
A - SECRETS MANAGER

upvoted 1 times

 **Mandar15** 1 month, 4 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 2 times

 **NaaVeeN** 1 month, 4 weeks ago

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

upvoted 3 times

 **novice16** 2 months ago

Selected Answer: A
Secret manager and auto rotation does the job
upvoted 1 times

 **Shaansd** 2 months, 1 week ago

can anyone please share the pdf to my email sstanudas@gmail.com
upvoted 1 times

 **praveenkumar2** 2 months, 1 week ago

I vote for A. If its something to deal with credentials and rotation. Only Secret Manager does the Job.
upvoted 1 times

 **sanjay_cloud_guy** 2 months, 1 week ago

A is correct answer. user name and password these are secrets so to be stored in secret manager.
upvoted 1 times

 **Blackberry** 2 months, 2 weeks ago

Can admit update only  answers. It's confusing most voted or correct answer which to prefer
upvoted 1 times

 **cyber_bedouin** 2 months, 2 weeks ago

most voted
upvoted 1 times

 **akshunn** 2 months, 3 weeks ago

Selected Answer: A
A it is
upvoted 1 times

 **MakaylaLearns** 2 months, 3 weeks ago

I meant to say WHY B at the end!
So I think A is the answer, here is a little video I made
<https://youtube.com/shorts/njodSsIsqOs?feature=share>
upvoted 2 times

 **Hassao0** 3 months ago

A is Right Because secret manager is meant for Rds Integration
upvoted 1 times

 **PLN6302** 3 months, 1 week ago

Option A
upvoted 1 times

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 (76%)

C (24%)

✉️  **Kartikey140**  1 year 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 73 times

✉️  **daizy** 10 months 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 6 times

✉️  **kanweng**  1 year 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 25 times

✉️  **theonlyhero**  2 weeks, 5 days ago

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

upvoted 3 times

✉️  **Ruffyit** 1 month 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 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 1 times

✉ **gldiazcardenas** 1 month, 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

✉ **danielpark99** 1 month, 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** 2 months 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

✉ **aropl** 2 months ago

A is correct, other answers have wrong origin or endpoint types.

Cloudfront supports multiple origins on the same distribution (ALB and S3) in our case.

B incorrect - Global Accelerator Standard accelerator doesn't support s3 endpoints

C incorrect - Global Accelerator Standard accelerator doesn't support CloudFront distribution as endpoint

D incorrect - Global Accelerator Standard accelerator doesn't support s3 endpoints

upvoted 4 times

✉ **MOSHE** 2 months ago

Selected Answer: A

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.

Here's the reasoning:

CloudFront with Multiple Origins: CloudFront allows you to set up multiple origins for your distribution, so you can use both the ALB (for dynamic content) and the S3 bucket (for static content) as origins. This means that both your dynamic and static content can be served through CloudFront, which will cache content at edge locations to reduce latency.

Route 53 Integration with CloudFront: Amazon Route 53 can be easily configured to route traffic for your domain to a CloudFront distribution.

Users will access your domain, and Route 53 will direct them to the nearest CloudFront edge location.

upvoted 1 times

✉ **David_Ang** 2 months ago

I did some research and "a" is correct but "c" is also correct. the thing is that "a" is more simple than c and the fact that does not use global accelerator makes it cheaper so is more correct

upvoted 1 times

✉ **gsax** 2 months, 3 weeks ago

Selected Answer: A

A - Simple solution, CloudFront itself is enough to reduce latency and improve performance. And it can use both as origins S3 and ALB.

A - Simple solution, CloudFront itself is enough to reduce latency and network

<https://repost.aws/knowledge-center/cloudfront-distribution-serve-content>

network

<https://repost.aws/knowledge-center/cloudfront-distribution-serve-content>

upvoted 1 times

✉ **Santku** 2 months, 3 weeks ago

The answer should be C

Considering the fact that to access dynamic content hosted by heterogeneous providers that are supported by AWS Global Accelerator as compared to CloudFront

Please refer following link to compare AWS Global Accelerator vs CloudFront

<https://www.techtarget.com/searchcloudcomputing/tip/Compare-AWS-Global-Accelerator-vs-Amazon-CloudFront>

upvoted 2 times

✉ **Santku** 2 months, 3 weeks ago

Also for dynamic content the caching is not recommended, which is CloudFront behavior
upvoted 1 times

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

What is the correct answer for the exam?

upvoted 1 times

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

I have been asking this on many questions because it is confusing that majority of people are disagreeing with what this dump and the 3 other dumps have as the answer. Yet the arguments for why they are wrong are very good and some prove right...but f'in aye...what is the answer we need to pick for the test.

upvoted 1 times

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

I think I am just going with the answers provided by exam topics....that is probably the safer bet.

upvoted 1 times

✉  **Tunde0** 2 months, 1 week ago

Answer to this is A

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

upvoted 3 times

✉  **AAAWreknG** 1 month, 2 weeks ago

Thank you, that appears to have the exact answer on it.

upvoted 1 times

✉  **Lorenzo1** 3 months, 4 weeks ago

Selected Answer: A

The answer A fulfills the requirements, so I would choose A.
The answer C may also seem to make sense though.

upvoted 1 times

✉  **gurmit** 4 months ago

A.

<https://stackoverflow.com/questions/71064028/aws-cloudfront-in-front-of-s3-and-alb>

upvoted 1 times

✉  **TariqKipkemei** 4 months ago

Selected Answer: A

Improve performance and reduce latency for the static data and dynamic data = Amazon CloudFront
upvoted 1 times

✉  **Lx016** 3 months, 2 weeks ago

And? All four answers are about CloudFront, to find the correct answer need to find correct origin(s) to distribute which are S3 and ALB

upvoted 1 times

✉  **hakim1977** 4 months, 1 week ago

Selected Answer: A

Answer is A.

Global Accelerator is a good fit for non-HTTP use cases.

upvoted 1 times

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, 1 month ago

Selected Answer: A

A is correct.

<https://aws.amazon.com/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/>
upvoted 19 times

✉️  **PhucVuu**  7 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 6 times

✉️  **Ruffyit**  1 month ago

<https://aws.amazon.com/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/> A is answer
upvoted 1 times

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

Selected Answer: A

Clearly A is the correct one.

upvoted 1 times

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

Option A MET THE REQUIREMENT

upvoted 1 times

✉  **cookieMr** 5 months, 2 weeks 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** 6 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

✉  **Musti35** 7 months, 3 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** 8 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** 9 months, 1 week ago

Selected Answer: A

A is correct.

upvoted 1 times

✉  **BlueVolcano1** 10 months, 2 weeks 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** 10 months, 3 weeks ago

Selected Answer: A

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

upvoted 2 times

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

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

upvoted 1 times

✉  **SilentMilli** 10 months, 3 weeks 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

✉  **Buruguduystunstugudunstuy** 11 months ago

Selected Answer: A

Option A, storing the credentials as secrets in AWS Secrets Manager and using multi-Region secret replication for the required Regions, and configuring Secrets Manager to rotate the secrets on a schedule, would meet the requirements with the least operational overhead.

AWS Secrets Manager allows you to store, manage, and rotate secrets, such as database credentials, across multiple AWS Regions. By enabling multi-Region secret replication, you can replicate the secrets across the required Regions to allow for seamless rotation of the credentials during maintenance activities. Additionally, Secrets Manager provides automatic rotation of secrets on a schedule, which would minimize the operational overhead of rotating the credentials on a monthly basis.

upvoted 2 times

 **Burugduystunstugudunstuy** 11 months ago

Option B, storing the credentials as secrets in AWS Systems Manager and using multi-Region secret replication, would not provide automatic rotation of secrets on a schedule.

Option C, storing the credentials in an S3 bucket with SSE enabled and using EventBridge to invoke an AWS Lambda function to rotate the credentials, would not provide automatic rotation of secrets on a schedule.

Option D, encrypting the credentials as secrets using KMS multi-Region customer managed keys and storing the secrets in a DynamoDB global table, would not provide automatic rotation of secrets on a schedule and would require additional operational overhead to retrieve the secrets from DynamoDB and use the RDS API to rotate the secrets.

upvoted 2 times

 **Zerotn3** 11 months, 1 week ago

vote A !

upvoted 1 times

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, 1 month 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 31 times

 **Buruguduystunstugudunstuy**  11 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 12 times

 **Buruguduystunstugudunstuy** 11 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 4 times

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

Selected Answer: C

Aurora

upvoted 1 times

 **Syruis** 3 months, 2 weeks ago

Selected Answer: C

C fit perfectly

upvoted 1 times

 **TariqKipkemei** 4 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** 4 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** 4 months, 2 weeks ago

Option C MET THE REQUIREMENT

upvoted 1 times

✉ **hiepdz98** 5 months ago

Selected Answer: C

Option C

upvoted 1 times

✉ **cookieMr** 5 months, 2 weeks 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** 6 months ago

Selected Answer: C

C meets the requirements.

upvoted 1 times

✉ **Mehkay** 6 months ago

C Aurora with read replicas

upvoted 1 times

✉ **big0007** 6 months, 2 weeks ago

Key words:

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

upvoted 4 times

✉ **cheese929** 6 months, 2 weeks ago

Selected Answer: C

C is correct since cost is not a concern.

upvoted 1 times

✉ **Abrar2022** 6 months, 2 weeks ago

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

upvoted 2 times

✉ **Abrar2022** 6 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

✉ **PhucVuu** 7 months, 3 weeks ago

Selected Answer: C

Keywords:

- The database's performance degrades quickly as application load increases.
- The application handles more read requests than write transactions.
- Automatically scale the database to meet the demand of unpredictable read workloads
- Maintaining high availability.

A: Incorrect - Amazon Redshift is used columnar block storage which is useful for Data Analytics and warehousing.

It also has the issue when migrating from MySQL to Redshift: storage procedure, trigger,.. Single node for leader doesn't maintain high availability.

B: Incorrect - The requirement said that: "Automatically scale the database to meet the demand of unpredictable read workloads" -> missing auto scaling.

C: Correct - it's resolved the issue of high availability and auto scaling.

D: Incorrect - Stop instance doesn't maintain high availability.

upvoted 6 times

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

C (92%) 8%

 **SilentMilli** Highly Voted 10 months, 3 weeks 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 68 times

 **Clouddon** 3 months, 3 weeks ago

Thank you for this reply

upvoted 5 times

 **BoboChow** Highly Voted 1 year, 1 month 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, 1 month ago

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

upvoted 3 times

 **danielpark99** Most Recent 1 month, 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** 2 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

 **nmywrlid** 3 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

 **Syruis** 3 months, 2 weeks ago

Selected Answer: C

C with no doubt
upvoted 1 times

 **Guru4Cloud** 4 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** 4 months, 2 weeks ago

Option C MET THE REQUIREMENT
upvoted 1 times

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

B is correct answer
upvoted 2 times

 **mbuck2023** 5 months, 4 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** 6 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** 6 months, 2 weeks 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

 **siyokko** 6 months, 2 weeks ago

Selected Answer: B

Option B, using Traffic Mirroring, is the most appropriate solution. Traffic Mirroring allows you to capture and forward network traffic from an Amazon VPC to an inspection instance or service for analysis and filtering. By mirroring the traffic from the production VPC, you can send it to an inspection server or a dedicated service that performs the required traffic flow inspection and filtering, replicating the functionalities of the on-premises inspection server.

upvoted 3 times

 **mbuck2023** 5 months, 4 weeks ago

Yes, so says chatgpt

upvoted 1 times

 **cheese929** 6 months, 2 weeks ago

Selected Answer: C

C is correct
upvoted 1 times

 **Abrar2022** 6 months, 2 weeks ago

Network Firewall is for inspection and traffic filtering.
upvoted 1 times

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

B (80%)	11%	8%
---------	-----	----

✉  **rodriviru**  1 year, 1 month ago

Selected Answer: B

<https://docs.aws.amazon.com/quicksight/latest/user/sharing-a-dashboard.html>
upvoted 56 times

✉  **mattlai** 1 year, 1 month ago

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

✉  **BoboChow** 1 year, 1 month ago

Agree with you
upvoted 2 times

✉  **PhucVuu**  7 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 28 times

✉  **cris93**  22 hours, 58 minutes 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

✉  **Ndlesty** 1 week, 6 days ago

Selected Answer: B

QuickSight suports users (standard) and groups (Enterprise), no support for IAM.
Other keywords: VISUALIZATION

upvoted 1 times

 **aptx4869** 1 month ago

Selected Answer: B

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

upvoted 1 times

 **Ruffyit** 1 month 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** 1 month, 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** 1 month, 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** 2 months, 1 week 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 6 times

 **MakaylaLearns** 2 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** 3 months 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** 4 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

 **Guru4Cloud** 4 months, 1 week ago

Selected Answer: B

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

 **james2033** 4 months, 1 week ago

Selected Answer: B

Question keyword "data visualization". "company's management team have full access to all the visualizations, the rest should have only limited access."

Answer keyword "Amazon QuickSight", "share the dashboards with the appropriate users and groups". Choose B.
upvoted 1 times

 **miki111** 4 months, 2 weeks ago

Option B MET THE REQUIREMENT
upvoted 1 times

 **RupeC** 4 months, 3 weeks ago

Selected Answer: B

C and D are out as there is no inbuilt visualisation function in Glue. Thus A or B. As Quicksite shares with users and groups, the answer is B.

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

upvoted 1 times

 **Mia2009687** 5 months ago

Answer is B
Dashboard cannot be shared with roles.
<https://docs.aws.amazon.com/quicksight/latest/user/share-a-dashboard-grant-access-users.html>

upvoted 1 times

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** Highly Voted 1 year, 1 month ago

Selected Answer: A

Always remember that you should associate IAM roles to EC2 instances
upvoted 66 times

 **Buruguduystunstugudunstuy** Highly Voted 11 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 41 times

 **GabrielSGoncalves** Most Recent 4 weeks ago

Selected Answer: A

For sure
upvoted 1 times

 **Ruffyit** 1 month 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** 1 month, 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** 3 months, 3 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** 4 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** 4 months, 1 week ago

Selected Answer: A

IAM roles should be associated to EC2 instance

upvoted 2 times

 **miki111** 4 months, 2 weeks ago

Option A MET THE REQUIREMENT

upvoted 1 times

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

Selected Answer: A

A is correct

upvoted 1 times

 **zoblazo** 7 months, 2 weeks ago

Selected Answer: A

always role for ec2 instance

upvoted 1 times

 **PhucVuu** 7 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

 **thanhvx1** 7 months, 4 weeks ago

A is correct

upvoted 1 times

 **r1skkam** 8 months, 1 week ago

Selected Answer: A

<https://aws.amazon.com/blogs/security/writing-iam-policies-how-to-grant-access-to-an-amazon-s3-bucket/>

upvoted 1 times

 **gold4otas** 8 months, 2 weeks ago

Selected Answer: A

IAM Role is the correct answer.

upvoted 1 times

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%)

 **Burugduystunstugudunstuy** Highly Voted 11 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 20 times

 **Burugduystunstugudunstuy** 11 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 16 times

 **hsinchang** 4 months ago

So storing states invokes the stateless principle, nice understanding!

upvoted 2 times

 **op22233** 1 month, 3 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, 1 month ago

Selected Answer: AB

It looks like A-B

upvoted 15 times

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

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

upvoted 1 times

 **Nava702** 2 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** 4 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** 4 months, 2 weeks ago

Option AB MET THE REQUIREMENT

upvoted 1 times

 **RupeC** 4 months, 3 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** 4 months, 3 weeks ago

Selected Answer: AB

A and B are optimal solutions

upvoted 1 times

 **cookieMr** 5 months, 2 weeks 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 4 times

 **beginnercloud** 6 months, 2 weeks ago

Selected Answer: AB

Option A nad B

upvoted 1 times

 **cheese929** 6 months, 2 weeks ago

Selected Answer: AB

A and B

upvoted 1 times

 **PhucVuu** 7 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** 8 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

 **cheese929** 8 months, 3 weeks ago

Selected Answer: AB

Agree with the general answer. its A+B.

upvoted 1 times

 **Nikhilcy** 9 months ago

Why B?

Message gets automatically deleted from queue once it goes out of it. FIFO

upvoted 1 times

 **camelstrike** 8 months, 3 weeks ago

Not deleted but hidden while being processed

upvoted 1 times

 **bilel500** 9 months ago

Selected Answer: AB

AB definitely Okay

upvoted 1 times

 **buiducvu** 9 months, 2 weeks ago

Selected Answer: AB

AB definitely Okay

upvoted 1 times

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

D (79%)	A (16%)	5%
---------	---------	----

CloudGuru99 [Highly Voted] 1 year, 1 month 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 39 times

pm2229 [Highly Voted] 1 year 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 34 times

leosmal [Most Recent] 1 week, 1 day ago

Selected Answer: D

Gateway load balancer is the answer

upvoted 1 times

Ruffyit 1 month 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 1 month ago

D. GAteway load balancer

upvoted 1 times

rlamberti 1 month, 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 1 month, 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 2 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** 2 months, 1 week ago

Selected Answer: D

Answer is D . Use Gateway Load balancer
upvoted 1 times

 **Meytiam** 3 months ago

Selected Answer: A

Given the straightforward nature of the requirement—inspecting all traffic before it reaches the web servers—the more suitable and operationally efficient solution would be to use a Network Load Balancer (Option A). NLB operates at the transport layer (Layer 4) and can route packets to the third-party firewall appliance with minimal complexity and overhead.

so its not B

and about D it mentioned with least operational overhead

upvoted 2 times

 **slackbot** 3 months, 2 weeks ago

Selected Answer: A

Option D is irrelevant - you are adding complexity when it is not needed. 3rd party appliances do not require GWLB when there is a SINGLE appliance. GWLB is used when there are multiple appliances (which was not mentioned).

NLB (working on layer 4) will forward the TCP traffic to the target (firewall in inspection VPC) which will route the traffic to the web tier.

upvoted 2 times

 **TariqKipkemei** 4 months ago

Selected Answer: D

Gateway Load Balancer for layer 3 ip traffic distribution across EC2 and ip address - it is used for routing traffic to 3rd party virtual appliances e.g. firewall, packet inspection systems before routing to destination apps on aws.

upvoted 1 times

 **Bogs123456711** 4 months ago

Selected Answer: D

Key word "Third party FW"

Gateway Load Balancers make it easy to deploy, scale, and manage third-party virtual appliances, such as security appliances.

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

upvoted 2 times

 **hsinchang** 4 months ago

So basically Gateway Load Balancer is the only LB that comes with inspection?

upvoted 1 times

 **Guru4Cloud** 4 months, 1 week ago

Selected Answer: D

The correct answer is D.

Here is the explanation:

Option D is correct because a Gateway Load Balancer (GWLB) is a global service, and it can be deployed in any VPC. This means that the GWLB can reach the appliance. Additionally, the GWLB can be configured to forward packets to the appliance for packet inspection.

Option A is incorrect because a Network Load Balancer (NLB) is a regional service, and the appliance is deployed in an inspection VPC. This means that the NLB would not be able to reach the appliance.

Option B is incorrect because an Application Load Balancer (ALB) is a regional service, and the appliance is deployed in an inspection VPC. This means that the ALB would not be able to reach the appliance.

Option C is incorrect because a transit gateway is a global service, and the appliance is deployed in an inspection VPC. This means that the transit gateway would not be able to reach the appliance.

upvoted 9 times

 **Undisputed** 4 months, 1 week ago

Selected Answer: D

The key word is Inspection, Gateway Load Balancer is a layer 3 used for inspection purposes.

upvoted 1 times

 **miki111** 4 months, 2 weeks ago

Option D is the ideal answer.

upvoted 1 times

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 (91%) 8%

 **UWSFish** Highly Voted 1 year, 1 month 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 26 times

 **PhucVuu** Highly Voted 7 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 11 times

 **Ruffyt** Most Recent 1 month 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

 **ukivanlamipi** 3 months, 2 weeks ago

Selected Answer: A

why not A? high I/O, no need durability

upvoted 1 times

 **JackLo** 2 months, 3 weeks ago

Although it is test environment, it's data should be durable

upvoted 1 times

 **TariqKipkemei** 4 months 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** 4 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

✉  **Guru4Cloud** 4 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 4 times

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

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

upvoted 1 times

✉  **idanr391** 4 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** 4 months, 2 weeks ago

Option D is the ideal answer.

upvoted 1 times

✉  **cookieMr** 5 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** 5 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** 6 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

✉  **Abrar2022** 6 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

✉  **EA100** 6 months, 3 weeks ago

ANSWER - C

upvoted 1 times

✉  **channn** 8 months ago

Selected Answer: D

Key words: minimize the time

upvoted 1 times

✉  **bilel500** 9 months ago

Selected Answer: D

The EBS fast snapshot restore feature allows you to restore EBS snapshots to new EBS volumes with minimal downtime. This is particularly useful when you need to restore large volumes or when you need to restore a volume to an EC2 instance in a different Availability Zone. When you enable the fast snapshot restore feature, the EBS volume is restored from the snapshot in the shortest amount of time possible, typically within a few minutes.

upvoted 1 times

✉  **Bofi** 9 months, 3 weeks ago

Selected Answer: A

Option A is correct because the question stated that the software that will access the test environment needs High I/O performance which is the core feature of instance store. The only risk for instance store is lost when the EC2 that it is attached to is terminated, however, this is a test environment, long term durability may not be required. Option C is not correct because it mentioned creating a new EBS and restoring the snapshot. The snapshot can be restored without creating a new EBS. It did not satisfy the minimum overhead requirement.

upvoted 5 times

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** Highly Voted 1 year, 1 month ago

Selected Answer: D

D because all of the components are infinitely scalable dynamoDB, API Gateway, Lambda, and of course s3+cloudfront
upvoted 30 times

 **Burugduystunstugudunstuy** Highly Voted 11 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 15 times

 **Burugduystunstugudunstuy** 11 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 11 times

 **Ruffyit** Most Recent 1 month 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** 1 month, 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** 4 months ago

Selected Answer: D

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

upvoted 2 times

 **hsinchang** 4 months ago

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

upvoted 2 times

 **Guru4Cloud** 4 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** 4 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 "LEAST operational overhead" (not mean migration/re-architect overhead, it is operational). Choose D.

upvoted 1 times

 **miki111** 4 months, 2 weeks ago

Option D is the right answer for this.

upvoted 1 times

 **cookieMr** 5 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** 5 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **cheese929** 6 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **MiteshB** 7 months ago

Selected Answer: D

ans: D

keywords: only one product on sale -- means static content

millions of requests each hour with millisecond latency -- dynamoDB

LEAST operational overhead -- choose serverless architecture -- lambda/ API Gateway that handle millions of request in one go with cost effective manner

upvoted 5 times

 **PhucVuu** 7 months, 3 weeks ago

Selected Answer: D

Keywords:

- Each day will feature exactly one product on sale for a period of 24 hours
- Handle millions of requests each hour with millisecond latency during peak hours.
- LEAST operational overhead

A: Incorrect - We cannot store all the data to S3 because our data is dynamic (Each day will feature exactly one product on sale for a period of 24 hours)

B: Incorrect - We don't have cache to improve performance (one product on sale for a period of 24 hours). Auto Scaling groups and RDS for MySQL need time to scale cannot scale immediately.

C: Incorrect - We don't have cache to improve performance (one product on sale for a period of 24 hours). Kubernetes Cluster Autoscaler can scale

better than Auto Scaling groups but it also need time to scale.

D: Correct - DynamoDB, S3, CloudFront, API Gateway are managed servers and they are highly scalable. CloudFront can cache static and dynamic data.

upvoted 8 times

 **gx2222** 8 months ago

Selected Answer: D

Option D uses Amazon S3 to host the website's static content, which requires no servers to be provisioned or managed. Additionally, Amazon CloudFront can be used to improve the latency and scalability of the website. The backend APIs can be built using Amazon API Gateway and AWS Lambda, which can handle millions of requests with low operational overhead. Amazon DynamoDB can be used to store order data, which can scale to handle high request volumes with low latency.

upvoted 1 times

 **apchandana** 8 months ago

Selected Answer: D

the most important key work is millisecond latency. only Dynamo DB can provide in this scale.

obviously, S3, Lambda, Cloud front, etc has built in scaling

upvoted 2 times

 **cheese929** 8 months, 2 weeks ago

Selected Answer: D

Answer is D. All services proposed are managed services and auto scalable.

upvoted 2 times

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** Highly Voted 1 year, 1 month 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 30 times

 **Buruguduystunstugudunstuy** Highly Voted 11 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 11 times

 **Buruguduystunstugudunstuy** 11 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 5 times

 **Ruffyit** Most Recent 1 month 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** 1 month, 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** 2 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** 2 months, 3 weeks ago

Unpredictable pattern, intelligent tiering will handle that.

B - is the answer..

upvoted 1 times

✉ **TariqKipkemei** 3 months, 4 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** 4 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** 4 months, 2 weeks ago

Option B is the right answer for this.

upvoted 1 times

✉ **james2033** 4 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** 4 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** 4 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** 5 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** 6 months, 2 weeks ago

B - for unpredictable patterns use intelligent tiering

upvoted 1 times

✉ **Rahulbit34** 7 months ago

B - "UNPREDICTABLE pattern" is the key

upvoted 2 times

✉ **PhucVuu** 7 months, 3 weeks ago

Selected Answer: B

Keywords:

- Must be resilient to the loss of an Availability Zone.

- files are accessed FREQUENTLY while other files are RARELY accessed in an UNPREDICTABLE pattern.

A - Incorrect: S3 Standard is not cost effective for rarely access files

B - Correct: S3 Intelligent-Tiering is good for file which frequently or rarely accessed in an unpredictable pattern. Intelligent-Tiering will help us analyze the pattern and move rarely access files to storage which has lower cost.

C - Incorrect: Standard-Infrequent Access is not cost effective for frequently access files

D - Incorrect: One Zone-Infrequent Access is not resilient to the loss of an Availability Zone

upvoted 4 times

 **channn** 8 months ago

Selected Answer: B

Key words: in an unpredictable pattern.

upvoted 1 times

 **cheese929** 8 months, 2 weeks ago

Selected Answer: B

S3 Intelligent-Tiering is the ideal storage class for data with unknown, changing, or unpredictable access patterns, independent of object size or retention period

upvoted 1 times

 **bilel500** 9 months 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.

upvoted 1 times

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 (97%)

✉️  **Buruguduystunstugudunstuy** Highly Voted  11 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 9 times

✉️  **Buruguduystunstugudunstuy** 11 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 3 times

✉️  **vgchan** 10 months, 2 weeks ago

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

upvoted 3 times

✉️  **ninjawrz** Highly Voted  1 year, 1 month ago

B: Transition to Glacier deep archive for cost efficiency

upvoted 7 times

✉️  **Ruffyit** Most Recent  1 month 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** 1 month, 4 weeks ago**Selected Answer: B**

Answer is B

upvoted 1 times

✉️  **sujanakakarla** 3 months ago**Selected Answer: B**

B as these files will be stored indefinitely after 1 month

upvoted 1 times

✉️  **TariqKipkemei** 3 months, 4 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 4 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 4 months, 2 weeks ago

Option B is the right answer for this.

upvoted 1 times

Kaab_B 4 months, 2 weeks ago

Selected Answer: B

Correct answer is B

upvoted 1 times

Debmalya_aws 4 months, 3 weeks ago

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

upvoted 1 times

bingusbongus 4 months, 2 weeks ago

You absolutely can.

upvoted 2 times

cookieMr 5 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 6 months, 1 week ago

Selected Answer: B

B is the correct answer

upvoted 1 times

beginnercloud 6 months, 2 weeks ago

Selected Answer: B

B is correct answer

upvoted 1 times

Rahulbit34 7 months ago

Transition to Glacier storage for cost efficient and can be queries in 5-7 hours time

upvoted 1 times

PhucVuu 7 months, 3 weeks ago

Selected Answer: B

Keywords:

- The files are accessed frequently for 1 month.
- Files are NOT accessed after 1 month.

A: Incorrect - We know the pattern (accessed frequently for 1 month, NOT accessed after 1 month) so we can configure it manually to make the cost reduce as much as possible.

B: Correct - Glacier Deep Archive is the most cost-effective for file which rarely use

C: Incorrect - Standard-Infrequent Access good for infrequent Access but not good for rarely(never) use.

D: Incorrect - One Zone-Infrequent Access can reduce more cost compare to Standard-Infrequent Access but it is not the best way compare to Glacier Deep Archive.

upvoted 3 times

enc_0343 9 months ago

The answer is B. "S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year." See here: <https://aws.amazon.com/s3/storage-classes/>

upvoted 1 times

KittieHearts 9 months, 1 week ago

Selected Answer: B

Files are only required to be kept up to 7 years for businesses to Deep archive is the most cost optimal as well as useful in this scenario.
upvoted 1 times

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

B (63%)	C (25%)	12%
---------	---------	-----

 **sba21**  1 year, 1 month ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/68306-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 30 times

 **123jh10**  1 year, 1 month 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 18 times

 **kidomaruto** 4 weeks ago

"The Cost Explorer Hourly and Resource level granularity allows you to access cost and usage data at hourly granularity for the past 14 days and resource level granularity."

<https://aws.amazon.com/fr/aws-cost-management/aws-cost-explorer/pricing/#:~:text=The%20Cost%20Explorer%20Hourly%20and,available%20for%20EC2%20instances%20only.>
upvoted 1 times

 **lofzee** 9 months, 2 weeks ago

14 days? Fam, you ever logged into the console?
upvoted 11 times

 **Udoyen** 12 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** 9 months, 3 weeks 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 7 times

 **t0nx**  1 week, 1 day 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 1 times

✉️ **Ruffyit** 1 month 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

✉️ **prabhjot** 1 month, 3 weeks ago

Option c-- adn why not B - Option B (Cost Explorer's granular filtering): Cost Explorer can provide detailed cost analysis, but it involves more manual work to create custom reports and may not offer the same level of simplicity for this specific analysis.

upvoted 1 times

✉️ **awsleffe** 1 month, 3 weeks ago

Option B

- Option B: Cost Explorer is a tool that enables you to view and analyze your costs and usage. You can filter graphs by values such as API operation, Availability Zone, AWS service, custom cost allocation tag, instance type, and more. This makes it a powerful tool for in-depth analysis of costs.
- Option C: The AWS Billing and Cost Management dashboard provides a high-level view of costs and does not offer the granular filtering needed for an in-depth analysis.

upvoted 3 times

✉️ **David_Ang** 2 months ago

Selected Answer: C

yeah this is really tricky, because "B" and "C"can do the job, but "B" using granular filtering cost money, even if is just 0.01\$ for every 1000 records, cost more money than answer "C" which does not cost any money at all, because you are just analyzing graphs.

upvoted 1 times

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

The answer is cost explorer

Billing and Cost management → An OVERALL look at all of the costs within your AWS organization or billing account

For central management.

In the management billing console you can do things such as add your credit card, add or remove regions, change your default currency but cost explorer is sort of different- its mainly for finding out what's being charged the most- you can review costs in both services but remember management billing console is for configurations mainly...

Cost Explorer can be used to filter and find the ROOT of problems

It can make visualizations, graphs

You can find unusual spending patterns

You can use cost allocation tags

Review your costs by day, week or month & custom timeframes

I hope this helps

upvoted 2 times

✉️ **midriss** 2 months, 3 weeks ago

AWS Cost and Usage Reports provide detailed billing data in a structured format, including instance types and costs, which makes it suitable for in-depth analysis. Answer is C

upvoted 1 times

✉️ **Hassao0** 3 months ago

answer is b because

The Monthly costs by service report shows your costs for the last six months, grouped by service.

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

upvoted 1 times

✉️ **BrijMohan08** 3 months ago

Selected Answer: D

Not B - Hourly granularity will reduce your dataset to your past 14 days of usage only.

upvoted 2 times

✉️ **bahaa_shaker** 3 months ago

Selected Answer: B

B is the right answer

upvoted 1 times

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

Selected Answer: B

I just logged into console: AWS Cost Management>AWS Cost Explorer>View in Cost Explorer>Filter Graph by 'DateRange', 'Service EC2', 'Instance Type'

upvoted 3 times

✉  **hsinchang** 4 months ago

Budgets is used to set goals, not for analysis.
The Billing and Cost Management dashboard is a dashboard, no in-depth analysis is provided.
Option D introduces S3 into the solution, adds operational overhead.
So B.

upvoted 3 times

✉  **Guru4Cloud** 4 months, 1 week ago

Selected Answer: D
AWS Cost and Usage Reports: By setting up AWS Cost and Usage Reports, you can collect detailed cost and usage data for your AWS resources, including EC2 instances, and store it in an S3 bucket. This provides the data required for an in-depth analysis.

Amazon S3 Bucket: Storing the cost and usage data in an S3 bucket allows you to have a centralized and secure location for your data, making it easily accessible for further analysis.

Amazon QuickSight: With Amazon QuickSight as a data visualization tool, you can easily connect to the data stored in the S3 bucket and create interactive graphs and visualizations. QuickSight offers various chart types and filtering options to perform an in-depth analysis based on instance types, cost trends, and usage patterns over the last 2 months.

upvoted 2 times

✉  **miki111** 4 months, 2 weeks ago

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

✉  **Kaab_B** 4 months, 2 weeks ago

Selected Answer: C
This way the job can be done with minimal effort.
upvoted 1 times

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 (99%)

 **123jh10** Highly Voted 1 year, 1 month 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 64 times

 **PhucVuu** Highly Voted 7 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 instances 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 12 times

 **pedestrianlove** Most Recent 1 week, 3 days 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 functions, 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 1 times

 **Ruffyt** 1 month ago

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

upvoted 1 times

 **xdkonorek2** 1 month, 1 week ago

Selected Answer: B

I think B would be better solution.
 How splitting one function into 2 increases scalability when company already increased service quota? Effectively they will have the 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 1 times

✉ **MakaylaLearns** 2 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** 2 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** 3 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** 3 months, 4 weeks ago

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

upvoted 1 times

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

Selected answer D

upvoted 1 times

✉ **miki111** 4 months, 2 weeks ago

Option D is the right answer for this.

upvoted 1 times

✉ **Kaab_B** 4 months, 2 weeks ago

Selected Answer: D

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

upvoted 1 times

✉ **Thornessen** 4 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 1 times

✉ **ichwilldoit** 4 months, 2 weeks 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** 5 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

✉ **TienHuynh** 5 months, 2 weeks ago

Selected Answer: D

D is correct, SQS can queue data

upvoted 1 times

✉ **Bmarodi** 6 months ago

Selected Answer: D

To improve scalability and minimize the configuration effort. Solutions architect can choose option D.
upvoted 1 times

 **Abrar2022** 6 months, 2 weeks ago

To improve scalability and minimize configuration efforts you can set up 2 lambda functions, one to receive the other to load. Then integrate the lambda functions using SQS.
upvoted 1 times

 **kakka22** 7 months, 2 weeks ago

Is the question wrong? Amazon Aurora use it's own DB not PostgreSQL, you need to provision an rds instance for that..
upvoted 1 times

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 11 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 34 times

✉️  **Buruguduystunstugudunstuy** 11 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 29 times

✉️  **gokalpkocer3** Highly Voted 1 year ago

Configuration changes= AWS Config

upvoted 22 times

✉️  **Ruffyit** Most Recent 1 month ago

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

upvoted 1 times

✉️  **TariqKipkemei** 3 months, 4 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** 4 months, 1 week 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** 4 months, 2 weeks ago

Option A is the right answer for this.

upvoted 1 times

✉️  **cookieMr** 5 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** 6 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** 7 months 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** 7 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** 8 months ago

Selected Answer: A

Key words:configuration changes

upvoted 1 times

✉ **linux_admin** 8 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** 9 months, 3 weeks ago

Selected Answer: A

aws: A - aws config

upvoted 1 times

✉ **Khushna** 10 months ago

AAAAaaaaaaaaaaaaaaaaaaaa

upvoted 1 times

✉ **SilentMilli** 10 months, 3 weeks 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

✉ **pazabal** 11 months, 1 week ago

Selected Answer: A

unauthorized config changes = aws config

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 11 months, 2 weeks 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 1 times

 **Buruguduystunstugudunstuy** 11 months, 2 weeks 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 1 times

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 (77%)

B (22%)

 **masetromain** Highly Voted 1 year, 1 month 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 67 times

 **123jhlo** 1 year, 1 month ago

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

upvoted 6 times

 **omoakin** 6 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 5 times

 **Azure55** 1 month ago

chatgpt chooses A

upvoted 1 times

 **Guru4Cloud** Highly Voted 4 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 9 times

 **emilyhu08** 1 month, 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 6 times

 **kt7** Most Recent 2 weeks, 6 days ago

A is correct

upvoted 1 times

 **Ruffyt** 1 month ago

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

upvoted 1 times

 **danielpark99** 1 month, 2 weeks ago

Selected Answer: A

Cloudwatch dashboards with people who do not have direct access to your aws account

upvoted 1 times

✉ **ABS_AWS** 2 months 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** 2 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 5 times

✉ **Examprep202324** 2 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** 3 months, 4 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** 4 months 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

✉ **bojila** 4 months ago

Selected Answer: B

You can create a link to add a user's email but to access the dashboard, the user will need to enter username/password... - "...The product manager does not have an AWS account..."

upvoted 1 times

✉ **bojila** 4 months ago

Share a single dashboard publicly, so that anyone who has the link can view the dashboard.

So, A

upvoted 1 times

✉ **NaaVeeN** 1 month, 4 weeks ago

its not private then.

upvoted 1 times

✉ **miki111** 4 months, 2 weeks ago

Option A is the right answer for this.

upvoted 1 times

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

Selected Answer: B

Answer B

Because A is not the best choice because it requires sharing a link that potentially could be accessed by unauthorized users, which does not follow the principle of least privilege.

upvoted 4 times

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

But we are also sharing a link to the dashboard in option B.

upvoted 1 times

✉ **oeufmeister** 4 months ago

But you still have to log in even after clicking on the link if you had chosen B, so it should not have such vulnerabilities, no?

upvoted 2 times

✉ **jaydesai8** 4 months, 3 weeks ago

Selected Answer: A

With CloudWatch you can share the dashboard entering the employees / user specific email address, Hence A is the answer

upvoted 1 times

 **nuray** 4 months, 3 weeks ago

In the question, it says the product manager does not have an AWS account. So the answer should be A.

I found this information on AWS's website. When you share dashboards, you can designate who can view the dashboard in three ways:

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.

Share a single dashboard publicly, so that anyone who has the link can view the dashboard.

Share all the CloudWatch dashboards in your account and specify a third-party single sign-on (SSO) provider for dashboard access. All users who are members of this SSO provider's list can access all the dashboards in the account. To enable this, you integrate the SSO provider with Amazon Cognito. The SSO provider must support Security Assertion Markup Language (SAML)

upvoted 5 times

 **nuray** 4 months, 3 weeks ago

Selected Answer: B

When you enable SSO, users registered with the selected SSO provider will be granted permissions to access all dashboards in this account.

When you disable the SSO provider, all dashboards will be automatically unshared.

so the question asks the principal of least privilege given to the product manager. That's why A gives more privileges. B is the right answer

upvoted 1 times

 **cookieMr** 5 months, 1 week ago

Selected Answer: A

This solution allows the product manager to access the CloudWatch dashboard without requiring an AWS account or IAM user credentials. By sharing the dashboard through the CloudWatch console, you can provide direct access to the specific dashboard without granting unnecessary permissions.

With this approach, the product manager can access the dashboard periodically by simply clicking on the provided link. They will be able to view the application metrics without the need for an AWS account or IAM user credentials. This ensures that the product manager has the necessary access while adhering to the principle of least privilege by not granting unnecessary permissions or creating additional IAM users.

upvoted 3 times

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 (78%) A (18%) 2%

✉️  **17Master**  1 year ago

Selected Answer: B

Tricky question!!! I forgot 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 55 times

✉️  **pbpally** 6 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 6 times

✉️  **pbpally** 6 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

✉️  **KADSM**  1 year 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 11 times

✉️  **pbpally** 6 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 2 times

✉️  **Ruffyit**  1 month 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 1 times

✉️  **rlamberti** 1 month, 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** 1 month, 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** 1 month, 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

 **parrtner73** 1 month, 3 weeks ago

B

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

upvoted 1 times

 **Examprep202324** 2 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** 3 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** 3 months, 2 weeks 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** 4 months, 2 weeks ago

Option B is the right answer for this.

upvoted 1 times

 **TheHadidi** 4 months, 4 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** 4 months, 2 weeks ago

This solution does not feature single-sign-on (SSO).

upvoted 3 times

 **cookieMr** 5 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 6 times

 **DuboisNicolasDuclair** 5 months, 3 weeks ago

Selected Answer: D

Can we have a moderator ?

upvoted 1 times

✉️  **omoakin** 6 months, 1 week ago

A is correct

Option B comes with security risk two way trust

upvoted 1 times

✉️  **sbnpj** 6 months, 2 weeks ago

Selected Answer: B

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

upvoted 3 times

✉️  **Abrar2022** 6 months, 2 weeks ago

AWS IAM Identity Center (successor to AWS Single Sign-On) requires a two-way trust so that it has permissions to read user and group.

upvoted 1 times

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 (82%)

Other

 **Six_Fingered_Jose** Highly Voted 1 year, 1 month 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 44 times

 **tavy** 1 month ago

ok but answer A does not mention service Global Accelerator, it mentions the NLB would act like one. Not sure if the wording is wrong or not.
' 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.' - keyword use NLB 'as an'
upvoted 1 times

 **bnagaraja9099** 1 month 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 3 times

 **awashenko** 1 month, 3 weeks ago

I also agree A after reading this link.
upvoted 1 times

 **ElaineRan** 4 months ago

Thank you, the link also helps me to know the differences between Global Acc and CloudFront.
upvoted 2 times

 **mouhannadhabj** Highly Voted 1 year 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 28 times

 **Ruffyit** Most Recent 1 month 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 1 times

 **rlamberti** 1 month, 1 week ago

Selected Answer: A

Keywords: UDP, VoIP, low latency.
<https://aws.amazon.com/global-accelerator/faqs/>
upvoted 1 times

✉  **tavy** 1 month 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 1 times

✉  **awashenko** 1 month, 3 weeks ago

Selected Answer: A

<https://aws.amazon.com/global-accelerator/faqs/>
upvoted 1 times

✉  **rainiverse** 2 months 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

✉  **midriss** 2 months, 3 weeks ago

Option A suggests using Network Load Balancers (NLB) and AWS Global Accelerator, which can provide lower-latency routing, but it does not inherently support automated failover between Regions.

upvoted 1 times

✉  **pavlinux** 3 months, 2 weeks ago

Selected answer: 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 1 times

✉  **Raggz** 3 months, 2 weeks 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

✉  **nafeez7950** 3 months, 3 weeks ago

Selected Answer: C

As much as I see A as a viable option, I would say C is the best option. Note that option A leverages the global accelerator to improve "PERFORMANCE". I would argue that performance and latency may not be the exact same thing. Subsequently, NLB operates at a regional level, which makes option A seems that there are no load balancers operating globally. With Route 53 to manage these latencies globally, and cloudfront, I would definitely say that option C is the more suitable option.

upvoted 3 times

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

Selected Answer: A

TCP and UDP = Global accelerator and Network Load Balancer

upvoted 1 times

✉  **Guru4Cloud** 4 months, 1 week ago

Selected Answer: C

The correct answer is C.

Deploy a Network Load Balancer (NLB) and an associated target group

An NLB is a good choice for a VoIP service because it can route traffic to the Region with the lowest latency. An NLB also provides load balancing and fault tolerance for your VoIP service.

Associate the target group with the Auto Scaling group

An Auto Scaling group can automatically scale your VoIP service up or down based on demand. This ensures that you have the right number of EC2 instances running to handle the load.

Create an Amazon Route 53 latency record that points to aliases for each NLB

A latency record in Amazon Route 53 routes traffic to the NLB that has the lowest latency. This ensures that your VoIP calls are routed to the Region with the lowest latency.

Create an Amazon CloudFront distribution that uses the latency record as an origin

Amazon CloudFront is a content delivery network (CDN) that can deliver your VoIP traffic closer to your users. This can improve the performance of your VoIP service.

upvoted 3 times

 **miki111** 4 months, 2 weeks ago

Option A is the right answer for this.

upvoted 1 times

 **karloscetina007** 4 months, 3 weeks ago

Selected Answer: A

UDP protocol and integration with cloudfront? it is a kind of trap in this question.

my answer is A

upvoted 2 times

 **cookieMr** 5 months, 1 week ago

Selected Answer: A

Option A, which suggests deploying a Network Load Balancer (NLB) and using it as an AWS Global Accelerator endpoint in each Region, does provide automated failover between Regions.

When using AWS Global Accelerator, it automatically routes traffic to the closest AWS edge location based on latency and network conditions. In case of a failure in one Region, AWS Global Accelerator will automatically reroute traffic to the healthy endpoints in another Region, providing automated failover.

So, option A does meet the requirement for automated failover between Regions, in addition to routing users to the Region with the lowest latency using AWS Global Accelerator.

upvoted 3 times

 **danielklein09** 6 months ago

Selected Answer: C

If the answer is A, how exactly we can accomplish this: "route users to the Region with the lowest latency"

upvoted 1 times

 **luisgu** 6 months, 2 weeks ago

Selected Answer: A

UDP --> NLB --> A or C.

I believe C is not an option because you cannot set up a route 53 record as a cloudfront origin:

https://docs.aws.amazon.com/cloudfront/latest/APIReference/API_Origin.html

upvoted 2 times

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

C (81%)

Other

✉  **hanhdroid** Highly Voted 1 year, 1 month ago

Selected Answer: C

Answer C, you still pay for storage when an RDS database is stopped
upvoted 27 times

✉  **KVK16** Highly Voted 1 year, 1 month 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

✉  **MiniYang** Most Recent 1 week, 5 days 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 1 times

✉  **roberto_rrt** 1 month, 2 weeks 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 1 times

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

Selected Answer: C

As DB snapshots is cost efficient.

upvoted 1 times

✉️ **miki111** 4 months, 2 weeks ago

Option C is the right answer for this.

upvoted 1 times

✉️ **cookieMr** 5 months, 1 week ago

Selected Answer: C

Option C can be a cost-effective solution for reducing the cost of running tests on the RDS instance.

By creating a snapshot and terminating the DB instance, you effectively stop incurring costs for the running instance. When you need to run the tests again, you can restore the snapshot to create a new instance and resume testing. This approach allows you to save costs during the periods when the tests are not running.

However, it's important to note that option C involves additional steps and may result in some downtime during the restoration process. You need to consider the time required for snapshot creation, termination, and restoration when planning the testing schedule.

upvoted 3 times

✉️ **Abrar2022** 5 months, 1 week ago

Selected Answer: C

Can't be A because you're still charged for provisioned storage even when it's stopped.

upvoted 1 times

✉️ **Peng001** 6 months ago

Selected Answer: C

By only stopping an Amazon RDS DB instance, you stop billing for additional instance hours, but you will still incur storage costs. See: <https://aws.amazon.com/rds/pricing/>

upvoted 1 times

✉️ **studynoplay** 7 months ago

Selected Answer: C

Trick: in a stopped RDS database, you will still pay for storage. If you plan on stopping it for a long time, you should snapshot & restore instead

upvoted 2 times

✉️ **channn** 8 months ago

Selected Answer: C

Compare A and C, for a 48 hours usage among a month, C's cost lower.

upvoted 1 times

✉️ **linux_admin** 8 months ago

Selected Answer: A

Option A, stopping the DB instance when tests are completed and restarting it when required, would be the most cost-effective solution to reduce the cost of running the tests while maintaining the same compute and memory attributes of the DB instance.

By stopping the DB instance when the tests are completed, the company will only be charged for storage and not for compute resources while the instance is stopped. This can result in significant cost savings as compared to running the instance continuously.

When the tests need to be run again, the company can simply start the DB instance, and it will be available for use. This solution is straightforward and does not require any additional configuration or infrastructure.

upvoted 3 times

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

if you stopped RDS it gets auto start after 7 days. Here the requirement is once in month ..hence C

upvoted 2 times

✉️ **cheese929** 8 months, 1 week ago

Selected Answer: C

C is the most cost effective.

upvoted 1 times

✉️ **Tiba** 10 months, 3 weeks ago

You can't stop an Amazon RDS for SQL Server DB instance in a Multi-AZ configuration.

upvoted 1 times

✉️ **SilentMilli** 10 months, 3 weeks ago

Selected Answer: C

Amazon RDS for MySQL allows you to create a snapshot of your DB instance and store it in Amazon S3. You can then terminate the DB instance and restore it from the snapshot when required. This will allow you to reduce the cost of running the resource-intensive tests without reducing the

compute and memory attributes of the DB instance.
upvoted 1 times

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 (97%)

✉️  **kurinei021** Highly Voted  11 months, 1 week 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 15 times

✉️  **aaroncelestin** 3 months, 2 weeks 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 7 times

✉️  **kidomaruto** 3 weeks, 6 days 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 1 times

✉️  **cookieMr** Highly Voted  5 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

✉️  **Ruffyit** Most Recent  1 month 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** 1 month, 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** 3 months, 1 week ago

Selected Answer: A

A without a doubt
upvoted 1 times

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

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

 **lelouchjedai** 5 months, 2 weeks ago

Selected Answer: A

The answer is A
upvoted 1 times

 **Bmarodi** 5 months, 4 weeks ago

Selected Answer: A

Option will accomplish the requirements
upvoted 1 times

 **beginnercloud** 6 months, 2 weeks ago

Selected Answer: A

AWS Config can track the configuration status of non-compliant resources :))
upvoted 1 times

 **caffee** 7 months, 3 weeks ago

Selected Answer: A

AWS Config can track the configuration status of non-compliant resources.
upvoted 2 times

 **gx2222** 7 months, 4 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** 8 months ago

Selected Answer: A

Key words: configured with tags
upvoted 1 times

 **linux_admin** 8 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

 **bilel500** 8 months, 3 weeks ago

Selected Answer: A

AWS Config provides a detailed view of the resources associated with your AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.
upvoted 1 times

 **Ello2023** 9 months, 3 weeks ago

I found this question very vague.
upvoted 2 times

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** Highly Voted 1 year, 1 month ago

Selected Answer: B

Good answer is B: client-side JavaScript. the website is static, so it must be S3.
upvoted 23 times

✉️  **BoboChow** Highly Voted 1 year, 1 month ago

Selected Answer: B

HTML, CSS, client-side JavaScript, and images are all static resources.
upvoted 8 times

✉️  **Ruffyt** Most Recent 1 month ago

HTML, CSS, client-side JavaScript, and images are all static resources.
upvoted 1 times

✉️  **AWSStudyBuddy** 1 month, 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** 2 months, 3 weeks ago

Selected Answer: B

Static website should work fine with S3
upvoted 1 times

✉️  **KawtarZ** 3 months, 1 week ago

Selected Answer: B

the website is static because the backend runs on client side.
upvoted 2 times

✉️  **evanhongo** 3 months, 3 weeks ago

Selected Answer: B

all static resources.
upvoted 1 times

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

Selected Answer: B

static website, cost-effective = S3 web hosting
upvoted 2 times

✉️  **james2033** 4 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** 4 months, 2 weeks ago

Option B is the right answer for this.

upvoted 1 times

 **Kaab_B** 4 months, 2 weeks ago

Selected Answer: B

S3 is amongst the cheapest services offered by AWS.

upvoted 1 times

 **karloscetina007** 4 months, 3 weeks ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

 **cookieMr** 5 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 4 times

 **Bmarodi** 5 months, 4 weeks ago

Selected Answer: B

Option B is the MOST cost-effective for hosting the website.

upvoted 1 times

 **beginnercloud** 6 months, 2 weeks ago

Selected Answer: B

static website = B

upvoted 1 times

 **Rahulbit34** 7 months ago

Since all are static, S3 can be used to host it

upvoted 1 times

 **kamx44** 7 months, 2 weeks ago

Selected Answer: B

static website B

upvoted 1 times

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 (81%)

B (19%)

 **ArielSchivo** Highly Voted  1 year, 1 month ago

Selected Answer: C

I would go for C. The tricky phrase is "near-real-time solution", pointing to Firehose, 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 54 times

 **SaraSundaram** 8 months, 2 weeks ago

There are many questions having Firehose and Stream. Need to know them in detail to answer. Thanks for the explanation
upvoted 3 times

 **diabloexodia** 4 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 6 times

 **Lonojack** 10 months, 1 week 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 2 times

 **lizzard812** 9 months, 4 weeks 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** 9 months, 1 week 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** Highly Voted  1 year, 1 month 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 26 times

 **wabosi** Most Recent  2 weeks, 3 days 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** 1 month 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** 1 month, 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** 1 month, 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** 2 months ago

I picked B. We need to understand how Kinesis Data Warehouse works to answer this question right.

upvoted 1 times

✉️ **spw7** 1 month ago

firehose can not send data to dynamoDB

upvoted 1 times

✉️ **sohailn** 3 months, 3 weeks ago

kinesis Data Firhouse optionally support lambda for transformation

upvoted 1 times

✉️ **TariqKipkemei** 3 months, 4 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** 5 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** 5 months, 2 weeks ago

Selected Answer: C

its c because yes

upvoted 1 times

✉ **Chris22usa** 5 months, 2 weeks ago

I think it is B. Kinesis data stream can import data from DynamoDB, but can not export data to DynamoDB. Data stream only support to export to Lamda, Kinesis Firehose, Kinesis Analytics or AWS Glue. Data stream's exporting to other object need to ETL transform process , which is Firehose's function.

upvoted 1 times

✉ **koneczny69** 5 months, 2 weeks ago

Selected Answer: B

near real time - firehose
besides - dynamo is no the destination, lambda is
and lambda can be used since you can expose it behind http

upvoted 1 times

✉ **Vlad** 6 months, 2 weeks ago

Selected Answer: B

That is definitely B:

It is saying "near real time" that makes sense :

near real time : Kinesis Data Firehose
real time : Kinesis Data Stream

Also, Kinesis Data Firehose supports DynamoDB. The link is below :

<https://dynobase.dev/dynamodb-faq/can-firehose-write-to-dynamodb/#:~:text=Answer,data%20to%20a%20DynamoDB%20table>.

upvoted 1 times

✉ **Clouddon** 3 months, 3 weeks ago

I disagree with the statement about firehose as stated from this source because aws says "Kinesis Data Firehose currently supports Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk, Datadog, NewRelic, Dynatrace, Sumo Logic, LogicMonitor, MongoDB, and HTTP End Point as destinations."

upvoted 1 times

✉ **sakurali** 1 month, 1 week ago

disagree with ur point, cuz Firehose is all about delivering data. It's like a reliable courier that ensures your data gets to its destination securely and promptly. While Firehose itself doesn't store data, it can deliver it to various AWS services, including Amazon DynamoDB and Amazon S3.

upvoted 1 times

✉ **ruqui** 6 months, 2 weeks ago

The problem says that Firehose will store data in Amazon DynamoDB and Amazon S3, I think it's not possible to have more than one consumer, so B solution is impossible

upvoted 3 times

✉ **plutonash** 6 months, 4 weeks ago

Selected Answer: B

for me the answer is B. kinesis data firehose can transfer data to dynamoDB and the key word in the question : Near Real Time
Real Time = Kinesis Data Stream
Near Real Time = Kinesis Data Firehose

upvoted 5 times

✉ **jramos** 7 months, 3 weeks ago

Selected Answer: B

Kinesis Data Firehose does have integration with Lambda. Kinesis Data Streams does not have that integration so B is correct

upvoted 2 times

✉ **bakamon** 8 months ago

Selected Answer: C

Near Real Time : Kinesis Data Stream & Kinesis Data Firehose
Kinesis Data Stream :: used for streaming live data
Kinesis Data Firehose :: used when you have to store the streaming data into S3, Redshift etc

upvoted 5 times

✉ **linux_admin** 8 months ago

Selected Answer: C

This solution meets the requirements for scalability, near-real-time processing, and sharing data with several internal applications. Kinesis Data Streams is a fully managed service that can handle millions of transactions per second, making it a scalable solution. Using Lambda to process the data and remove sensitive information provides a fast and efficient method to perform data transformation in near-real-time. Storing the processed data in DynamoDB allows for low-latency retrieval, and the data can be shared with other applications using the Kinesis data stream.

upvoted 2 times

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** Highly Voted  1 year, 1 month 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 28 times

 **Ruffyit** Most Recent  1 month 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** 1 month, 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** 1 month, 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** 3 months, 4 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** 4 months ago

Selected Answer: B

CONFIG - AWS CONFIG
RECORD API CALLS - CLOUDTRAIL
upvoted 1 times

 **hsinchang** 4 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** 4 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** 4 months, 2 weeks ago

Option B is the right answer for this.

upvoted 1 times

✉ **karloscetina007** 4 months, 3 weeks ago

Selected Answer: B

B is the answer with no doubts

upvoted 1 times

✉ **minhpn** 5 months, 1 week ago

Selected Answer: B

config => AWS config

record API calls => AWS CloudTrail

upvoted 1 times

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

Selected Answer: B

Option B meets requirements.

upvoted 1 times

✉ **linux_admin** 8 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** 8 months, 3 weeks 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

✉ **bilel500** 8 months, 3 weeks 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

 **Mcmono** 9 months, 1 week ago

Selected Answer: B

AWS Config is basically used to track config changes, while cloudtrail is to monitor API calls
upvoted 1 times

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, 1 month ago

Selected Answer: D

Answer is D
C is incorrect because question says Third party DNS and route 53 is AWS proprietary
upvoted 33 times

✉  **kidomaruto** 3 weeks, 6 days ago

Right answer, wrong explanation.
You can use Route 53 with a custom domain.. it's all about the "large-scale DDOS attack".
upvoted 1 times

✉  **BoboChow**  1 year, 1 month 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 25 times

✉  **leonardh** 6 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 4 times

✉  **OmegaLambda7XL9**  1 week, 5 days ago

This one got me to be honest
upvoted 1 times

✉  **Ruffyit** 1 month 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** 1 month 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** 1 month, 3 weeks ago

D, but can be tricky, the third party negates Route53
upvoted 1 times

✉  **Ak9kumar** 2 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** 3 months ago

answer is D

upvoted 1 times

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

Selected Answer: D

DDos = AWS Shield

upvoted 2 times

✉  **hsinchang** 4 months ago

Selected Answer: D

large-scale DDos leads to advanced instead of standard AWS Shield.

upvoted 1 times

✉  **james2033** 4 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** 4 months, 2 weeks ago

Option D is the right answer for this.

upvoted 1 times

✉  **Kaab_B** 4 months, 2 weeks ago

Selected Answer: D

DDoS extended is AWS Sheild Advance without a doubt.

upvoted 1 times

✉  **karloscetina007** 4 months, 3 weeks ago

A third-party service

D is the answer with no doubts

upvoted 1 times

✉  **cookieMr** 5 months, 1 week ago

Selected Answer: D

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 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 6 times

✉  **Bmarodi** 5 months, 4 weeks ago

Selected Answer: D

I voting for the option D.

upvoted 1 times

✉  **channn** 8 months ago

Selected Answer: D

Key words: DDos -> Shield

upvoted 2 times

✉  **Daiking** 9 months ago

Selected Answer: D

DDoS attack is a feature of AWS Shield, so I confused C or D. But it usually determines by Health-Check, and Health-Check runs in the level target group of ELB. Finally, I would go with D.

upvoted 1 times

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 (55%)

D (43%)

✉️  **pooppants**  1 year, 1 month ago

Selected Answer: B

KMS Multi-region keys are required <https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>
upvoted 52 times

✉️  **dwx101** 1 month, 3 weeks ago

AWS services that integrate with AWS KMS for encryption at rest or digital signatures currently treat multi-Region keys as though they were single-Region keys. They might re-wrap or re-encrypt data moved between Regions. For example, 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.

upvoted 2 times

✉️  **sohailn** 3 months, 3 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 3 times

✉️  **sakurali** 1 month, 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 2 times

✉️  **Instantqueue** 1 month, 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 2 times

✉️  **hypnozz** 5 months, 2 weeks ago

The answer is C, because "Server-side encryption with Amazon S3 managed keys (SSE-S3) is the base level of encryption configuration for every bucket in Amazon S3. If you want to use a different type of default encryption, you can also specify server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS) or customer-provided keys (SSE-C)"

By using SSE-KMS, you can encrypt the data stored in the S3 buckets with a customer managed KMS key. This ensures that the data is protected and allows you to have control over the encryption key. By creating an S3 bucket in each Region and configuring replication between them, you can have data and key redundancy in both Regions.

upvoted 3 times

✉️  **Clouddon** 3 months, 3 weeks ago

Option B, 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. 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. You can use multi-Region keys with client-side encryption libraries, such as the AWS Encryption SDK, the DynamoDB Encryption Client, and Amazon S3 client-side encryption. For an example of using multi-Region keys with Amazon DynamoDB global tables and the DynamoDB Encryption Client, see Encrypt global data client-side with AWS KMS multi-Region keys in the AWS Security Blog.
<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>

upvoted 3 times

✉️  **KJa**  1 year, 1 month 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 46 times

✉ **BoboChow** 1 year, 1 month 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, 1 month ago

key change across regions unless you use multi-Region keys

upvoted 2 times

✉ **Clouddon** 3 months, 3 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 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** 7 months, 4 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 3 times

✉ **mattlai** 1 year, 1 month ago

fun joke, if u dont do encryption on client side, where else could it be?

upvoted 1 times

✉ **Newptone** 1 year 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 4 times

✉ **Newptone** 1 year ago

Sorry for the typo, I mean option D.

upvoted 2 times

✉ **Marco_St** Most Recent 2 weeks, 3 days ago

Selected Answer: B

A multi-Region KMS key allows you to create a primary key in one region and replicate it in another region. The replica key in the different region is a separate AWS resource but shares the same key material as the primary key.

upvoted 1 times

✉ **NickGordon** 3 weeks, 2 days ago

Selected Answer: B

D is incorrect as it does not mention key replication. the keys created in 2 different regions are not same.

B is correct as it is the only one has key replication enabled.

upvoted 1 times

✉ **kidomaruto** 3 weeks, 6 days ago

Selected Answer: D

- A. not using KMS
- B. key need to be store in AWS so not a client side encryption
- C. Not using KMS for encryption
- D. good answer

upvoted 1 times

✉ **Eneiss** 1 month ago

Selected Answer: D

D because server-side encryption with customer-managed KMS key

upvoted 2 times

 **sweetheatmn** 1 month, 1 week ago

Selected Answer: D

It cannot be B because it is an extreme operational overhead case, client-side encryption requires setting up encryption SDK to encrypt the file before sending to S3 a call to KMS generateDataKey for encryption and with every read of the file, the same process reversed will be done

+ There is no point in creating the key in two regions if the app itself will encrypt the files before sending them to S3
upvoted 3 times

 **AWSStudyBuddy** 1 month, 1 week ago

Selected Answer: B

I go with Option B.

The solution with the least operational overhead to meet the company's requirements is to use a multi-Region key in AWS KMS.

Multi-Region keys are AWS KMS keys in different AWS Regions that can be used interchangeably. They have 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 2 times

 **AWSStudyBuddy** 1 month, 1 week ago

<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>

upvoted 1 times

 **iwannabeawsgod** 1 month, 2 weeks ago

i think B is correct

upvoted 1 times

 **daniel1** 1 month, 2 weeks ago

Answer by ChatGPT 4.0 is D

upvoted 3 times

 **Barbie54** 1 month, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>

AWS services that integrate with AWS KMS for encryption at rest or digital signatures currently treat multi-Region keys as though they were single-Region keys. They might re-wrap or re-encrypt data moved between Regions. For example, 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.

upvoted 1 times

 **dwx101** 1 month, 3 weeks ago

you know what, Multi KMS i get the argument, its true be like having one key in diff regions, but its the way it encrypting on replication...gonna go try it.....be back with this one

upvoted 1 times

 **awashenko** 1 month, 3 weeks ago

Selected Answer: B

So its obvious that A and C are incorrect as those keys are managed on AWS side. Answer comes down to B and D. I had to do some research and re-read the question a few times and I think the answer is B. If you go with D, you end up creating 2 keys that can't be the same. B is 1 key.

A multi-Region replica key is a KMS key that has the same key ID and key material as its primary key and related replica keys, but exists in a different AWS Region. A replica key is a fully functional KMS key with its own key policy, grants, alias, tags, and other properties.

upvoted 1 times

 **awashenko** 1 month, 3 weeks ago

Correction; its two keys that act as 1 basically

upvoted 1 times

 **David_Ang** 2 months ago

Selected Answer: B

the reason why "B" is correct it's because they are asking for only one key, if you create a key per region you now have 2 Keys one for each bucket and they need the same one to work in both of the buckets. C and D are incorrect

upvoted 1 times

 **MOSHE** 2 months ago

Selected Answer: B

B. This solution creates a customer managed multi-Region KMS key, which meets the requirement to use the same KMS key across two regions. It uses client-side encryption with the KMS key, which means the application is responsible for encryption and decryption processes. This satisfies all requirements.

D. While this solution does use customer managed KMS keys, it creates separate KMS keys in each region. Although it uses SSE-KMS, which would be closer to the requirement, it doesn't meet the requirement of using the same KMS key across two regions.

upvoted 1 times

 **SymnuiSlon** 2 months ago

Selected Answer: D

"The company must use an AWS Key Management Service (AWS KMS) customer managed key

(AWS-KMS) was mentioned only in a D option, then only D meets the requirements

upvoted 1 times

 **dagr** 2 months ago

Selected Answer: B

I think the key to this question is mult-region keys

upvoted 1 times

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

B (94%)

6%

✉️  **BoboChow**  1 year, 1 month 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 17 times

✉️  **Nightducky** 1 year 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 1 times

✉️  **sohailn** 3 months, 3 weeks ago

session manager works with linux, windows, and mac too

upvoted 3 times

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

"Cross-platform support for Windows, Linux, and macOS"

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

upvoted 2 times

✉️  **JayBee65** 12 months ago

Session Manager provides support for Windows, Linux, and macOS from a single tool

upvoted 5 times

✉️  **AWSStudyBuddy**  1 month, 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 1 times

✉️  **AWSStudyBuddy** 1 month, 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 1 times

✉  **Guru4Cloud** 3 months, 3 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** 3 months, 4 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** 4 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** 4 months, 2 weeks ago

Option B is the right answer for this.

upvoted 1 times

✉  **TienHuynh** 5 months, 1 week 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** 5 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** 5 months, 4 weeks ago

Selected Answer: B

The choice for me is the option B.

upvoted 1 times

✉  **cheese929** 7 months, 3 weeks ago

Selected Answer: B

B is correct and has the least overhead.

upvoted 1 times

✉  **linux_admin** 8 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** 8 months, 1 week 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** 8 months, 4 weeks 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** 9 months, 3 weeks 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** 9 months, 3 weeks 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

 **Pranav_523** 10 months, 2 weeks ago

Selected Answer: B

correct answer is B

upvoted 1 times

 **SilentMilli** 10 months, 3 weeks ago

Selected Answer: B

Option B. Attaching the appropriate IAM role to each existing instance and new instance and using AWS Systems Manager Session Manager to establish a remote SSH session would meet the requirements with the least operational overhead. This approach allows for secure remote access to the instances without the need to manage additional infrastructure or maintain a separate connection to the instances. It also allows for the use of native AWS services and follows the AWS Well-Architected Framework.

upvoted 1 times

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** Highly Voted 5 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 21 times

 **Ruffyt** Most Recent 1 month 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** 3 months, 3 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** 3 months, 3 weeks ago

Keywords:

Global, Reduce latency, S3, Static Website, Cost effective = Amazon CloudFront

upvoted 2 times

 **james2033** 4 months, 1 week ago

Selected Answer: C

Keyword "Amazon CloudFront" (C).

upvoted 1 times

 **miki111** 4 months, 2 weeks ago

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

 **miki111** 4 months, 2 weeks ago

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

 **TienHuynh** 5 months, 1 week ago

Selected Answer: C

key words:
-around the world
-decrease latency
-most cost-effective

answer is C

upvoted 1 times

 **cheese929** 7 months, 3 weeks ago

Selected Answer: C

C is the most cost effective.
upvoted 1 times

 **linux_admin** 8 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** 8 months, 2 weeks ago

Selected Answer: C

Cloud front
upvoted 1 times

 **bilel500** 8 months, 3 weeks 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** 9 months, 1 week 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** 9 months, 3 weeks 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

 **AndyMartinez** 9 months, 4 weeks ago

Selected Answer: C

Option C.
upvoted 1 times

 **SilentMilli** 10 months, 3 weeks ago

Selected Answer: C

Option C. Adding an Amazon CloudFront distribution in front of the S3 bucket and editing the Route 53 entries to point to the CloudFront distribution would meet the requirements most cost-effectively. CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content by distributing it across a global network of edge locations. When a user accesses the website, CloudFront will automatically route the request to the edge location that provides the lowest latency, reducing the time it takes for the content to be delivered to the user. This solution also allows for easy integration with S3 and Route 53, and provides additional benefits such as DDoS protection and support for custom SSL certificates.

upvoted 2 times

 **pazabal** 11 months, 1 week ago

Selected Answer: C

decrease latency and most cost-effective = cloudfront in front of S3 bucket (content can be served closer to the user, reducing latency). Replicating S3 bucket and Global accelerator would also decrease latency but would be less cost-effective. Transfer accelerator wouldn't decrease latency since it's not for delivering content, but for transferring it

upvoted 2 times

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

A (97%)

 **pazabal** Highly Voted 11 months, 1 week 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 23 times

 **cookieMr** Highly Voted 5 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 14 times

 **aptx4869** Most Recent 1 month 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** 1 month 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** 1 month, 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** 1 month, 3 weeks ago

Selected Answer: A

Key: database storage performance is the problem.
upvoted 1 times

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

Selected Answer: A

Provisioned IOPS SSD it is.

upvoted 1 times

 **Suvam90** 4 months, 1 week ago

Option A is correct

upvoted 1 times

 **james2033** 4 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

 **Monu11394** 4 months, 2 weeks ago

who decides what the correct answer is?

the question clearly says "company determined storage issue"

upvoted 2 times

 **miki111** 4 months, 2 weeks ago

Option A is the right answer for this.

upvoted 1 times

 **Jayendra0609** 4 months, 2 weeks ago

Selected Answer: B

Memory-optimized instances are helpful for efficient performance in the case of workloads that handle huge data sets in memory.

[https://www.projectpro.io/article/aws-rds-instance-types/749#:~:text=Memory%20Optimized%20AWS%20RDS%20Instances,%2C%20X2g\)%2C%20and%20Z1d](https://www.projectpro.io/article/aws-rds-instance-types/749#:~:text=Memory%20Optimized%20AWS%20RDS%20Instances,%2C%20X2g)%2C%20and%20Z1d).

upvoted 1 times

 **omerap12** 5 months ago

Selected Answer: A

need I/O

upvoted 1 times

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

A (84%)	D (16%)
---------	---------

 **Sinaneos** Highly Voted 1 year, 1 month 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 32 times

 **Kelvin_ke** 11 months, 3 weeks ago

what about the 30 days minimum requirement to transition to S3 glacier?

upvoted 8 times

 **Abrar2022** 6 months, 2 weeks ago

GLACIER IS 7 DAYS REQUIREMENT NOT 30

upvoted 2 times

 **coffee** 7 months, 3 weeks ago

This constraint is related to moving from Standard to IA/IA-One Zone only. Nothing to do with Glacier

upvoted 2 times

 **studis** 11 months, 2 weeks 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 3 times

 **ErnShm** 6 months ago

the current article doesn't enable the current option, minimum days are 30

upvoted 1 times

 **Suvam90** 3 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

 **123jh10** Highly Voted 1 year, 1 month 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 13 times

 **OmegaLambda7XL9** Most Recent 1 week, 5 days 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** 1 month ago

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

upvoted 1 times

✉ **tom_cruise** 1 month, 3 weeks ago

Selected Answer: A

Key: MOST operationally efficient solution

upvoted 1 times

✉ **David_Ang** 2 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** 2 months ago

I picked A. Appeared to be right answer.

upvoted 1 times

✉ **chandu7024** 2 months, 1 week ago

Should be A

upvoted 1 times

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

Selected Answer: A

The MOST operationally efficient option is A.

upvoted 1 times

✉ **james2033** 4 months, 1 week ago

Selected Answer: A

Keyword "Amazon S3 Glacier" (A).

upvoted 1 times

✉ **miki111** 4 months, 2 weeks ago

Option A is the right answer for this.

upvoted 1 times

✉ **cookieMr** 5 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 6 times

✉ **Abrar2022** 6 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

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

Selected Answer: D

D is the correct answer. Check the link below

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

upvoted 1 times

✉ **linux_admin** 8 months ago

Selected Answer: A

Amazon Kinesis Data Firehose is a fully managed service that can capture, transform, and deliver streaming data into storage systems or analytics tools, making it an ideal solution for ingesting and storing status alerts. In this solution, the Kinesis Data Firehose delivery stream ingests the alerts and delivers them to an S3 bucket, which is a cost-effective storage solution. An S3 Lifecycle configuration is set up to transition the data to Amazon S3 Glacier after 14 days to minimize storage costs.

upvoted 2 times

 **bilel500** 8 months, 3 weeks ago

Selected Answer: A

The correct answer is 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.

upvoted 1 times

 **Ello2023** 9 months, 3 weeks ago

This question was tricky but after some reading my choice went from D to A. Which is Operationally efficient.

upvoted 1 times

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 (72%)

A (28%)

✉  **Six_Fingered_Jose**  1 year, 1 month ago

Selected Answer: B

This question just screams AppFlow (SaaS integration)
<https://aws.amazon.com/appflow/>

upvoted 25 times

✉  **Six_Fingered_Jose** 1 year, 1 month 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 15 times

✉  **jdr75**  8 months 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 19 times

✉  **MoshiurGCP**  1 week, 1 day ago

SaaS - AppFlow

upvoted 1 times

✉  **OmegaLambda7XL9** 1 week, 5 days 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 1 times

✉  **Ruffyit** 1 month ago

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

upvoted 1 times

✉  **sweetheatmn** 1 month, 1 week ago

Selected Answer: B

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

upvoted 1 times

 **ACloud_Guru15** 1 month, 2 weeks ago

Selected Answer: B

B suits the requirement

upvoted 1 times

 **tom_cruise** 1 month, 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** 1 month, 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** 2 months, 1 week 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** 3 months, 3 weeks ago

Selected Answer: B

SaaS Integration = Amazon AppFlow

upvoted 1 times

 **hsinchang** 4 months ago

Selected Answer: B

SaaS -> AppFlow

upvoted 1 times

 **miki111** 4 months, 2 weeks ago

Option B is the right answer.

upvoted 1 times

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

So true, This question just screams AppFlow (SaaS integration)

upvoted 1 times

 **Rahulbit34** 7 months ago

With Amazon AppFlow automate bi-directional data flows between SaaS applications and AWS services in just a few clicks. So B is the right answer

upvoted 1 times

 **cheese929** 7 months, 3 weeks ago

Selected Answer: B

Amazon AppFlow is a fully-managed integration service that enables you to securely exchange data between software as a service (SaaS) applications, such as Salesforce, and AWS services, such as Amazon Simple Storage Service (Amazon S3) and Amazon Redshift.

The use of Appflow helps to remove the ec2 as the middle layer which slows down the process of data transmission and introduce an additional variable.

Appflow is also a fully managed AWS service, thus reducing the operational overhead.

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

upvoted 3 times

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** Highly Voted 10 months, 3 weeks 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 46 times

✉  **OmegaLambda7XL9** 1 week, 5 days ago

Precisely

upvoted 1 times

✉  **johne42** 3 months, 1 week ago

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 2 times

✉  **Bmarodi** 5 months, 4 weeks ago

Very good explanation!

upvoted 5 times

✉  **MoshiurGCP** Most Recent 1 week, 1 day ago

Avoid regional data transfer charge - VPC endpoint

upvoted 1 times

✉  **Ruffyit** 1 month ago

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 1 times

✉  **ACloud_Guru15** 1 month, 2 weeks ago

Selected Answer: C

Gateway Endpoint bests suits the requirement

upvoted 1 times

✉  **srinivasmn** 2 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** 3 months, 3 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** 3 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** 4 months, 2 weeks ago

Option C is the right answer.

upvoted 1 times

✉  **cookieMr** 5 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 3 times

✉  **Bmarodi** 5 months, 4 weeks ago

Selected Answer: C

Option C is the answer.

upvoted 1 times

✉  **linux_admin** 8 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** 9 months, 4 weeks ago

Selected Answer: C

C - gateway VPC endpoint.

upvoted 1 times

✉  **secdaddy** 11 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 1 times

✉  **pazabal** 11 months, 1 week 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** 11 months, 2 weeks 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** 11 months, 2 weeks ago

Selected Answer: C

VPC endpoint

upvoted 1 times

✉  **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 28 times

 **Buruguduystunstugudunstuy** Highly Voted 11 months, 2 weeks 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 15 times

 **Buruguduystunstugudunstuy** 11 months, 2 weeks 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 5 times

 **OmegaLambda7XL9** 1 week, 5 days 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 1 times

 **Bofi** 9 months, 1 week 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 1 times

 **Buruguduystunstugudunstuy** 9 months ago

You're right Option B is the correct answer. I answered Option B as the correct answer above.
 upvoted 1 times

 **MoshiurGCP** Most Recent 1 week, 1 day ago

Resolve Internet connection problem - Direct Connect
 upvoted 1 times

 **Ruffyit** 1 month 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** 1 month, 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** 1 month, 2 weeks ago

Selected Answer: B

Key: time sensitive. So snowball does not apply here.

upvoted 1 times

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

Typo correction to my my above comment. The right option is B.

upvoted 1 times

✉ **chandu7024** 2 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** 3 months, 3 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** 3 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** 4 months, 2 weeks ago

Option B is the right answer.

upvoted 1 times

✉ **Kaab_B** 4 months, 2 weeks ago

Selected Answer: B

This is long-term and provides solution for internet speed as well

upvoted 1 times

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

Galleta siempre veo tus comentarios! sos crack!

upvoted 1 times

✉ **Bmarodi** 5 months, 4 weeks ago

Selected Answer: B

Option B meets these requirements.
upvoted 1 times

 **Abrar2022** 6 months, 2 weeks 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

 **linux_admin** 8 months ago

Selected Answer: B

AWS Direct Connect is a dedicated network connection that provides a more reliable and consistent network experience compared to internet-based connections. By establishing a new Direct Connect connection, the company can dedicate a portion of its network bandwidth to transferring data to Amazon S3, ensuring timely backups while minimizing the impact on internal users.

upvoted 1 times

 **SilentMilli** 10 months, 3 weeks ago

Selected Answer: B

Establishing a new AWS Direct Connect connection and directing backup traffic through this new connection would meet these requirements. AWS Direct Connect is a network service that provides dedicated network connections from on-premises data centers to AWS. It allows the company to bypass the public Internet and establish a direct connection to AWS, providing a more reliable and lower-latency connection for data transfer. By directing backup traffic through the Direct Connect connection, the company can reduce the impact on internet connectivity for internal users and improve the speed of backups to Amazon S3. This solution would provide a long-term solution for timely backups with minimal impact on internet connectivity.

upvoted 4 times

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** Highly Voted 1 year, 1 month 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 50 times

 **cookieMr** Highly Voted 5 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 7 times

 **MoshiurGCP** Most Recent 1 week, 1 day ago

Prevent accidental deletion - MFA, Versioning

upvoted 1 times

 **Marco_St** 2 weeks, 3 days ago

Selected Answer: AB

MFA will add extra security of deleting item from s3

Versioning will make the data recovering

upvoted 1 times

 **JustEugen** 3 weeks, 4 days 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 weeks, 1 day 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

 **Ruffyit** 1 month ago

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-audit-deleted-missing-objects/>
upvoted 1 times

 **AWSStudyBuddy** 1 month, 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** 1 month, 2 weeks ago

A+B is the correct answer
upvoted 1 times

 **Tralfalgarlaw** 1 month, 2 weeks ago

Selected Answer: AB

Keyword: accidental deletions
upvoted 1 times

 **tom_cruise** 1 month, 2 weeks ago

Selected Answer: A

D has nothing to do with deletion, not sure why it is even shown as correct answer?
upvoted 1 times

 **awashenko** 1 month, 3 weeks ago

Selected Answer: AB

Agree A and B. D doesn't do anything for deletion. E helps more with deleting objects. C is more about access control than deletion.
upvoted 1 times

 **paniya93** 1 month, 4 weeks ago

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 1 times

 **Guru4Cloud** 3 months, 3 weeks ago

Selected Answer: AB

Enable versioning on the S3 bucket. This will create a history of all object versions in the bucket, including deleted objects. This way, even if an object is deleted, it can be restored from a previous version.
Enable MFA Delete on the S3 bucket. This will require users to enter their MFA token in addition to their password in order to delete objects from the bucket. This adds an extra layer of protection against accidental deletion.
upvoted 2 times

 **TariqKipkemei** 3 months, 3 weeks ago

Selected Answer: AB

Enable versioning to ensure restore is possible, Enable two step verification of file deletion using MFA delete to ensure unwanted persons are unable to perform this action.
upvoted 1 times

 **Bill_** 3 months, 4 weeks ago

AB is the correct answer.
Admin please don't make us fail the exam 😱
upvoted 4 times

 **miki111** 4 months, 2 weeks ago
Option AB is the right answer.
upvoted 2 times

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.)

- Deploy the Lambda function in multiple Availability Zones.
- Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic.
- Increase the CPU and memory that are allocated to the Lambda function.
- Increase provisioned throughput for the Lambda function.
- Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue.

Correct Answer: BE

Community vote distribution

BE (97%)

✉  **Incognito013** Highly Voted 1 year, 1 month 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 22 times

✉  **Oluseun** 8 months, 3 weeks 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, 1 month ago

Selected Answer: BE

BE so that the lambda function reads the SQS queue and nothing gets lost

upvoted 8 times

✉  **OmegaLambda7XL9** Most Recent 1 week, 5 days 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 1 times

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

Selected Answer: BE

Key: network connectivity issues

upvoted 1 times

✉  **awashenko** 1 month, 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** 3 months, 2 weeks ago

B and E , the FAN out model , SQS will help to retrive the work and delayed processing

upvoted 1 times

✉  **Guru4Cloud** 3 months, 3 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** 3 months, 3 weeks ago

Selected Answer: BE

BE is most logical answer.

upvoted 1 times

 **miki111** 4 months, 2 weeks ago

Option BE is the right answer.

upvoted 1 times

 **cookieMr** 5 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** 5 months, 4 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** 8 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** 9 months, 2 weeks ago

Help

Can SQS Queue have multiple consumers so SNS and Lambda can consume at the same time?

upvoted 1 times

 **Lonojack** 10 months 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 the connectivity so maybe it will be less likely to lose connectivity and fail in the first place?

upvoted 2 times

 **ProfXsamson** 9 months, 3 weeks ago

What does connectivity have to do with Provisioned IOPS which is supposed to enhance I/O rate?

upvoted 2 times

 **SilentMilli** 10 months, 3 weeks 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

 **pazabal** 11 months, 1 week ago

Selected Answer: BE

B and E, allow the data to be queued up in the event of a failure, rather than being lost, then by reading from the queue, the Lambda function will be able to process the data

A, improves reliability but doesn't ensure all data is ingested

C and D, they improve performance but not ensure all data is ingested

upvoted 3 times

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*

B (58%)

D (42%)

✉️  **Gatt**  1 year 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 26 times

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

Yes. Why should we be concerned about the LEAST development effort if we can't even accomplish what the clients asked? I know that B is more efficient in terms of development effort, but you should prioritize your clients' requests.

upvoted 1 times

✉️  **dodino** 1 week, 5 days ago

D is not correct because it mentions SES, not SNS.

upvoted 1 times

✉️  **acuaws** 7 months, 2 weeks ago

the problem is... you'd have to write lambda to detect PII? AWS has a product for that and we know that's Macie

upvoted 8 times

✉️  **Maxpayne009** 7 months ago

Macie has file size limit and clearly the question mentions 200GB file sizes are possible. Lambda is the way to go ..

upvoted 5 times

✉️  **grzeev**  1 year 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 15 times

✉️  **grzeev** 1 year 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 9 times

✉️  **MoshiurGCP**  1 week, 1 day ago

Amazon Macie to scan the object

upvoted 1 times

✉️  **xdkonorek2** 4 weeks, 1 day ago

Selected Answer: D

B is incorrect because Macie can't process such big files

upvoted 1 times

✉ **Eneiss** 1 month 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

✉ **Ruffyit** 1 month 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** 1 month, 1 week 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** 1 month, 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

✉ **tom_cruise** 1 month, 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

✉ **RSavio** 1 month, 3 weeks ago

Option A, while using Amazon S3 and Amazon inspector, doesn't provide as specialized PP 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

✉ **awashenko** 1 month, 3 weeks ago

Selected Answer: B

Amazon Macie discovers sensitive data using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks.

upvoted 1 times

✉ **KarthikRock25** 2 months ago

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.

upvoted 2 times

✉ **Its_SaKar** 2 months ago

Selected Answer: B

PII = Macie
upvoted 2 times

 **axelrodb** 2 months, 2 weeks ago

Selected Answer: B
B is the correct answer
upvoted 1 times

 **RNess** 2 months, 3 weeks ago

Selected Answer: B
AWS Macie
• Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.
• Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII)
upvoted 1 times

 **Chiquitabandita** 2 months, 3 weeks ago

the file size and the automate remediation part cancels out B and makes the best choice out of these to be D I think.
upvoted 2 times

 **Fakhrudin** 2 months, 4 weeks ago

AWS has macie to discovers PII, that's true. But also stated that sometimes, the files reach up to 200 GB. Please note that for files, Amazon macie can only process uncompressed file up to 10 GB. So, I think it's D
<https://docs.aws.amazon.com/macie/latest/user/macie-quotas.html>
upvoted 1 times

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 Highly Voted 1 year, 1 month ago

Reserved instances are for long term so on-demand will be the right choice - Answer D
upvoted 22 times

Buruguduystunstugudunstuy Highly Voted 11 months, 2 weeks 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 16 times

BlueVolcano1 10 months, 1 week 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 16 times

MoshiurGCP Most Recent 1 week, 1 day ago

Guarantee capacity on 3 AZ - on demand reservation, specify region & Availability Zone
upvoted 1 times

Ruffyit 1 month 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 1 month, 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 3 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 3 months, 3 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** 4 months, 2 weeks ago

Option D is the right answer.

upvoted 1 times

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

Reserved instances is for long term

On-demand Capacity reservation enables you to choose specific AZ for any duration

upvoted 1 times

 **Eden** 8 months, 2 weeks ago

Just for 1 week so D on demand

upvoted 1 times

 **killbots** 8 months, 2 weeks 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** 9 months, 3 weeks 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** 10 months, 1 week 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** 10 months, 3 weeks 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

 **pazabal** 11 months, 1 week ago

Selected Answer: D

D, specify the number of instances and AZs for a period of 1 week and then use them whenever needed.

A and C, aren't designed to provide guaranteed capacity

B, doesn't guarantee that EC2 capacity will be available in the three specific AZs

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

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

D (92%)	8%
---------	----

✉  **Six_Fingered_Jose** Highly Voted 1 year, 1 month 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 33 times

✉  **Fakhrudin** 2 months, 4 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 3 times

✉  **rajendradba** Highly Voted 1 year, 1 month ago

Selected Answer: D

ElastiCache is in Memory, EFS is for durability
upvoted 15 times

✉  **Ruffyit** Most Recent 1 month 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

✉  **awashenko** 1 month, 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 2 times

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

Selected Answer: D

EFS is most durable solution

upvoted 1 times

✉  **Fakhrudin** 2 months, 4 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** 3 months 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** 3 months, 2 weeks 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 3 times

Guru4Cloud 3 months, 3 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 3 months, 3 weeks ago

Selected Answer: D

Highly available and durable = Elastic File System (Amazon EFS)

upvoted 1 times

miki111 4 months, 2 weeks ago

Option D is the right answer.

upvoted 1 times

unhinged22 4 months, 4 weeks ago

Selected Answer: A

By default, the data in a Redis node on ElastiCache resides only in memory and isn't persistent. If a node is rebooted, or if the underlying physical server experiences a hardware failure, the data in the cache is lost.

If you require data durability, you can enable the Redis append-only file feature (AOF). When this feature is enabled, the node writes all of the commands that change cache data to an append-only file. When a node is rebooted and the cache engine starts, the AOF is "replayed." The result is a warm Redis cache with all of the data intact.

AOF is disabled by default. To enable AOF for a cluster running Redis, you must create a parameter group with the appendonly parameter set to yes. You then assign that parameter group to your cluster. You can also modify the appendfsync parameter to control how often Redis writes to the AOF file.

upvoted 4 times

unhinged22 4 months, 4 weeks ago

Selected Answer: A

Is Redis durable?

Durable Redis Persistence Storage | Redis Enterprise

Redis Enterprise is a fully durable database that serves all data directly from memory, using either RAM or Redis on Flash.

upvoted 1 times

aadityaravi8 5 months, 1 week ago

Amazon Elastic File System (Amazon EFS) provides a scalable and durable file storage service that can be mounted on multiple EC2 instances simultaneously. By moving the catalog to an EFS file system, the data will be stored in a durable location with built-in redundancy. It will also be accessible from multiple EC2 instances, ensuring high availability.

upvoted 1 times

cookieMr 5 months, 1 week ago

Selected Answer: D

Option A is not suitable for storing the catalog as ElastiCache is an in-memory data store primarily used for caching and cannot provide durable storage for the catalog.

Option B would not address the requirement for high availability or durability. Instance stores are ephemeral storage attached to EC2 instances and are not durable or replicated.

Option C would provide durability but not high availability. S3 Glacier Deep Archive is designed for long-term archival storage, and accessing the data from Glacier can have significant retrieval times and costs.

Therefore, option D is the most suitable choice to ensure high availability and durability for the company's catalog.

upvoted 3 times

Bmarodi 5 months, 4 weeks ago

Selected Answer: A

Option A meets the requirements.

upvoted 1 times

Rahulbit34 7 months ago

ElastiCache is using cache functionality. EFS is for durability.

upvoted 1 times

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

B (70%)	C (21%)	6%
---------	---------	----

✉  **masetromain**  1 year, 1 month 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 37 times

✉  **ssoffline** 6 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

✉  **IngenieriaEGlobal** 1 month, 3 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 99.99999999% durability, and offers the same low latency and high throughput performance of S3 Standard

upvoted 2 times

✉  **RupeC** 4 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

✉  **MutiverseAgent** 4 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 1 times

✉  **sachin** 9 months 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** 9 months, 1 week 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** 8 months, 2 weeks ago

it doesnt say predictable, it says files are accessed random. Random = Unpredictable. Answer is B
upvoted 6 times

✉ **Lilibell** Highly Voted 1 year, 1 month ago

The answer is B
upvoted 12 times

✉ **wantu** Most Recent 19 hours, 59 minutes ago

Selected Answer: B

os 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 1 times

✉ **xogete** 1 week, 5 days 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** 2 weeks, 3 days 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 1 times

✉ **SAA463** 4 weeks, 1 day ago

I think the answer is C is cost effective
upvoted 1 times

✉ **ACloud_Guru15** 1 month, 2 weeks 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** 1 month, 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** 1 month, 3 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

✉ **awashenko** 1 month, 3 weeks ago

Selected Answer: B

So for me it came down to B and D. I choose B because of this statement "Users access the files randomly within 1 year of the call" Had it said they access the files all the time on a regular basis for the first year, I would have went with D but because they access those files at random I think B is the better choice.
upvoted 1 times

✉ **awashenko** 1 month, 3 weeks ago

Although, now that I'm thinking about it. S3 is cheaper than RDS so C would have been the better choice if that statement wasn't there.
upvoted 1 times

 **ABS_AWS** 2 months ago

Correct answer is C

As B has got Athena mentioned which is not fit as per question.

upvoted 2 times

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

"For archive data that needs immediate access, such as medical images, news media assets, or genomics data, choose the S3 Glacier Instant Retrieval storage class, an archive storage class that delivers the lowest cost storage with milliseconds retrieval. For archive data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases, choose S3 Glacier Flexible Retrieval (formerly S3 Glacier), with retrieval in minutes or free bulk retrievals in 5-12 hours." <https://aws.amazon.com/about-aws/whats-new/2021/11/amazon-s3-glacier-instant-retrieval-storage-class/>

upvoted 1 times

 **benacert** 2 months, 3 weeks ago

B is the right answer..

upvoted 1 times

 **Wayne23Fang** 2 months, 3 weeks ago

Selected Answer: C

The question is about Cost-effective. Athena search of S3 is probably too much. It cost at least 2.5 times of simple S3 Sql query.

upvoted 1 times

 **Syruis** 3 months, 2 weeks ago

Selected Answer: C

C and not B just because Athena will be costly.

upvoted 4 times

 **Yonimoni** 3 months, 1 week ago

Exactly what i thought

upvoted 1 times

 **Guru4Cloud** 3 months, 3 weeks ago

Selected Answer: B

I would recommend option B.

The key reasons are:

S3 Intelligent-Tiering automatically moves files between frequent and infrequent access tiers based on actual access patterns, optimizing cost. Lifecycle policies can move older files to Glacier Flexible Retrieval after 1 year, which has higher latency and lower cost than S3.

Athena allows querying the metadata of files in S3 without retrieving the files themselves.

Glacier Select can directly query files in Glacier without needing to restore the entire file.

upvoted 2 times

 **TariqKipkemei** 3 months, 3 weeks ago

Selected Answer: B

Users access the files randomly = Amazon S3 Intelligent-Tiering

Users access the files infrequently = S3 Glacier Flexible Retrieval

Ability to query files as quickly as possible = Amazon Athena, S3 Glacier Select

upvoted 2 times

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 (70%)

B (30%)

✉️  **tinyfoot** Highly Voted 1 year 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 43 times

✉️  **Fakhrudin** 2 months, 4 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 3 times

✉️  **Shasha1** Highly Voted 11 months, 2 weeks 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 19 times

✉️  **MoshiurGCP** Most Recent 1 week, 1 day ago

Third party software - Custom command.

upvoted 1 times

✉️  **bnagaraja9099** 4 weeks, 1 day 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** 1 month, 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** 1 month, 2 weeks ago

Selected Answer: D

Key: third-party software and run custom command
upvoted 2 times

 **poponpo** 1 month, 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** 2 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]** 2 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** 1 month, 2 weeks ago

Not true it patches Linux too
upvoted 1 times

 **Abdou1604** 3 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** 3 months, 3 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 3 times

 **TariqKipkemei** 3 months, 3 weeks ago

Selected Answer: B

Technically both 'Patch Manager' and 'Run Command' would work. But the patch manager was built specifically to apply patches for both operating systems and applications.

upvoted 2 times

 **johne42** 3 months, 1 week 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

 **miki111** 4 months, 2 weeks ago

Option D is the right answer.
upvoted 1 times

 **cookieMr** 5 months, 1 week ago

Selected Answer: B

SSM Patch Manager offers a centralized and automated approach to patch management, allowing administrators to efficiently manage patching operations across a large number of instances. It provides features such as patch compliance reporting and ability to specify maintenance windows to control timing of patch installations.

A suggests using an Lambda to apply the patch. It requires additional development effort to create and manage it, handle error handling and retries, and scale solution appropriately to handle a large number of instances.

C suggests scheduling an SSM maintenance window. While it can be used to orchestrate patching activities, they may not provide fastest patching time for all instances, as execution is scheduled within defined maintenance window timeframe.

D suggests using Run Command to run a custom command for patching. While it can be used for executing commands on multiple instances, it requires manual execution and may not provide the scalability and automation capabilities that Patch Manager offers.

upvoted 2 times

✉️ **Clouddon** 3 months, 3 weeks ago

I found this: Patch Manager controls the deployment of updates to operating system and 3rd party applications (ONLY Microsoft) on network endpoints.<https://aws.amazon.com/about-aws/whats-new/2019/05/aws-systems-manager-patch-manager-supports-microsoft-application-patching/>

upvoted 2 times

✉️ **Clouddon** 3 months, 3 weeks ago

Is it true that Patch Manager is not designed to apply third-party software patches?

upvoted 1 times

✉️ **konieczny69** 5 months, 2 weeks ago

Selected Answer: D

answer D

keyword - The workload is powered by third-party software

patch manager patches AWS managed nodes OSs

we don't know what is running on the ec2 and what kind of vulnerability is that

upvoted 1 times

✉️ **Abrar2022** 6 months, 2 weeks ago

Since it's a third-party application then use custom command to apply patches manually on all EC2's.

upvoted 1 times

✉️ **AlaTaftaf** 7 months ago

Selected Answer: B

Answer of ChatGPT: "To remediate the critical security vulnerability in the third-party software running on 1,000 Amazon EC2 instances, the most appropriate solution is to use AWS Systems Manager Patch Manager to apply the patch to all instances. AWS Systems Manager Patch Manager automates the process of patching instances across hybrid environments and reduces the time and effort required to patch instances. Patch Manager enables administrators to select and approve patches for automatic deployment to instances in a controlled and secure manner. The patching process can be scheduled, tracked, and automated using Patch Manager, which also provides compliance reporting and dashboards. By using Patch Manager, the solutions architect can quickly and efficiently patch all EC2 instances and ensure that the workload remains secure."

upvoted 2 times

✉️ **jzam123** 6 months, 2 weeks ago

okay here, ChatGPT is insanely inaccurate, when I ask ChatGPT a question on this

I first copy paste the question, then I write "the correct answer is [whatever the correct answer determined by the discussion]"

Then I get correct information on why the other answer choices are wrong and why the correct answer choice is correct

upvoted 3 times

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

BD (65%)	DE (18%)	Other
----------	----------	-------

✉️  **whosawsome**  1 year, 1 month 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 25 times

✉️  **apchandana** 8 months 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 3 times

✉️  **Clouddon** 3 months, 3 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 1 times

✉️  **backbencher2022**  1 year 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 19 times

✉️  **slimen** 4 weeks, 1 day ago

the daily schedule can be achieve with event bridge

- schedule and event bridge to trigger daily
- the event briode 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

✉️  **RupeC** 4 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 1 times

✉️  **MoshiurGCP**  1 week, 1 day ago

Key: Send email every morning same time - 1. Simple email 2. AWS Event Bridge with lambda

upvoted 1 times

✉️  **wearrexdzw3123** 2 weeks, 3 days 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** 1 month ago

Selected Answer: BD

Key: retrieval by a REST API, that's why use lambda

upvoted 1 times

✉️ **tom_cruise** 1 month, 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 3 times

✉️ **David_Ang** 2 months 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 1 times

✉️ **hieulam** 2 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** 2 months, 1 week 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** 3 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 1 times

✉️ **miki111** 4 months, 1 week ago

Option BD is the correct answer

upvoted 1 times

✉️ **miki111** 4 months, 2 weeks ago

Option BD is the right answer.

upvoted 1 times

✉️ **RupeC** 4 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** 4 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** 4 months, 3 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

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

A: NOT (Firehose not needed here)

B: NOT (SES supports HTML but does NOT explicitly format data)

D: YES (Schedule process, extract & format)

E: YES (Save emails in S3 for further reference, Send email)

upvoted 4 times

✉️ **Dhaysindhu** 5 months ago

Selected Answer: DE

D: To schedule the event every morning and format the HTML

E: To store the HTML in S3 and send the email using SNS

upvoted 1 times

✉️ **Mia2009687** 5 months ago

Selected Answer: DE

SES cannot format the data.

upvoted 1 times

 **cookieMr** 5 months, 1 week ago

Selected Answer: BD

D: Create an EventBridge (CloudWatch Events) scheduled event that invokes Lambda to query API for data. This scheduled event can be set to trigger at desired time every morning to fetch shipping statistics from API.

B: Use SES to format data and send report by email. In Lambda, after retrieving shipping statistics, you can format data into an easy-to-read HTML format using any HTML templating framework.

Options A, C, and E are not necessary for achieving the desired outcome. Option A is typically used for real-time streaming data ingestion and delivery to data lakes or analytics services. Glue (C) is a fully managed extract, transform, and load (ETL) service, which may be an overcomplication for this scenario. Storing the application data in S3 and using SNS (E) can be an alternative approach, but it adds unnecessary complexity.

upvoted 2 times

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** Highly Voted 1 year, 1 month ago

Selected Answer: C

EFS is a standard file system, it scales automatically and is highly available.
upvoted 23 times

✉  **masetromain** Highly Voted 1 year, 1 month 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** 9 months, 2 weeks 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 1 times

✉  **RBSK** 11 months, 3 weeks ago

None meets 100s of TB / file. Bit confusing / misleading

upvoted 3 times

✉  **JayBee65** 11 months, 4 weeks ago

S3 and EBS are block storage but you are looking to store files, so EFS is the correct option.

upvoted 1 times

✉  **OmegaLambda7XL9** 1 week, 4 days ago

A lil correction,S3 is Object storage not Block Storage

upvoted 1 times

✉  **Ello2023** 10 months, 2 weeks ago

S3 is object storage.

upvoted 11 times

✉  **wantu** Most Recent 19 hours, 48 minutes ago

Selected Answer: C

Palabras clave: autoescalado y ficheros
upvoted 1 times

 **leosmal** 4 days, 15 hours ago

The key is Multi-AZ ,EBS does not support it.
upvoted 1 times

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

Option C is the correct answer
upvoted 1 times

 **cookieMr** 5 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** 5 months, 3 weeks ago

Selected Answer: C

Option C meets the requirements.
upvoted 1 times

 **joshnort** 7 months ago

Selected Answer: C

Keywords: file system structure, scales automatically, highly available, and minimal operational overhead
upvoted 1 times

 **harirkmusa** 9 months, 2 weeks 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** 10 months 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** 10 months, 3 weeks 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** 10 months, 3 weeks 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

 **pazabal** 11 months, 1 week ago

Selected Answer: C

C = File storage system, Multi AZ ASG lets you maintain high availability
Not A, B or D because they don't meet the requirement of file system storage
upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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.

To meet the requirements, a solution that would allow the company to migrate its on-premises application to AWS and scale automatically, be highly available, and require minimum operational overhead would be to migrate the application to Amazon Elastic Compute Cloud (Amazon EC2) instances in a Multi-AZ (Availability Zone) Auto Scaling group.

upvoted 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

The Auto Scaling group would allow the application to automatically scale up or down based on demand, ensuring that the application has the required capacity to handle incoming requests. To store the data produced by the application, the company could use Amazon Elastic File System (Amazon EFS), which is a file storage service that allows the company to store and access file data in a standard file system structure. Amazon EFS is highly available and scales automatically to support the workload of the application, making it a good choice for storing the data produced by the application.

upvoted 2 times

 **Futurebones** 6 months, 3 weeks ago

my only question is : since EFS is also highly available and scalable, why not use EFS alone in this case? Is there any suggestion for using Auto Scaling as a must.

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C. Using EBS as storage is not a right option as it will not scale automatically.

Using ECS and EKS for running the application is not a requirement here and it is not clearly mentioned that application can be containerized or not.

upvoted 2 times

 **benaws** 11 months, 3 weeks ago

Selected Answer: C

Highly available & Autoscales == Multi-AZ Auto Scaling group.

Standard File System == Amazon Elastic File System (Amazon EFS)

upvoted 3 times

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%)

 **Ruffyit** 1 month 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 2 times

 **axelrodb** 2 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 2 times

 **Guru4Cloud** 3 months, 3 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 2 times

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

Option C is the correct answer

upvoted 2 times

 **MutiverseAgent** 4 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** 1 month, 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** 5 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 7 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 8 months, 3 weeks 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

Whericanstart 9 months ago

Selected Answer: C

S3 Glacier Deep Archive all day....

upvoted 1 times

SilentMilli 10 months, 3 weeks 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 11 months, 1 week 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 11 months, 1 week 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

Burugudystunstugudunstuy 11 months, 1 week 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

Burugudystunstugudunstuy 11 months, 1 week 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 11 months, 2 weeks 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** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **Marge_Simpson** 11 months, 3 weeks ago

Selected Answer: C

They should've put Glacier Vault Lock into Option C to make it even more obvious

upvoted 1 times

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 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 13 times

✉  **Buruguduystunstugudunstuy** Highly Voted 1 year ago

Selected Answer: C

Windows file shares = Amazon FSx for Windows File Server

Hence, the correct answer is C

upvoted 6 times

✉  **Buruguduystunstugudunstuy** 11 months, 1 week 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

✉  **Ruffyit** Most Recent 1 month ago

<https://aws.amazon.com/fsx/windows/faqs/>

Thousands of compute instances and devices can access a file system concurrently.

upvoted 1 times

✉  **AWSStudyBuddy** 1 month, 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** 3 months, 3 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** 3 months, 3 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** 4 months, 1 week ago

Option C is the correct answer
upvoted 1 times

✉ **cookieMr** 5 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** 7 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** 7 months, 1 week ago

Selected Answer: C

C is correct. Amazon FSx for Windows File Server.

upvoted 3 times

✉ **satosis** 7 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** 7 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** 10 months, 3 weeks 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** 11 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

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

Selected Answer: D

The best option to meet the requirements specified in the question is option 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.

Amazon EFS is a fully managed, elastic file storage service that scales on demand. It is designed to be highly available, durable, and secure, making it well-suited for hosting file shares. By using a Multi-AZ configuration, the file share will be automatically replicated across multiple Availability Zones, providing high availability and durability for the data.

To migrate the data, you can use a variety of tools and techniques, such as Robocopy or AWS DataSync. Once the data has been migrated to EFS, you can simply update the file share configuration on the existing EC2 instances to point to the EFS file system, and users will be able to access the files in the same way they currently do.

upvoted 1 times

 **Ello2023** 10 months, 2 weeks ago

EFS is not support by windows.
upvoted 4 times

 **Buruguduystunstugudunstuy** 9 months ago

You're 100% right Ello2023. I humbly acknowledged my first answer was WRONG. I am changing my answer. "The correct answer is Option 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.

upvoted 6 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Option A, migrating all the data to Amazon S3 and setting up IAM authentication for user access, would not preserve the current file share access methods and would require users to access the files in a different way.

Option B, setting up an Amazon S3 File Gateway, would not provide the high availability and durability needed for hosting file shares.

Option C, extending the file share environment to FSx for Windows File Server, would provide the desired high availability and durability, but would also require users to access the files in a different way.

upvoted 3 times

 **ronaldchow** 11 months, 1 week ago

EFS is for Linux only not Windows
upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months ago

You're right Ronald Chow. Thanks! Option D is incorrect because Amazon Elastic File System (EFS) is a file storage service that is not natively compatible with the Windows operating system, and would not preserve the existing access methods for users.

I am taking back my answer. "The correct answer is Option 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.

upvoted 6 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **Shasha1** 11 months, 2 weeks ago

D

Amazon EFS is fully compatible with the SMB protocol that is used by Windows file shares, which means that users can continue to access the files in the same way they currently do. Extending the file share environment to FSx for Windows File Server with a Multi-AZ configuration would not be a suitable solution, as FSx for Windows File Server is not as scalable or cost-effective as Amazon EFS.

upvoted 1 times

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 DB 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** Highly Voted 1 year, 1 month ago

Selected Answer: C

- A: doesn't fully configure the traffic flow
- B: security groups don't have deny rules
- C: peering is mostly between VPCs, doesn't really help here

answer is C, most mainstream way

upvoted 37 times

 **Gary_Phllips_2007** Highly Voted 9 months ago

Just took the exam today and EVERY ONE of the questions came from this dump. Memorize it all. Good luck.

upvoted 17 times

 **orhan64** 4 months ago

Hey bro, did you buy premium access?

upvoted 3 times

 **AWSStudyBuddy** Most Recent 1 month, 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** 3 months, 3 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 1 times

 **TariqKipkemei** 3 months, 3 weeks ago

Selected Answer: C

Security groups only have allow rules

upvoted 1 times

 **praveenvky83** 3 months, 4 weeks ago

Selected Answer: C

option C
upvoted 1 times

✉ **miki111** 4 months, 1 week ago

Option C is the correct answer
upvoted 1 times

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

Selected Answer: C

Option C meets the requirements.
upvoted 1 times

✉ **Abrar2022** 6 months, 2 weeks 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** 7 months ago

Selected Answer: C

CCCCCCCCCC
upvoted 1 times

✉ **SilentMilli** 10 months, 3 weeks 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

✉ **Burugduystunstugudunstuy** 11 months, 1 week 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

✉ **Burugduystunstugudunstuy** 11 months, 1 week 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** 11 months, 2 weeks 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 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 ago

C is correct

upvoted 1 times

 **17Master** 1 year ago

Selected Answer: C

Ans correct.

upvoted 2 times

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

 **Buruguduystunstugudunstuy** Highly Voted  11 months, 1 week 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 31 times

 **t0nx** 1 week, 1 day ago

Why the "reveal solution" most of the time gives the wrong answer ?

upvoted 1 times

 **aadityaravi8** 5 months ago

google bard reply..

upvoted 3 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 5 times

 **masetromain** Highly Voted  1 year, 1 month 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 28 times

✉️ **MutiverseAgent** 4 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

✉️ **Valero_** 1 year, 1 month 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

✉️ **luongtrann** Most Recent ⓘ 1 month, 1 week ago

Selected Answer: C

Correct answer

upvoted 1 times

✉️ **Abitek007** 1 month, 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 1 times

✉️ **Abitek007** 1 month, 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 1 times

✉️ **paniya93** 1 month, 4 weeks ago

Selected Answer: C

Explain why this saying a different region which not mentioned in the Q.

upvoted 1 times

✉️ **Hassao0** 3 months 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 1 times

✉️ **Guru4Cloud** 3 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 HTTPS

upvoted 1 times

✉️ **TariqKipkemei** 3 months, 3 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** 4 months, 1 week ago

Option C is the correct answer

upvoted 1 times

✉️ **cookieMr** 5 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 2 times

✉ **Bmarodi** 5 months, 3 weeks ago

Selected Answer: C

I switch to option C too, which meets the requirements.

upvoted 1 times

✉ **Bmarodi** 5 months, 3 weeks ago

Selected Answer: D

I vote for option D.

upvoted 1 times

✉ **dydzah** 6 months, 1 week ago

<https://www.youtube.com/watch?v=Ro0rgeLDkO4>

upvoted 1 times

✉ **Siva007** 6 months, 2 weeks ago

Selected Answer: C

C: It should be in the same Region

upvoted 1 times

✉ **linux_admin** 8 months ago

Selected Answer: C

In this scenario, the goal is to design the API Gateway URL with the company's domain name and corresponding certificate so that third-party services can use HTTPS. To accomplish this, a solutions architect should create a Regional API Gateway endpoint and associate it with the company's domain name. The public certificate associated with the company's domain name should be imported into AWS Certificate Manager (ACM) in the same Region as the API Gateway endpoint. The certificate should then be attached to the API Gateway endpoint to enable HTTPS. Finally, Route 53 should be configured to route traffic to the API Gateway endpoint.

upvoted 2 times

✉ **gmehra** 8 months, 3 weeks ago

ACM is always in US east 1

upvoted 2 times

✉ **cosmiccliff** 3 weeks, 6 days ago

"No. ACM certificates must be in the same Region as the resource where they are being used. The only exception is Amazon CloudFront, a global service that requires certificates in the US East (N. Virginia) region."

<https://aws.amazon.com/certificate-manager/faqs/#:~:text=No.%20ACM%20certificates,for%20that%20distribution.>

upvoted 1 times

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%)

 **masetromain** Highly Voted 1 year, 1 month ago

Selected Answer: B

Good Answer is B :

<https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html?pg=In&sec=ft>

upvoted 13 times

 **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 12 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 9 times

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

Selected Answer: B

comprehend is for NLP

sagemaker is for training and deploying ML and AI models

deploying cutom models using fargate requires time and development effort wich is not recommended by the question

upvoted 1 times

 **Ruffyit** 1 month ago

<https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html?pg=In&sec=ft>

upvoted 1 times

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

Selected Answer: B

B is the best solution as far

upvoted 1 times

✉ **Guru4Cloud** 3 months, 3 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** 3 months, 3 weeks ago

Selected Answer: B

Amazon Rekognition to the rescue...whooosh!

upvoted 1 times

✉ **cookieMr** 5 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** 8 months, 2 weeks 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** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

✉ **Shasha1** 11 months, 2 weeks 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 ago

B is correct

upvoted 1 times

✉ **ArielSchivo** 1 year, 1 month ago

Selected Answer: B

Option B.

<https://docs.aws.amazon.com/rekognition/latest/dg/a2i-rekognition.html>

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 21 times

 **Ruffyit** Most Recent 1 month 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** 1 month, 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** 2 months, 2 weeks ago

Option C is the correct answer.

upvoted 1 times

 **Syruis** 3 months, 2 weeks ago

Selected Answer: C

C for Fargate

upvoted 1 times

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

Option C is the correct answer

upvoted 1 times

 **cookieMr** 5 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 4 times

 **cheese929** 7 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** 10 months, 3 weeks ago

Selected Answer: C

ECS + Fargate

upvoted 3 times

 **gustavtd** 11 months ago

Selected Answer: C

AWS Fargate will hide all the complexity for you

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **benaws** 11 months, 3 weeks ago

Selected Answer: C

Obviously anything with EC2 in the answer is wrong...

upvoted 1 times

 **ashish_t** 1 year 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 ago

C is correct

upvoted 1 times

 **PS_R** 1 year ago

Selected Answer: C

Agree Serverless Containerization Think Fargate

upvoted 2 times

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

D (88%)	12%
---------	-----

✉  **Burugduystunstugudunstuy** Highly Voted 11 months, 1 week 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 18 times

✉  **Burugduystunstugudunstuy** 11 months, 1 week 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 4 times

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

The question does not say that real-time is needed here

upvoted 3 times

✉  **ArielSchivo** Highly Voted 1 year, 1 month 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** 11 months, 4 weeks 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 2 times

✉  **Reckless_Jas** Most Recent 3 months, 1 week ago

when you see clickstream data, think about Kinesis Data Stream

upvoted 4 times

✉ **Guru4Cloud** 3 months, 3 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** 4 months, 1 week ago

Option D is the correct answer

upvoted 1 times

✉ **cookieMr** 5 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** 7 months ago

Clickstream is the key - Answer is D

upvoted 1 times

✉ **PaoloRoma** 8 months, 1 week ago

Selected Answer: A

I am going to be unpopular here and I'll go for A). Even if here 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** 4 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** 1 month, 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

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉ **studis** 11 months, 2 weeks 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

✉ **sebasta** 12 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** 11 months, 3 weeks 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 2 times

 **Wpcorgan** 1 year ago

D is correct

upvoted 1 times

 **PS_R** 1 year ago

Click Stream & Analyse/ process- Think KDS,

upvoted 2 times

 **BoboChow** 1 year, 1 month ago

Selected Answer: D

D seems to make sense

upvoted 4 times

 **JesseeS** 1 year, 1 month ago

Option D is correct... See the resource. Thank you Ariel

upvoted 1 times

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%)

✉  **Burugudystunstugudunstuy** Highly Voted 11 months, 1 week 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 15 times

✉  **Burugudystunstugudunstuy** 11 months, 1 week 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 13 times

✉  **masetromain** Highly Voted 1 year, 1 month 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 13 times

✉  **Ruffyit** Most Recent 1 month ago

C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.

upvoted 1 times

✉  **AWSStudyBuddy** 1 month, 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 1 times

✉  **Tom123456ac** 1 month, 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 1 times

✉  **Guru4Cloud** 3 months, 3 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 5 times

 **miki111** 4 months, 1 week ago

Option C is the correct answer

upvoted 1 times

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

A solutions architect should create listen rules to direct http traffic to https.

upvoted 1 times

 **cheese929** 7 months, 2 weeks ago

Selected Answer: C

C is correct. Traffic redirection will solve it.

upvoted 2 times

 **elearningtakai** 8 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** 8 months, 3 weeks 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** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **Shasha1** 11 months, 2 weeks 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 ago

C is correct

upvoted 1 times

 **hanhdroid** 1 year, 1 month ago

Selected Answer: C

Answer C: <https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/>

upvoted 4 times

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** Highly Voted 1 year, 1 month ago

Selected Answer: C

Secrets manager supports Autorotation unlike Parameter store.
upvoted 18 times

✉️  **JesseeS** 1 year, 1 month ago

Parameter store does not support autorotation.
upvoted 8 times

✉️  **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 10 times

✉️  **Buruguduystunstugudunstuy** 11 months, 1 week 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 5 times

✉️  **dumpsowner** Most Recent 1 month ago

100% valid dumps i found this site <https://www.linkedin.com/company/amazon-dumps/?viewAsMember=true>
upvoted 1 times

✉️  **Ruffyit** 1 month 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** 3 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 3 months, 3 weeks ago

Selected Answer: C

Key Autorotation = AWS Secrets Manager

upvoted 1 times

miki111 4 months, 1 week ago

Option C is the right answer.

upvoted 1 times

cookieMr 5 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 5 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 6 months, 1 week ago

Selected Answer: C

My choice is c.

upvoted 1 times

AndyMartinez 9 months, 3 weeks ago

Selected Answer: C

The right option is C.

upvoted 1 times

Adios_Amigo 10 months ago

C is the most correct answer. Automatic replacement must be performed by the secret manager.

upvoted 1 times

career360guru 11 months, 2 weeks 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 ago

C is correct

upvoted 2 times

BoboChow 1 year, 1 month ago

Selected Answer: C

AWS Secrets Manager is a newer service than SSM Parameter store

upvoted 3 times

ArielSchivo 1 year, 1 month ago

Selected Answer: C

Option C.

https://docs.aws.amazon.com/secretsmanager/latest/userguide/create_database_secret.html

upvoted 3 times

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 (93%)	7%
---------	----

✉  **Sinaneos** Highly Voted 1 year, 1 month 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 36 times

✉  **mabotega** Highly Voted 1 year 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 17 times

✉  **xdkonorek2** Most Recent 3 weeks, 5 days 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

✉  **Ruffyit** 1 month 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** 2 months, 3 weeks ago

answer is D

upvoted 1 times

✉  **Guru4Cloud** 3 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** 4 months, 1 week ago

Option D is the right answer.

upvoted 2 times

 **cookieMr** 5 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** 5 months, 2 weeks ago

D is correct, since it's an external certificate

upvoted 1 times

 **Bmarodi** 5 months, 3 weeks ago

Selected Answer: D

Option D meets these requirements.

upvoted 1 times

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

EXTERNAL certofocation is the key - Manual rotation is required so Answer is D

upvoted 3 times

 **cheese929** 7 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

 **channn** 8 months ago

Selected Answer: D

Key word: External CA -> manually

upvoted 1 times

 **linux_admin** 8 months ago

Selected Answer: D

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.

This option meets the requirements because it uses an SSL/TLS certificate issued by an external CA and involves a manual rotation process that can be done yearly before the certificate expires. The other options involve using AWS Certificate Manager to issue the certificate, which does not meet the requirement of using an external CA.

upvoted 1 times

 **AndyMartinez** 9 months, 3 weeks ago

Selected Answer: D

Option D. ACM cannot automatically renew imported certificates.

upvoted 1 times

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, 1 month 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 36 times

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

I'm thinking when you wrote DocumentDB you meant it as DynamoDB...yes?
upvoted 3 times

✉  **benjl** 11 months, 1 week ago

Yes, DynamoDB has 400KB limit for the item.
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/ServiceQuotas.html>
upvoted 4 times

✉  **rob74** 1 year ago

In addition to this Lambda is paid only when used....
upvoted 5 times

✉  **raffaello44** 1 year, 1 month ago

is lambda scalable as an EC2 ?
upvoted 4 times

✉  **Ruffyit**  1 month 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** 3 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 2 times

 **RDX19** 4 months, 1 week ago

Selected Answer: A

Option A is right answer since Dynamo DB has size limitations.

upvoted 1 times

 **miki111** 4 months, 1 week ago

Option A is the right answer.

upvoted 1 times

 **cookieMr** 5 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 4 times

 **Bmarodi** 5 months, 3 weeks ago

Selected Answer: A

The solution meets these requirements most cost-effectively is option A.

upvoted 1 times

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

Selected Answer: A

Answer A is the most cost effective solution that meets the requirement

upvoted 1 times

 **channn** 8 months ago

Selected Answer: A

Key words: MOST cost-effectively, so S3 + Lambda

upvoted 1 times

 **SilentMilli** 10 months, 3 weeks 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

 **Buruguduystunstugudunstuy** 11 months, 1 week 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

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 10 months, 3 weeks 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** 11 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **JayBee65** 11 months, 3 weeks 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

 **Wpcorgan** 1 year ago

A is correct

upvoted 1 times

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*

D (79%) A (17%) 4%

✉️  **sba21**  1 year, 1 month ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/83281-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 18 times

✉️  **MutiverseAgent** 4 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 2 times

✉️  **MrAWS**  10 months, 2 weeks 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 12 times

✉️  **DarthVaper** 2 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 1 times

✉️  **MiniYang**  1 week, 1 day 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

✉️  **tom_cruise** 1 month 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 1 times

✉ **Ruffyt** 1 month 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 1 times

✉ **AWSStudyBuddy** 1 month, 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** 1 month, 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** 1 month, 3 weeks ago

Selected Answer: A

they already have a site to site VPN connection

upvoted 2 times

✉ **paniya93** 1 month, 4 weeks ago

Selected Answer: D

Answer is D

somewhere, the 6xx question gives the correct answer as D.

upvoted 1 times

✉ **axelrodb** 2 months, 2 weeks ago

Selected Answer: D

D is the correct answer

upvoted 1 times

✉ **bahaa_shaker** 3 months ago

Selected Answer: A

ITs A and the company use site 2 site VPN which means they can connect to fsx.

upvoted 3 times

✉ **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: D

the requirements are to provide access to both on-premises and AWS file storage with minimum latency, while minimizing operational overhead and avoiding significant changes to existing file access patterns. Additionally, an AWS Site-to-Site VPN connection is in place for connectivity.

upvoted 1 times

✉ **miki111** 4 months, 1 week ago

Option D is the right answer.

upvoted 1 times

 **cookieMr** 5 months, 1 week ago

Selected Answer: D

Amazon FSx File Gateway (FSx File Gateway) is a new File Gateway type that provides low latency and efficient access to in-cloud FSx for Windows File Server file shares from your on-premises facility. If you maintain on-premises file storage because of latency or bandwidth requirements, you can instead use FSx File Gateway for seamless access to fully managed, highly reliable, and virtually unlimited Windows file shares provided in the AWS Cloud by FSx for Windows File Server.

FSx File Gateway provides the following benefits:

1. Helps eliminate on-premises file servers and consolidates all their data in AWS to take advantage of the scale and economics of cloud storage.
2. Provides options that you can use for all your file workloads, including those that require on-premises access to cloud data.
3. Applications that need to stay on premises can now experience the same low latency and high performance that they have in AWS, without taxing your networks or impacting the latencies experienced by your most demanding applications.

upvoted 8 times

 **Bmarodi** 5 months, 3 weeks ago

Selected Answer: D

Option D meets these requirements.

upvoted 1 times

 **beginnercloud** 6 months, 2 weeks ago

Selected Answer: D

D is correct

<https://aws.amazon.com/blogs/storage/accessing-your-file-workloads-from-on-premises-with-file-gateway/>

upvoted 1 times

 **Rahulbit34** 7 months ago

Amazon Fix File Gateway for low latency and efficient access to in-cloud FSx for windows File server.

upvoted 1 times

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 11 months, 1 week 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 13 times

✉  **Buruguduystunstugudunstuy** 11 months, 1 week 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 4 times

✉  **Ruffyit** Most Recent 1 month 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** 1 month, 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** 2 months, 3 weeks ago

with the choices here, I would go with C, but if offered, I would use amazon textract for the text and use Macie to do the scanning of text files, not comprehend.

upvoted 1 times

✉  **Guru4Cloud** 3 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** 4 months, 1 week ago

Option C is the right answer.

upvoted 2 times

✉ **cookieMr** 5 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** 8 months ago

Key word: hospital!

upvoted 1 times

✉ **alexiscloud** 8 months ago

Answer C:

upvoted 1 times

✉ **Chirantan** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

✉ **SONA_M_** 11 months, 2 weeks ago

WHY OPTION D IS WRONG

upvoted 1 times

✉ **mj61** 10 months, 2 weeks ago

B/C you use TextTract to extract text not Rekognition.

upvoted 1 times

✉ **s_fun** 11 months ago

D is wrong only because Amazon Rekognition doesn't read text, only explicit image contents.

upvoted 3 times

✉ **k1kavi1** 11 months, 2 weeks ago

Selected Answer: C

Agreed

upvoted 1 times

✉ **Rameez1** 12 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 ago

C is correct

upvoted 1 times

✉ **bansalhp** 1 year, 1 month ago

Selected Answer: C

Textract -to extract textand Comprehend -to identify Medical info

upvoted 3 times

 **JesseesS** 1 year, 1 month ago

Textract and Comprehend is HIPPA compliant

<https://aws.amazon.com/blogs/machine-learning/amazon-textract-is-now-hipaa-eligible/>

upvoted 1 times

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

C (64%)	A (21%)	B (16%)
---------	---------	---------

 **Six_Fingered_Jose** Highly Voted  1 year, 1 month 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 64 times

 **Kumaran1508** 6 months, 1 week 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 3 times

 **JayBee65** 11 months, 3 weeks 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 5 times

 **syh_rapha** 11 months, 3 weeks 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** 3 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 2 times

 **wearrexdzw3123** 1 month ago

Because it requires the lowest cost

upvoted 2 times

 **ninjawrz** Highly Voted  1 year, 1 month 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 24 times

 **wearrexdzw3123** 1 month ago

Glaciers usually take some time to retrieve
upvoted 1 times

✉  **wh1t4k3r** 11 months, 3 weeks ago

Instant Retrieval was never mentioned. The exams always mention the tier when needed to. To be A the answer given should at least include the step mentioning that instant retrieval would be used.

upvoted 9 times

✉  **Help2023** 9 months, 2 weeks ago

Would agree if that was one of the answers, however many questions that are asked do have alternative solutions but again they are doing this on purpose to check your knowledge. Here C is best.

upvoted 2 times

✉  **wh1t4k3r** 11 months, 3 weeks 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

✉  **ad11934** Most Recent 2 days, 13 hours ago

Selected Answer: A

Looks like it needs immediate access always so it should be s3 glacier retrieval.

S3 Glacier Instant Retrieval for archive data that needs immediate access.

upvoted 1 times

✉  **MrPCarrot** 1 week, 3 days ago

I would go for C as A did not clarify the Glacier Class

upvoted 1 times

✉  **wabosi** 2 weeks, 2 days ago

Selected Answer: C

To me is C because it says "Immediate accessibility is always required" and "MOST cost-effective"; till Glacier Instant Retrieval retrieval time is instantaneous. If you go for Glacier Flexible Retrieval, retrieval is more expensive than flexible retrieval unless you use Bulk which is free but then it's not immediate retrieval.

upvoted 1 times

✉  **NickGordon** 3 weeks, 2 days ago

Selected Answer: A

A is the MOST cost effective. Glacier instant Retrieve is charged by size for retrieval 0.03/GB and storage cost is \$0.004 per GB. IA storage is charged by total storage \$0.0125/GB. Given each file is just 5MB, and the company has a large number of file. The cost of storage should overweight the cost of retrieval.

upvoted 1 times

✉  **xdkonorek2** 3 weeks, 5 days ago

Selected Answer: A

A is better than C

there is no class specified in Glacier so we can choose what is the best fit

With S3 Glacier Instant Retrieval, you can save up to 68% on storage costs compared to using the S3 Standard-Infrequent Access (S3 Standard-IA) storage class, when your data is accessed once per quarter.

upvoted 1 times

✉  **slimen** 4 weeks, 1 day ago

Selected Answer: B

keys: cost effective, immidiate accesss withihn 30 days

answer is B

s3 one zone-ia make the data accessible immediately
and cost 20% less than s3 standard-ia

upvoted 1 times

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

Selected Answer: A

Most COST EFFECTIVE

upvoted 1 times

✉  **GB_12345** 1 month, 2 weeks ago

Selected Answer: C

problem states the most cost effective, instant access & available for 4 yrs, so it has to be C

if Glacier Instant was an option, that would be cheaper, but it's just listed as generic Glacier (probably an older question)

upvoted 1 times

✉  **David_Ang** 1 month, 3 weeks ago

Selected Answer: C

"C" is not the most cost efficient, but it's the only answer that meets the requirements because glacier is going to be slower and one-zone is not going to be resilient, they say that the data is critical, so obviously the data can not be lost.

upvoted 1 times

✉ **Abitek007** 1 month, 3 weeks ago

so the difference between Glacier and Infrequent S3 is instant retrieval? Good to know

upvoted 1 times

✉ **daniel1** 2 months ago

A is the right answer; You would be paying high for Storage -IA for almost 4 years compared to Glacier. I get the point the Instant Retrieval is not mentioned and we cant assume also its a deep archive or flexible hence the answer A as its most cost effective

upvoted 1 times

✉ **Subhrangsu** 2 months ago

As they have not mentioned the S3 Glacier Instant Retrieval (which is 68% cheaper than S3 Standard IA) in the options still 'A' should be the option as in question it is mentioned as most COST-EFFECTIVE Way.

upvoted 1 times

✉ **Hassao0** 3 months ago

c is right in my way because in question immediate accessibility is required still for 4 years "Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce"

it refers to standard IA after 30 days

upvoted 1 times

✉ **mesutal** 3 months ago

Selected Answer: A

AAAAAAAAAAAAAAAAAAAAAA

upvoted 1 times

✉ **Soumya198725** 3 months ago

It will be Option : D as per Google bard

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 35 times

✉️  **JayBee65** 11 months, 3 weeks 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 12 times

✉️  **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 6 times

✉️  **karbob** 10 months, 3 weeks ago

not relevant to this issue. ??? what is added value

upvoted 3 times

✉️  **Buruguduystunstugudunstuy** 9 months 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 3 times

✉️  **Subhrangsu** Most Recent 2 months ago

I also opt for D, but asking does increasing MessageVisibilityTimeOut good always?

upvoted 1 times

✉️  **miki111** 4 months, 1 week ago

Option D is the right answer.

upvoted 1 times

✉️  **cookieMr** 5 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** 7 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **alexiscloud** 8 months ago

Answer D:

visibility timeout begins when Amazon SQS returns a message

upvoted 1 times

 **test_devops_aws** 8 months, 2 weeks ago

Selected Answer: D

D = ChangeMessageVisibility

upvoted 1 times

 **dev1978** 10 months, 2 weeks 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** 10 months, 3 weeks ago

Selected Answer: D

Increasing visibility timeout makes sure message is not visible for time taken to process the message.

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **Wpcorgan** 1 year ago

D is correct

upvoted 1 times

 **mabotega** 1 year 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, 1 month ago

Selected Answer: D

True, it's D.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

upvoted 6 times

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 (91%) 9%

✉️  **KVK16** Highly Voted 1 year, 1 month ago

Selected Answer: A

Direct Connect + VPN best of both

upvoted 14 times

✉️  **mabotega** Highly Voted 1 year 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 11 times

✉️  **Ruffyt** Most Recent 1 month 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 1 times

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

A is the right choice to save cost

upvoted 1 times

✉️  **Guru4Cloud** 3 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** 3 months, 3 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** 4 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** 4 months, 1 week ago

Even though, there are lots of variables 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** 4 months, 1 week ago

Option A is the right answer.
upvoted 1 times

 **cookieMr** 5 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** 7 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** 8 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** 10 months 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** 10 months, 2 weeks ago

Why not B? Two VPNs on different connections? Direct Connect costs a fortune?

upvoted 1 times

 **J3nkinz** 10 months, 2 weeks 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 2 times

 **thanhch** 11 months, 1 week 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

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Selected Answer: C

This a tricky question but let's try to understand the requirements of the question.

The company requires VS The company needs.

The main difference between need and require is that needs are goals and objectives a business must achieve, whereas require or requirements are the things we need to do in order to achieve a need.

upvoted 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

To meet the requirements specified in the question, the best solution is to provision two AWS Direct Connect connections to the same Region. This will provide a highly available connection with consistently low latency to the AWS Region and minimize costs by eliminating internet usage fees. Provisioning a second Direct Connect connection as a backup will ensure that there is a failover option available in case the primary connection fails.

upvoted 4 times

 **studynoplay** 6 months, 4 weeks ago

2 Direct connections will not minimize costs. Correct Answer is A

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Using VPN connections as a backup, as described in options A and B, is not the best solution because VPN connections are typically slower and less reliable than Direct Connect connections. Additionally, having two VPN connections to the same Region may not provide the desired level of availability and may not meet the company's requirement for low latency.

Option D, which involves using the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails, is not a valid option because the Direct Connect failover attribute is not available in the AWS CLI.
upvoted 6 times

 **ruqui** 6 months, 2 weeks ago

You forgot to consider that "the company is willing to accept slower traffic if the primary connection fails", so option A is the best answer
upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

See pricing for more info.
<https://aws.amazon.com/directconnect/pricing/>
upvoted 1 times

 **ocbn3wby** 10 months ago

I love your comments!
upvoted 2 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

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

B (94%)	6%
---------	----

✉️  **SilentMilli**  10 months, 3 weeks 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 14 times

✉️  **KVK16**  1 year, 1 month ago

Selected Answer: B

RDS Proxy for Aurora <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 8 times

✉️  **MiniYang**  1 week, 1 day 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

✉️  **asulhi** 2 months, 1 week ago

Selected Answer: B

ASG and MultiAZ is the best answer

upvoted 1 times

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

B is the right answer

upvoted 1 times

✉️  **Guru4Cloud** 3 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** 3 months, 3 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** 4 months, 1 week ago

Option B is the right answer.
upvoted 1 times

✉ **hiepdz98** 5 months ago

Selected Answer: B
B is correct answer
upvoted 2 times

✉ **cookieMr** 5 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 5 times

✉ **Abrar2022** 6 months, 2 weeks 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** 9 months, 3 weeks 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** 11 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** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: B
Option B
upvoted 1 times

✉ **Shasha1** 11 months, 2 weeks 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

✉ **Wajif** 1 year ago

Selected Answer: A
Why not A?
upvoted 2 times

 **Buruguduystunstugudunstuy** 11 months ago

Here is why Option A is not the correct solution:

Option A: Place the EC2 instances in different AWS Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.

While this solution would provide high availability with minimum downtime, it would involve significant operational effort and may result in data loss. Placing the EC2 instances in different Regions would require significant infrastructure changes and could impact the performance of the application. Additionally, Aurora PostgreSQL Cross-Region Replication is designed to provide disaster recovery rather than high availability, and it may result in some data loss during the replication process.

upvoted 4 times

 **koreanmonkey** 1 year ago

maybe because of load balancer, diffrent region can't be answer.

upvoted 2 times

 **WZN** 12 months ago

"The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones". Why not A?

upvoted 1 times

 **javitech83** 11 months, 4 weeks ago

They need to be in the same Region

upvoted 1 times

 **JayBee65** 11 months, 3 weeks ago

The question states multiple regions not multiple Availability Zones, a big difference!

upvoted 1 times

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

C (88%) 12%

✉️  **123jh10**  1 year, 1 month 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 23 times

✉️  **Ack3rman** 1 year ago

can you elaborate more pls

upvoted 2 times

✉️  **BlueVolcano1** 10 months, 1 week 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 7 times

✉️  **km142646** 7 months, 1 week ago

What's the difference between endpoint URL and health check path?

upvoted 1 times

✉️  **majubmo** 5 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 6 times

✉️  **ArielSchivo**  1 year, 1 month 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 13 times

✉️  **BlueVolcano1** 10 months, 1 week 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

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

Selected Answer: C

ALB allows you to specify the path which helps to check the error. NLB cannot do that.

upvoted 1 times

 **Guru4Cloud** 3 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** 4 months, 1 week ago

Option C is the right answer.

upvoted 1 times

 **cookieMr** 5 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** 6 months, 2 weeks 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** 8 months, 2 weeks 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** 8 months, 2 weeks ago

Also A doesn't offer what bellow in C offers...

Configure an Auto Scaling action to replace unhealthy instances

upvoted 1 times

 **Tony1980** 9 months, 4 weeks 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** 10 months ago

I will go with A as Network load balancer supports HTTP and HTTPS health checks, maybe the answer is outdated.

upvoted 2 times

 **John_Zhuang** 11 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** 10 months, 1 week 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

 **benjl** 11 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** 11 months, 1 week ago

Selected Answer: C

Correct answer - C

Network load balancers (Layer 4) allow to:

- Forward TCP & UDP traffic to your instances
- Handle millions of requests per second
- Less latency ~100 ms (vs 400 ms for ALB)

Best choice for HTTP traffic - replace to Application load balancer

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 11 months, 1 week 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 4 times

✉ **vipyodha** 5 months, 2 weeks 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** 11 months, 1 week 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** 11 months, 1 week 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

✉ **Schladde** 8 months ago

This won't increase availability when instances become unavailable.

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: A

Option A is very much a valid option as Autoscaling group can be configured to remove EC2 instances that fail http health check of NLB. AWS NLB supports http based health check.

upvoted 1 times

✉ **LeGlopier** 1 year ago

Selected Answer: A

A is the best option.

NLB supports http healthcheck, so why do we need to move to ALB ?

moreover the sentence "Configure an Auto Scaling action to replace unhealthy instances" in C seems to be wrong, as auto scaling removes any unhealthy instance by default, you do not need to configure it.

upvoted 1 times

✉ **JayBee65** 11 months, 3 weeks ago

I would say A will not give you what you want. "If you add a TLS listener to your Network Load Balancer, we perform a listener connectivity test." (<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html>) So a check will be made to see that something is listening on port 443. What it will not check is the status of the application e.g. HTTP 200 OK. Now the Application Load Balancer HTTP health check using the URL of the company's application, will do this, so C is the correct answer.

upvoted 2 times

 **Wpcorgan** 1 year ago

C is correct

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 35 times

✉  **LionelSid** 10 months 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 3 times

✉  **piavik** 7 months, 3 weeks ago

What is "DynamoDB service on the instance" ?

upvoted 1 times

✉  **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 6 times

✉  **Buruguduystunstugudunstuy** 11 months, 1 week 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 4 times

 **Guru4Cloud** Most Recent 3 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** 5 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** 6 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]** 7 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** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **Shasha1** 11 months, 2 weeks 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 ago

B is correct

upvoted 1 times

 **SimonPark** 1 year, 1 month ago

Selected Answer: B

B is the answer

upvoted 1 times

 **BoboChow** 1 year, 1 month 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, 1 month ago

I THINK B.

<https://dynobase.dev/dynamodb-point-in-time-recovery/>

upvoted 1 times

 **priya2224** 1 year, 1 month ago

answer is D

upvoted 1 times

 **[Removed]** 1 year, 1 month ago

bhk gandu chutiye glt ans btata hai

upvoted 1 times

 **Az900500** 1 year ago

Try communicate in English for audience

upvoted 4 times

 **123jhlo** 1 year, 1 month ago

DynamoDB is serverless, so no storage snapshots available. <https://aws.amazon.com/dynamodb/>

upvoted 2 times

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** Highly Voted 11 months, 1 week 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 27 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 8 times

 **KVK16** Highly Voted 1 year, 1 month ago

Selected Answer: D

To reduce costs get rid of NAT Gateway , VPC endpoint to S3

upvoted 22 times

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

Selected Answer: D

Prevent traffic from traversing the internet = Gateway VPC endpoint for S3.

upvoted 1 times

 **Guru4Cloud** 3 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** 5 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** 5 months, 3 weeks ago

Selected Answer: D

Option D is correct answer.

upvoted 1 times

 **Erbug** 10 months 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** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **9014** 11 months, 3 weeks 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** 11 months, 3 weeks 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** 11 months, 3 weeks ago

Yes correct

upvoted 1 times

 **Wpcorgan** 1 year ago

D is correct

upvoted 1 times

 **yd_h** 1 year, 1 month 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

 **123jh10** 1 year, 1 month ago

Selected Answer: D

Close question to the Question #4, with same solution.

upvoted 3 times

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

CD (90%)	8%
----------	----

 **Six_Fingered_Jose**  1 year, 1 month 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 31 times

 **Marco_St**  1 week, 5 days 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 1 times

 **ATInnovandoJuntos** 1 week, 4 days ago

https://en.wikipedia.org/wiki/Network_address_translation

That's the reason is C and not B

upvoted 1 times

 **slimen** 4 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 1 times

 **wearrexdzw3123** 1 month ago

Why are there always such unclear questions?

upvoted 1 times

 **tom_cruise** 1 month, 2 weeks ago

Selected Answer: CD

Key: through the company's internet connection

upvoted 1 times

 **prabhjot** 1 month, 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** 2 months ago

Please check first comments from top of them:

Help2023

WherecanIstart

Buruguduystunstugudunstuy

upvoted 1 times

 **TariqKipkemei** 3 months, 2 weeks 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** 5 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** 7 months ago

the internal and external IP range is not clear

upvoted 4 times

 **PLN6302** 3 months, 1 week ago

yes same for me

upvoted 1 times

 **km142646** 7 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** 9 months ago

Why external and not internal?

upvoted 2 times

 **TariqKipkemei** 8 months, 3 weeks ago

Because the traffic goes through the public internet. In the public internet, public IP(external IP) is used.

upvoted 6 times

 **Help2023** 9 months, 1 week 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

 **WhericanIstart** 9 months 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 2 times

 **swolfgang** 10 months, 2 weeks 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** 4 months, 2 weeks 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** 11 months, 1 week ago

Selected Answer: CD

<https://www.examtopics.com/discussions/amazon/view/51356-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 1 week 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

 **career360guru** 11 months, 2 weeks ago

Selected Answer: CD

C and D

upvoted 1 times

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 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 18 times

 **ArielSchivo**  1 year, 1 month 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 15 times

 **TariqKipkemei**  3 months, 2 weeks 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** 3 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** 5 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** 6 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 2 times

 **beginnercloud** 6 months, 2 weeks ago

Selected Answer: AC

AC is correct

upvoted 1 times

 **Whericanstart** 9 months 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** 10 months, 3 weeks 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** 10 months, 3 weeks ago

Selected Answer: AC

Security group => focus on inbound traffic since by default outbound traffic is allowed

upvoted 2 times

 **orionizzie** 11 months, 1 week ago

why both are inbound rules

upvoted 1 times

 **kraken21** 8 months ago

Because security groups are stateful.

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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

 **PassNow1234** 11 months, 1 week 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

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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** 10 months, 3 weeks ago

Chatgpt is unreliable this answer from same.

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

 **Wpcorgan** 1 year ago

A and C

upvoted 1 times

 **gcmrjbr** 1 year, 1 month ago

Agree with AC.

upvoted 2 times

 **srcshekhar** 1 year, 1 month ago

Very good questions

upvoted 3 times

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

A (78%) D (22%)

✉  **gcmrjbr** Highly Voted 1 year, 1 month ago

Agree with A>>> Lambda = serverless + autoscale (modernize), SQS= decouple (no more drops)
upvoted 26 times

✉  **LuckyAro** Highly Voted 10 months 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 15 times

✉  **remand** 10 months ago

it says "one tier becomes overloaded" , Not communication failure...
upvoted 2 times

✉  **LuckyAro** 9 months, 3 weeks ago

D says: "Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected".
upvoted 4 times

✉  **MrPCarrot** Most Recent 1 week, 3 days ago

A is the perfect answer no need for the ASG
upvoted 1 times

✉  **xdkonorek2** 3 weeks, 5 days 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** 1 month, 2 weeks ago

Selected Answer: A

ASG is not as efficient as Lambda!
upvoted 1 times

✉  **vijaykamal** 2 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 3 times

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

Selected Answer: A

MOST operationally efficient = Serverless = AWS Lambda functions, Amazon Simple Queue Service
upvoted 1 times

✉  **zjcorpuz** 4 months, 1 week 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** 5 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** 4 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

 **prakashiyanarappan** 7 months ago

ANS: A Key word - RESTful services - Amazon API Gateway

upvoted 4 times

 **ajaynaik44** 7 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** 7 months, 3 weeks ago

@Buruguduystunstugudunstuy Kindly share your comments for this question

upvoted 1 times

 **remand** 10 months 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

 **bullrem** 10 months, 1 week ago

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. This solution allows for horizontal scaling of the application servers and allows for automatic scaling based on communication failures, which can help prevent transactions from being dropped when one tier becomes overloaded. It also provides a more modern and operationally efficient way to handle communication between application services compared to traditional RESTful services.

upvoted 3 times

 **goodmail** 10 months, 3 weeks ago

Selected Answer: A

Can be A only. Other 3 answers use CloudWatch, which does not make sense for this question.

upvoted 2 times

 **techhb** 10 months, 3 weeks ago

Selected Answer: A

Server less and de couple.

upvoted 2 times

 **Parsons** 11 months ago

Selected Answer: A

Serverless (Lambda) + Decouple (SQS) is a modernized application.

The flow looks like this: API Gateway --> SQS (act as decouple) -> Lambda functions (act as subscriber pull msg from the queue to process)

upvoted 3 times

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** Highly Voted 1 year, 1 month 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 25 times

 **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 11 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 8 times

 **doorahmie** 10 months ago

explanation about D option is good
upvoted 1 times

 **Ruffyit** Most Recent 1 month 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 1 times

 **TariqKipkemei** 3 months, 2 weeks ago

Selected Answer: B

Secure and Most reliable transfer = AWS DataSync over AWS Direct Connect
upvoted 1 times

 **Guru4Cloud** 3 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** 4 months, 2 weeks ago

Not over public hence AC out / DMS is for databases and here refers to "JSON files".

upvoted 1 times

✉️ **cookieMr** 5 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** 6 months, 1 week ago

Best option and correct is B

upvoted 1 times

✉️ **Abrar2022** 6 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** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

✉️ **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B. DMS is not needed as there is no Database migration requirement.

upvoted 1 times

✉️ **Wajif** 1 year 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 ago

B is correct

upvoted 1 times

✉️ **yd_h** 1 year, 1 month 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

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

C (95%) 5%

✉  **123jh10** Highly Voted 1 year, 1 month 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 36 times

✉  **Futurebones** 6 months, 3 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 3 times

✉  **Remy_d** 1 month, 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 1 times

✉  **TariqKipkemei** Highly Voted 3 months, 2 weeks 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 8 times

✉  **Ruffyit** Most Recent 1 month 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 1 times

✉  **peekingpicker** 1 month, 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** 1 month, 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 1 times

✉ **Guru4Cloud** 3 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** 4 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** 5 months ago

Selected Answer: C

C - is the answer

upvoted 1 times

✉ **cookieMr** 5 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** 6 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** 8 months, 2 weeks 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

✉ **bullrem** 10 months, 1 week 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** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **Wpcorgan** 1 year ago

C is correct

upvoted 1 times

 **Cristian93** 1 year, 1 month ago

Selected Answer: C

C is correct answer

upvoted 2 times

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** Highly Voted 1 year, 1 month 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 39 times

✉  **MutiverseAgent** 4 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

✉  **LuckyAro** 10 months, 1 week ago

I think the answer is C because of storage time.

upvoted 1 times

✉  **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 9 times

✉  **Buruguduystunstugudunstuy** 11 months, 1 week 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 8 times

✉  **Guru4Cloud** Most Recent 3 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** 5 months ago

Selected Answer: B

B - is the answer because its easy to setup via AWS Backup & It indicates the keyword "MOST Operational Efficient". Other answers are indicating Cost efficient

upvoted 1 times

 **cookieMr** 5 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** 5 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** 6 months ago

using AWS Backup cheaper than DynamoDB point-in-time recovery

upvoted 1 times

 **kraken21** 7 months, 4 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** 8 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** 8 months, 2 weeks ago

Selected Answer: B

B = AWS backup

upvoted 1 times

 **Jiggs007** 10 months, 2 weeks ago

C is correct because we have to store data in s3 and an S3 Lifecycle configuration for the S3 bucket for 7 year.and its used on-demand backup of the table by using the DynamoDB console because If you need to store backups of your data for longer than 35 days, you can use on-demand backup. On-demand provides you a fully consistent snapshot of your table data and stay around forever (even after the table is deleted).

upvoted 2 times

 **Mainroad4822** 8 months, 2 weeks ago

In AWSBackup Plan, you can choose 7year Retention with Daily, Weekly or Monly frequency. From operational perspective, I think B is correct.

upvoted 1 times

 **LuckyAro** 10 months, 1 week ago

I think you are correct

upvoted 1 times

 **SilentMilli** 10 months, 3 weeks ago

Selected Answer: B

B. Use AWS Backup to create backup schedules and retention policies for the table.

AWS Backup is a fully managed service that makes it easy to centralize and automate the backup of data across AWS resources. It can be used to create backup schedules and retention policies for DynamoDB tables, which will ensure that the data is retained for the desired period of 7 years. This solution will provide the most operationally efficient method for meeting the requirements because it requires minimal effort to set up and manage.

upvoted 3 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B AWS Backup
upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: B

AWS Backup
upvoted 1 times

✉ **Wpcorgan** 1 year ago

B is correct
upvoted 2 times

✉ **mabotega** 1 year ago

Selected Answer: B

We recommend you use AWS Backup to automatically delete the backups that you no longer need by configuring your lifecycle when you created your backup plan.

<https://docs.aws.amazon.com/aws-backup/latest/devguide/deleting-backups.html>

upvoted 1 times

✉ **SimonPark** 1 year, 1 month ago

Selected Answer: B

B is clear
upvoted 2 times

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 (76%)

C (24%)

SimonPark [Highly Voted] 1 year, 1 month 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 35 times

123jh10 [Highly Voted] 1 year, 1 month 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 16 times

NasosoAuxtyno 8 months, 4 weeks ago

Thanks. Your reference link perfectly supports the option "A". 100% correct

upvoted 1 times

MiniYang [Most Recent] 1 week, 1 day 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 1 week, 1 day ago

Sorry I want to change my answer to A. Because the point is the "cost"

upvoted 1 times

BartoszGolebiowski24 1 month 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 3 weeks, 4 days ago

This is important, thank you for the link. A definitely

upvoted 1 times

Wayne23Fang 1 month, 3 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** 2 months, 1 week 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** 3 months, 2 weeks ago

Selected Answer: A

With on-demand capacity mode, DynamoDB instantly accommodates your workloads as they ramp up or down.

upvoted 1 times

✉ **ontheyun** 5 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** 5 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** 6 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** 6 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** 7 months, 1 week 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** 7 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** 8 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** 8 months, 1 week 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** 8 months, 3 weeks 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

 **Help2023** 9 months, 1 week ago

Selected Answer: A

A. This is because the traffic spikes have no set time as they can happen at any time, it being morning or evening

upvoted 1 times

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

B (89%) 5%

 **Sauran** Highly Voted 1 year, 1 month 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 15 times

 **ManoAni** Highly Voted 1 year, 1 month 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

 **xdkonorek2** Most Recent 3 weeks, 4 days 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** 1 month ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html>
upvoted 1 times

 **TariqKipkemei** 3 months, 2 weeks ago

Selected Answer: B

Share the AMI and Key with the MSP Partner's AWS account only
upvoted 1 times

 **tamefi5512** 5 months 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** 5 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** 6 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 1 times

 **Abrar2022** 6 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** 8 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** 8 months ago

Selected Answer: D

Option D

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 4 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 7 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **Jtic** 1 year ago

Selected Answer: B

Must use and share the existing KMS key to decrypt the same key

upvoted 3 times

 **fbcobra** 1 year ago

Selected Answer: B

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

upvoted 1 times

 **tubtab** 1 year, 1 month ago

Selected Answer: C

MOST secure way should be C

upvoted 2 times

 **Chunslı** 1 year, 1 month ago

MOST secure way should be C, with a separate key, not the one already used.

upvoted 1 times

 **Sauran** 1 year, 1 month ago

A seperate/new key is not possible because it won't be able to decrypt the AMI snapshot which was already encrypted with the existing/old key.

upvoted 10 times

 **UWSFish** 1 year, 1 month ago

This is truth

upvoted 2 times

 **Jtic** 1 year ago

Must use and share the existing KMS key to decrypt the same key

upvoted 1 times

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** Highly Voted 11 months, 3 weeks ago

Selected Answer: C

decoupled = SQS
Launch template = AMI
Launch configuration = EC2
upvoted 29 times

 **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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** 11 months, 1 week 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 6 times

 **graveend** 3 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** 3 weeks, 1 day ago

SQS satisfies the decoupling requirement

upvoted 1 times

 **slimen** Most Recent 4 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 1 times

✉ **darekw** 2 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** 3 months, 2 weeks 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** 3 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

✉ **cookieMr** 5 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 4 times

✉ **Bmarodi** 6 months, 1 week ago

Selected Answer: C

C for sure

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: C

SQS with EC2 autoscaling policy based number of messages in the queue.

upvoted 1 times

✉ **Uhrien** 11 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

✉ **kelljons** 12 months ago

what about the word "coupled"

upvoted 1 times

✉ **kewl** 12 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** 12 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 4 times

✉  **lulzsec2019** 10 months, 3 weeks ago

There's launch configuration. Search

upvoted 3 times

✉  **Liliwood** 1 year ago

I was not sure between Launch template and Launch configuration.

upvoted 1 times

✉  **Wpcorgan** 1 year ago

C is correct

upvoted 1 times

✉  **devopspro** 1 year ago

Selected Answer: C

answer is c

upvoted 1 times

✉  **Wilson_S** 1 year ago

<https://www.examtopics.com/discussions/amazon/view/22139-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

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*

D (51%) B (47%)

✉  **LeGlopier**  1 year, 1 month ago

B

AWS Config has a managed rule named acm-certificate-expiration-check to check for expiring certificates (configurable number of days)

upvoted 52 times

✉  **Mia2009687** 4 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 2 times

✉  **ChrisG1454** 8 months, 3 weeks 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 4 times

✉  **TTaws** 4 months, 2 weeks ago

Its B, simply because in option D - event bridge cannot "detect" anything.

upvoted 1 times

✉  **darekw** 2 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

✉  **RupeC** 4 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

✉  **LeGloupier** 1 year, 1 month ago
<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>
upvoted 10 times

✉  **ManoAni**  1 year, 1 month ago
Selected Answer: B
<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>
upvoted 11 times

✉  **Shalen**  2 days, 22 hours ago
Selected Answer: A
the correct answer should be A
ACM - Aws Certificate Manager
"Maintain SSL/TLS certificates, including certificate renewals, with automated certificate management."
see : <https://aws.amazon.com/certificate-manager/>
upvoted 1 times

✉  **MrPCarrot** 1 week, 3 days ago
The Answer is B.....
upvoted 1 times

✉  **slots** 1 week, 5 days ago
Selected Answer: B
I don't see a reason for custom alert therefore going for B.
upvoted 1 times

✉  **xdkonorek2** 3 weeks, 4 days ago
Selected Answer: D
aws config will send event to eventbridge but won't allow for customizing this message, so "custom alert" is not possible
D is correct, eventBridge can listen for acm-certificate-expiration-check event
upvoted 1 times

✉  **aptx4869** 1 month ago
Selected Answer: D
D is correct answer after I read this article. Most cost -efficient option is D.
upvoted 1 times

✉  **wearrexdzw3123** 1 month ago
B D is okay, but D is more effective
upvoted 1 times

✉  **iwannabeawsgod** 1 month, 2 weeks ago
its B.
upvoted 1 times

✉  **Andriy300** 1 month, 3 weeks ago
Selected Answer: B
B
Because
<https://repost.aws/knowledge-center/acm-certificate-expiration>
upvoted 1 times

✉  **Hibiki761** 1 month, 3 weeks ago
Selected Answer: B
<https://docs.aws.amazon.com/config/latest/developerguide/acm-certificate-expiration-check.html>
Config is used for expiration detection.
upvoted 1 times

✉  **Subhrangsu** 2 months ago
Why not A?
<https://docs.aws.amazon.com/acm/latest/userguide/managed-renewal.html>(1st paragraph)
upvoted 1 times

✉  **blurtiger320918** 2 months, 1 week ago
Selected Answer: D
Tested in AWS account, answer is D
upvoted 1 times

✉  **BrijMohan08** 2 months, 2 weeks ago
Selected Answer: B
<https://repost.aws/knowledge-center/acm-certificate-expiration>

upvoted 1 times

✉️  **RDM10** 2 months, 1 week ago

As per the above link, AWS Config incur additional charges so D is better.

upvoted 1 times

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

I believe it is D based on this article mentioning EventBridge event of a certificate expiring
<https://docs.aws.amazon.com/acm/latest/userguide/supported-events.html>

upvoted 1 times

✉️  **darekw** 2 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 1 times

✉️  **Hassao** 3 months ago

Option D is a viable solution, but Option B provides a more direct approach by leveraging AWS Config's compliance checking capabilities and integrating with CloudWatch Events and Amazon SNS for streamlined and automated alerting.

upvoted 1 times

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 11 months, 1 week 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 20 times

 **Euowellima** 2 months, 2 weeks ago

excelente explicação

upvoted 1 times

 **TariqKipkemei** 8 months, 3 weeks ago

good explanation..thanks

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 6 times

 **Ruffyit** Most Recent 1 month ago

C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

upvoted 1 times

 **Guru4Cloud** 3 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** 5 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** 6 months, 1 week ago

Selected Answer: C

C is best solution.

upvoted 1 times

 **gustavtd** 11 months ago

Selected Answer: C

Within few days you can not do more than using CloudFront

upvoted 3 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **kajal1206** 12 months ago

Selected Answer: C

C is correct answer

upvoted 1 times

 **koreanmonkey** 1 year ago

Selected Answer: C

CloudFront = CDN Service

upvoted 3 times

 **Liliwood** 1 year 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 ago

C is correct

upvoted 1 times

 **Hunkie** 1 year 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, 1 month ago

Selected Answer: C

Option C, use CloudFront.

upvoted 3 times

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

B (94%) 6%

 **ArielSchivo**  1 year, 1 month 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 13 times

 **cookieMr**  5 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 5 times

 **devmon** 2 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 1 times

 **MrPCarrot**  1 week, 3 days ago

B = Reserved for Prod and On Demand for Dev
upvoted 1 times

 **Bmarodi** 6 months, 1 week ago

Selected Answer: B

B meets the requirements, and most cost-effective.
upvoted 1 times

 **ChanghyeonYoon** 7 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** 8 months ago

Answeer B:
Sopt block are not longer available and you can't use spot instace on production
upvoted 1 times

 **Nandan747** 11 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** 11 months, 1 week 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** 6 months, 1 week 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** 11 months, 1 week 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

 **PassNow1234** 11 months, 1 week ago

The production EC2 instances run 24 hours a day.

upvoted 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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** 9 months 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 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **Vickysss** 11 months, 2 weeks 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 Flees may be even a better solution from a cost-wise perspective)

upvoted 1 times

 **Wpcorgan** 1 year ago

B is correct

upvoted 1 times

 **Jtic** 1 year 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 ago

B is the answer

<https://www.examtopics.com/discussions/amazon/view/80956-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 23 times

 **Burugduystunstugudunstuy** Highly Voted 11 months, 1 week 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 7 times

 **Burugduystunstugudunstuy** 11 months, 1 week 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 3 times

 **Guru4Cloud** Most Recent 3 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** 2 months ago

Liked the explanation for option C.Thanks!

upvoted 1 times

 **cookieMr** 5 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 Loc 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** 6 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** 10 months, 3 weeks 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** 11 months, 2 weeks ago

Selected Answer: A

Option A. Object Lock will prevent modifications to documents

upvoted 1 times

 **HarryZ** 11 months, 3 weeks ago

Why not C

upvoted 3 times

 **JayBee65** 11 months, 2 weeks 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 ago

A is correct

upvoted 1 times

 **flbcobra** 1 year ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

upvoted 1 times

 **Evangelia** 1 year, 1 month ago

Selected Answer: A

aaaaaaaaaa

upvoted 1 times

 **Evangelia** 1 year, 1 month ago

aaaaaaaaaaaaaa

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 21 times

✉️  **MrPCarrot** Most Recent 1 week, 3 days ago

A = Rotation of user credentials can be automated using Secrets Manager.

upvoted 1 times

✉️  **Ruffyit** 1 month 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** 3 months, 1 week ago

Selected Answer: A

AWS Secrets Manager to the rescue....up up and awaaaay

upvoted 1 times

✉️  **Guru4Cloud** 3 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

✉️  **cookieMr** 5 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 3 times

✉ **Bmarodi** 6 months, 1 week ago

Selected Answer: A

Option A is ans.

upvoted 2 times

✉ **vherman** 9 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

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

literally screams for AWS secrets manager to rotate the credentials

upvoted 4 times

✉ **Buruguduystunstugudunstuy** 11 months, 1 week 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 4 times

✉ **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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 4 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

✉ **kewl** 12 months ago

Selected Answer: A

Rotate credentials = Secrets Manager

upvoted 3 times

✉ **Wpcorgan** 1 year ago

A is correct

upvoted 1 times

✉ **renekton** 1 year ago

Selected Answer: A

Answer is A

upvoted 2 times

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

D (61%)

A (39%)

✉  **brushek** Highly Voted 1 year, 1 month 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 40 times

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

You are going to tell your boss that the customer is going to occasionally lose //only// 33% of their data, as if that's just acceptable?

upvoted 9 times

✉  **ekisako** 3 weeks, 1 day ago

lol read and understand carefully, it says REDUCES FAILOVER TIMES BY UP TO 66%.

upvoted 1 times

✉  **bgsanata** 6 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 17 times

✉  **Abdou1604** 3 months, 2 weeks ago

rDS PROXY Supports RDS (MySQL, PostgreSQL, MariaDB, MS SQL Server) and Aurora (MySQL, PostgreSQL)

upvoted 1 times

✉  **attila9778** 1 year ago

Aurora supports RDS proxy!

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

upvoted 5 times

✉  **PassNow1234** 11 months, 1 week ago

This is MySQL Database. RDS proxy = no no

upvoted 1 times

✉  **Robrobtutu** 7 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

✉  **123jh0** Highly Voted 1 year, 1 month 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 24 times

✉  **tinyfoot** 1 year 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 9 times

✉  **Duke_YU** 8 months 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** 6 months, 3 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

✉  **adeyinkaamole** 3 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** 3 months ago

I meant the answer answer is A

upvoted 1 times

✉  **JayBee65** 11 months, 2 weeks ago

It does, according to that link

upvoted 1 times

✉  **gcmrjbr** 1 year 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

✉  **Shalen** Most Recent 2 days, 21 hours 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** 1 week ago

ChatGPT chooses SQS

upvoted 1 times

✉  **Bjfikky** 1 week, 2 days 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

✉  **MrPCarrot** 1 week, 3 days ago

D = because RDS Proxy does not support Aurora DB

upvoted 1 times

✉  **ekisako** 3 weeks, 1 day ago

Selected Answer: A

RDS Proxy queues or throttles application connections that can't be served immediately from the pool of connections.

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

upvoted 1 times

✉  **brk_ravi** 3 weeks, 4 days ago

chatGPT says option D.

Proxy never talks about the saving the intermediate transaction ..

upvoted 1 times

✉️ **slimen** 3 weeks, 6 days ago

Selected Answer: D

seriously why D?!

RDS proxy is good when having a lot of connections to the database, it reduces the number of connections overhead on a database, when the DB is down the Proxy doesn't do anything!

this is a good case for decoupling the architecture and introducing a queue

upvoted 2 times

✉️ **tom_cruise** 1 month 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

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

Selected Answer: D

If the RDS is down, where does the RDS Proxy point to?

upvoted 3 times

✉️ **David_Ang** 1 month, 3 weeks ago

Selected Answer: D

"D" is more correct as it simply better, you are using a system that ensures data resilience, scalability and Decoupling which can help to secure the customer data during the DB upgrades.

upvoted 2 times

✉️ **joshik** 2 months ago

Selected Answer: A

I think this is most suitable, as both SQS and RDS would not store customer data in the right format for RDS

upvoted 1 times

✉️ **vijaykamal** 2 months ago

Answer is D, RDS proxy would not help if DB is down unless multi AZ is used.

upvoted 2 times

✉️ **BrijMohan08** 2 months, 2 weeks ago

Selected Answer: A

Aurora stores copies of the data in a DB cluster across multiple Availability Zones in a single AWS Region. Aurora stores these copies regardless of whether the instances in the DB cluster span multiple Availability Zones.

upvoted 1 times

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

Selected Answer: D

Data is needed to be stored somewhere till the DB is up, can be kept in SQS. So the ideal solution would be to send the data to SQS and poll the queue by Lambda and save the data in DB. The data can stay till successfully processed.

upvoted 1 times

✉️ **Hassao0** 3 months ago

Option B (increasing runtime and adding a retry mechanism) could help reduce the impact of connection disruptions, but it doesn't address the requirement to seamlessly store customer data during database upgrades.

Options C and D involve storing data locally or using Amazon SQS, but these approaches might not ensure data consistency and availability during database upgrades, which is a critical requirement.

In summary, using Amazon RDS Proxy (Option A) is the best approach to address the challenge of maintaining data availability and consistency during database upgrades for Lambda functions that interact with the Amazon Aurora MySQL database.

upvoted 1 times

✉️ **parrtner73** 1 month, 3 weeks ago

The question does not require data availability, just not to lose data while upgrade,

D makes sense.

upvoted 1 times

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

A (46%)	B (45%)	8%
---------	---------	----

✉  **Six_Fingered_Jose** Highly Voted 1 year, 1 month 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 48 times

✉  **parrtner73** 1 month, 3 weeks ago

If the requestor pays your cost is 0. can not go lower.
upvoted 3 times

✉  **thwvthunder** 3 months ago

is S3 Cross-Region Replication works between 2 separate aws accounts? shouldn't the answer is C?
upvoted 2 times

✉  **Kp88** 4 months, 1 week ago

I would go with A , If I am an SA of the company I would prefer to have other people pay the data transfer fees because same scenario can happen with multiple different firms in future.
upvoted 2 times

✉  **MutiverseAgent** 4 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** Highly Voted 1 year, 1 month 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 29 times

✉  **VladanO** Most Recent 22 hours, 58 minutes ago

Selected Answer: A
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/RequesterPaysBuckets.html>
upvoted 1 times

✉  **RyanMccar** 2 weeks ago

Selected Answer: C

Cross account access. No transfer fees at all
upvoted 1 times

 **aptx4869** 1 month ago

Selected Answer: C

The answer is obviously C. We can share the s3 bucket using IAM of other AWS account.

upvoted 2 times

 **David_Ang** 1 month, 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 it 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 it has absolutely no sense to pay more to transfer data in any way, the correct answer is "B".

upvoted 2 times

 **Abitek007** 1 month, 3 weeks ago

Selected Answer: B

Best way to reduce cost.

choosing A will be additional cost for data transfer

upvoted 1 times

 **Ramdi1** 1 month, 3 weeks ago

Selected Answer: B

I think it is B. The question says reduces charges and not to offload charges or something similar

upvoted 2 times

 **Ramdi1** 2 months, 2 weeks ago

Selected Answer: A

A similar question came up on tutorial dojo and I first assumed it was B, configure S3 Cross Region Replication. However they said the right answer was A in this case configure the requester pay feature.

upvoted 4 times

 **anhthang17** 2 months, 3 weeks ago

Selected Answer: C

C is my answer

upvoted 1 times

 **anhthang17** 2 months, 3 weeks ago

I think the answer must be C.

upvoted 1 times

 **oayoade** 3 months ago

Selected Answer: C

S3 Cross account access

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example2.html>

upvoted 2 times

 **karloscetina007** 3 months, 2 weeks ago

Selected Answer: B

transfer region replica still have lower cost against others manners to transfer and share s3 resources

upvoted 1 times

 **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: B

The best solution here is to configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.

The key requirements are to minimize data transfer costs while sharing large amounts of data with the marketing firm.

S3 Cross-Region Replication will replicate objects from the source bucket to a destination bucket in a different region. This avoids any data transfer charges for the company when the marketing firm accesses the replicated data in their own region

upvoted 1 times

 **Monu11394** 4 months, 1 week ago

The company (US) is looking to reduce "its" data transfer costs. So A.

upvoted 1 times

 **HassanYoussef** 4 months, 4 weeks ago

Selected Answer: A

A is the right answer as the source owner of the bucket will remain paying on the data hosted in the S3 bucket but the data transfer to the other account will be charged to the consumer, so in this case the source owner minimizes the cost:

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

upvoted 1 times

 **LePMGC** 5 months ago

Selected Answer: B

In the statement it is well said that "the company wants its transfert cost to remain as slow as possible" so the point is about reducing the cost of the company and not the european marketing firm.

upvoted 1 times

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** Highly Voted 1 year, 1 month ago

Selected Answer: A

Same as Question #44

upvoted 11 times

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

Selected Answer: A

Enable the versioning to ensure restoration in case of accidental deletion and MFA Delete for double verification before deletion.

upvoted 1 times

 **Guru4Cloud** 3 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** 5 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** 6 months, 1 week ago

Selected Answer: A

A is answer.

upvoted 1 times

 **Bmarodi** 6 months, 1 week ago

Selected Answer: A

A is answer.

upvoted 1 times

 **Robrobtutu** 7 months, 2 weeks ago

Selected Answer: A

A is correct.

upvoted 1 times

 **remand** 10 months, 2 weeks 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** 10 months, 3 weeks 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** 10 months, 2 weeks ago

only accidental deletion should be avoided. IAM policy will completely remove their access.hence, MFA is the right choice.

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 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 2 times

 **Buruguduystunstugudunstuy** 11 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** 11 months, 2 weeks ago

Selected Answer: A

A is the right answer

upvoted 1 times

 **Wpcorgan** 1 year ago

A is correct

upvoted 1 times

 **Jtic** 1 year ago

Selected Answer: A

Enable the versioning and MFA Delete features on the S3 bucket.

upvoted 1 times

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 (95%) 5%

 **alvarez100**  1 year, 1 month 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 29 times

 **Gil80**  1 year 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 13 times

 **NitiATOS** 10 months 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 2 times

 **slimen**  3 weeks, 6 days ago

Selected Answer: B

lol seriously the person who wrote the answer wants us to fail

upvoted 3 times

 **tom_cruise** 1 month, 2 weeks ago

Selected Answer: B

This is what we do in the real world.

upvoted 1 times

 **joshik** 2 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** 2 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** 3 months ago

the correct answer should be A, you can't create a read replica on a single-AZ DB instance

upvoted 1 times

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

Selected Answer: B

a read replica is always fit for these type of scenarios.

upvoted 1 times

✉ **Guru4Cloud** 3 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** 5 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** 6 months, 1 week ago

Selected Answer: B

For LEAST operational overhead, I recommended to use read replica DB

upvoted 1 times

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

Selected Answer: B

B is correct. Read replica for read only script any analytical loads.

upvoted 1 times

✉ **cheese929** 7 months ago

Selected Answer: B

B is correct. Run the script on the read replica.

upvoted 1 times

✉ **alexiscloud** 8 months ago

B:

read replica would be the best choice

upvoted 1 times

✉ **Mahadeva** 10 months, 4 weeks ago

Selected Answer: B

Reason to have a Read Replica is improved performance (key word) which is native to RDS. Elastic Cache may have misses.

The other way of looking at this question is : Elastic Cache could be beneficial for development tasks (and hence improve the overall DB performance). But then, Option D mentions that the queries for scripts are cached, and not the DB content (or metadata). This may not necessarily

improve the performance of the DB.

So, Option B is the best answer.

upvoted 1 times

 **DavidNamy** 10 months, 4 weeks ago

Selected Answer: B

The correct answer would be option B

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 23 times

 **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 12 times

 **Ruffyit** Most Recent 1 month 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** 1 month, 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** 3 months, 1 week ago

Selected Answer: A

Prevent traffic from traversing the internet = Gateway VPC endpoint for S3.

upvoted 1 times

 **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: A

Configure an S3 gateway endpoint

upvoted 1 times

 **tamefi5512** 5 months ago

Selected Answer: A

<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html>

upvoted 1 times

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

Selected Answer: A

Configure an S3 gateway endpoint is answer.

upvoted 1 times

 **gustavtd** 11 months ago

Selected Answer: A

S3 Gateway Endpoint is a VPC endpoint,

upvoted 1 times

 **langiac** 11 months, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html>

upvoted 1 times

 **Wpcorgan** 1 year ago

A is correct

upvoted 1 times

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 (85%) CD (15%)

 **Ruffyit** 1 month 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** 1 month, 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 1 times

 **Guru4Cloud** 3 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** 3 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** 3 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** 5 months ago

Selected Answer: AC

AC is the right answer

upvoted 1 times

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

Selected Answer: AC

A & C the correct solutions.

upvoted 2 times

 **TillieEhaung** 6 months, 2 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

 **annabellehiro** 8 months, 1 week ago

Selected Answer: AC

A and C

upvoted 1 times

 **Help2023** 9 months, 1 week 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** 9 months, 1 week ago

Selected Answer: AC

AC is correct

upvoted 1 times

 **bdp123** 9 months, 2 weeks ago

Selected Answer: AC

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-private-connection-noauthentication/>

upvoted 2 times

 **remand** 10 months, 2 weeks ago

Selected Answer: CD

c & D for security. A addresses accessibility which is not a concern here imo

upvoted 2 times

 **goodmail** 10 months, 2 weeks 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

 **mhmt4438** 10 months, 4 weeks ago

C and D

To provide secure access to the S3 bucket from the application tier running on EC2 instances inside a VPC, you should create a bucket policy that limits access to only the application tier running in the VPC. This will ensure that only the application tier has access to the bucket and its contents.

Additionally, you should create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance. This will allow the EC2 instance to access the S3 bucket using the IAM user's permissions.

Option A, configuring a VPC gateway endpoint for Amazon S3 within the VPC, would not provide any additional security for the S3 bucket.

Option B, creating a bucket policy to make the objects in the S3 bucket public, would not provide sufficient security for sensitive user information.

Option E, creating a NAT instance and having the EC2 instances use the NAT instance to access the S3 bucket, would not provide any additional security for the S3 bucket

upvoted 1 times

 **career360guru** 11 months, 1 week ago

Selected Answer: AC

A and C is right among the choice.

But instead of having bucket policy for VPC access better option would be to create a role with specific S3 bucket access and attach that role EC2 instances that needs access to S3 buckets.

upvoted 3 times

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

B (86%)	14%
---------	-----

✉  **Burugduystunstugudunstuy** Highly Voted 11 months, 1 week 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 10 times

✉  **Burugduystunstugudunstuy** 11 months, 1 week 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 13 times

✉  **Burugduystunstugudunstuy** 11 months, 1 week 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 5 times

✉  **MutiverseAgent** 4 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 to 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 2 times

✉  **arashjs1993** Most Recent 3 weeks, 5 days ago

Selected Answer: B

Aura MySQL is very fast in comparison to RDS for creating a clone of DB, you can create even a clone of a clone while you still work on your own clone, this will allow the dev team to continue working during the cloning step.

<https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/>

upvoted 1 times

✉️ **Ruffyit** 1 month 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** 2 months ago

Selected Answer: B

B is the correct

upvoted 1 times

✉️ **TariqKipkemei** 3 months, 1 week 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** 3 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** 5 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** 8 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** 8 months ago

Answer B:

upvoted 1 times

✉️ **bdp123** 9 months, 2 weeks ago

Selected Answer: B

<https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/>

upvoted 3 times

✉️ **john2323** 9 months, 2 weeks ago

Selected Answer: B

Database cloning is the best answer

upvoted 1 times

✉ **techhb** 11 months, 1 week ago

Selected Answer: B

Database cloning is right answer here.

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Option B is right.

You can not access Standby instance for Read in RDS Multi-AZ Deployments.

upvoted 3 times

✉ **aadi7** 11 months, 1 week 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

✉ **aadi7** 11 months, 1 week 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

✉ **333666999** 11 months, 3 weeks ago

Selected Answer: C

why not C

upvoted 4 times

✉ **MutiverseAgent** 4 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** 4 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** 4 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 ago

Selected Answer: B

Option B

upvoted 1 times

✉ **pspinelli19** 1 year 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

✉ **KLLIM** 1 year, 1 month ago

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Clone.html>

upvoted 2 times

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** Highly Voted 1 year ago

Option C
Dynamo DB is a NoSQL-JSON supported
upvoted 10 times

 **rjam** 1 year ago

also Use an AWS Lambda - serverless - less operational overhead
upvoted 8 times

 **cookieMr** Highly Voted 5 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 6 times

 **Ruffyit** Most Recent 1 month 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** 2 months ago

Selected Answer: C

C: Lambdas are made for that

upvoted 1 times

 **TariqKipkemei** 3 months, 1 week ago

Selected Answer: C

C is best

upvoted 1 times

 **Guru4Cloud** 3 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** 6 months, 1 week ago

Selected Answer: C

Option C is correct - Dynamo DB is a NoSQL-JSON supported

upvoted 1 times

 **Abrar2022** 6 months, 1 week ago

Selected Answer: C

SQS + LAMDA + JSON >>>> Dynamo DB

upvoted 1 times

 **Bmarodi** 6 months, 1 week ago

Selected Answer: C

The option C is right answer.

upvoted 1 times

 **jy190** 7 months ago

can someone explain why SQS? it's a poll-based messaging, does it guarantee reacting the event asap?

upvoted 1 times

 **Zerotn3** 11 months ago

Selected Answer: C

Dynamo DB is a NoSQL-JSON supported

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 2 weeks 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** 11 months, 3 weeks ago

Selected Answer: C

CCCCCC

upvoted 1 times

 **AlaN652** 11 months, 3 weeks ago

Selected Answer: C

Answer C

upvoted 1 times

 **HussamShokr** 12 months ago

Selected Answer: C

answer is C

upvoted 1 times

 **Kapello10** 1 year ago

Selected Answer: C

cccccccccccc

upvoted 1 times

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 (96%) 4%

✉ **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 12 times

✉ **Ruffyit** Most Recent 1 month 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 1 times

✉ **TariqKipkemei** 3 months, 1 week 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** 3 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** 4 months, 2 weeks ago

Read replica + Same resources as we may need to turn replica to primary in few cases

upvoted 1 times

✉ **cookieMr** 5 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** 6 months, 1 week ago

Selected Answer: D

D meets the requirements.

upvoted 1 times

 **Adeshina** 6 months, 3 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** 6 months ago

Err, just curious, what if the production database is 51% full? Your half storage read replica would explode...?

upvoted 4 times

 **Oldman2023** 8 months ago

Can anyone explain why B is not an option?

upvoted 4 times

 **caffee** 7 months, 3 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

 **draum010** 8 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

 **SuketuKohli** 8 months, 2 weeks 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** 6 months, 1 week ago

I think for RDS it is 5 read replicas. 15 is for aurora serverless

upvoted 1 times

 **DivaLight** 1 year ago

Selected Answer: D

Option D

upvoted 1 times

 **Wpcorgan** 1 year ago

D is correct

upvoted 1 times

 **Nigma** 1 year ago

D

<https://www.examtopics.com/discussions/amazon/view/46461-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Hunkie** 1 year ago

Selected Answer: D

If you scale the source DB instance, also scale the read replicas.
upvoted 2 times

 **ArielSchivo** 1 year, 1 month ago

Selected Answer: D

D is correct.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html
upvoted 2 times

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 (63%)

D (38%)

✉  **Joxtat**  10 months, 4 weeks ago

What the policy means:

1. Allow termination of any instance if user's source IP address is 100.100.254.

2. Deny termination of instances that are not in the us-east-1 Combining this 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 36 times

✉  **KMohsoe** 6 months, 3 weeks ago

Nice explanation. Thanks

upvoted 4 times

✉  **Subh_fidelity**  12 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 17 times

✉  **Bmarodi** 6 months, 1 week ago

A good explanation!

upvoted 2 times

✉  **Bjfikky** Most Recent 1 week, 2 days 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

✉  **sweetheatmn** 1 month, 1 week ago

Selected Answer: C

C because the explicit deny blocks other regions than us-east-1
upvoted 1 times

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

Selected Answer: C

The first statement is a subset of the second statement.
upvoted 1 times

✉  **prabhjot** 1 month, 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** 2 months ago

D is not because of Deny & NOT Equals
upvoted 1 times

✉  **Valder21** 2 months, 4 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** 3 months, 1 week 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** 3 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** 4 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 4 times

✉  **JoeGuan** 3 months, 3 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** 2 months ago

oh, ok got it now.

upvoted 1 times

✉  **MNotABot** 4 months, 2 weeks ago

<https://cidr.xyz/>
upvoted 1 times

✉  **beginnercloud** 6 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

 **Bmarodi** 6 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 right one.
upvoted 2 times

 **Moccorso** 6 months, 3 weeks ago

I think D

upvoted 1 times

 **darn** 7 months, 1 week ago

Selected Answer: C

its C

Deny & NOT Equal = CAN (basic logic folks)

upvoted 2 times

 **shinejh0528** 7 months, 3 weeks ago

Selected Answer: C

Oh... tricky.. TT... C is correct ...

upvoted 1 times

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 11 months, 1 week 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 15 times

 **Ruffyit** Most Recent 1 month 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** 3 months, 1 week ago

Selected Answer: D

Microsoft Windows shared file storage = Amazon FSx for Windows File Server

upvoted 1 times

 **Guru4Cloud** 3 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

 **cookieMr** 5 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 3 times

 **cheese929** 7 months ago

Selected Answer: D

D is correct. FSx is for windows and supports AD authentication

upvoted 1 times

 **kakka22** 7 months, 1 week ago

Why not B? Migrating the workload? Maybe is needed a hybrid cloud solution

upvoted 1 times

 **gx2222** 7 months, 4 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** 11 months, 2 weeks ago

Selected Answer: D

FSx is for Windows

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **xeun88** 11 months, 3 weeks ago

I'm going for D as the answer because FSx is compatible with windows

upvoted 1 times

 **kajal1206** 12 months ago

Selected Answer: D

Answer is D

upvoted 1 times

 **Wpcorgan** 1 year ago

D is correct

upvoted 1 times

 **TonyghostR05** 1 year ago

Windows only available for using FSx

upvoted 3 times

 **Nigma** 1 year 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 ago

EFS is for Linux

FSx is for Windows

upvoted 6 times

 **Hunkie** 1 year ago

Selected Answer: D

DDDDDDDD

upvoted 1 times

 **dokaedu** 1 year, 1 month ago

Correct Answer:D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>

upvoted 2 times

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

C (81%)

Other

✉  **Six_Fingered_Jose**  1 year, 1 month 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 39 times

✉  **JoeGuan** 3 months, 3 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 2 times

✉  **PLN6302** 3 months, 1 week ago

amazon s3 doesn't support fifo queues

upvoted 2 times

✉  **MutiverseAgent** 4 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

✉  **Ello2023** 10 months, 2 weeks 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 3 times

✉  **Robrobtutu** 7 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 sent 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 3 times

✉  **Abdou1604** 3 months, 2 weeks ago

i agree because the issue is multiple received email for an image uploaded

upvoted 1 times

✉  **aadityaravi8** 5 months ago

I agree with your answer explanation

upvoted 1 times

✉ **MrAWS** 10 months, 2 weeks ago

I tend to agree with you. See my comments above.

upvoted 1 times

✉ **brushek** Highly Voted 1 year, 1 month 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 13 times

✉ **Ruffyit** Most Recent 1 month 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 1 times

✉ **lqw** 1 month, 2 weeks ago

Selected Answer: C

least operational overheads

upvoted 1 times

✉ **prabhjot** 1 month, 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** 2 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** 2 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** 3 months ago

D is an incorrect answer because Lambda automatically deletes message from the queue when finish process

upvoted 1 times

✉ **TariqKipkemei** 3 months, 1 week 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** 3 months, 2 weeks ago

Selected Answer: C

I would go with the C.

upvoted 1 times

✉ **Olaunfazed** 5 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** 2 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** 5 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

✉️ **Abrar2022** 6 months, 1 week ago

FIFO - IS A SOLUTION BUT REQUIRES OPERATIONAL OVERHEAD.
INCREASING VISIBILITY TIMEOUT - REQUIRES FAR LESS OPERATIONAL OVERHEAD.
upvoted 3 times

✉️ **Bmarodi** 6 months, 1 week ago

Selected Answer: C
I go for option C.
upvoted 2 times

✉️ **Rahulbit34** 7 months ago

SQS VISIBILITY TIMEOUT can help preventing the reprocessing of the message from the queue. By default the timeout is 30 secs, min 0 and max is 12 hours.

upvoted 1 times

✉️ **quanbui** 7 months, 1 week ago

Selected Answer: C
ccccccc
upvoted 2 times

✉️ **tikytaka** 7 months, 2 weeks ago

Apologies, I meant A is wrong
upvoted 1 times

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

D (91%) 9%

 **123jh10**  1 year, 1 month ago

Selected Answer: D

Answer is D.

Lustre in the question is only available as FSx

<https://aws.amazon.com/fsx/lustre/>

upvoted 23 times

 **Buruguduystunstugudunstuy**  11 months, 1 week 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 9 times

 **Ruffyit**  1 month 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** 3 months, 1 week ago

Selected Answer: D

Lustre clients = Amazon FSx for Lustre file system

upvoted 1 times

 **Guru4Cloud** 3 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** 4 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** 1 month, 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** 3 months, 3 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

✉ **james2033** 4 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** 5 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** 7 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** 7 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** 8 months, 3 weeks ago

Selected Answer: D

seriously? it spells out "Lustre" for you

upvoted 1 times

✉ **CaoMengde09** 9 months, 3 weeks 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** 10 months ago

D is correct

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉ **Wpcorgan** 1 year ago

D is correct
upvoted 1 times

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

C (76%)

D (22%)

 **Chunsli** Highly Voted 1 year, 1 month ago

C makes a better sense. Between C (S3) and D (EBS), S3 is highly available with LEAST operational overhead.
upvoted 34 times

 **MutiverseAgent** 4 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 2 times

 **MXB05** Highly Voted 1 year, 1 month ago

Selected Answer: C

Correct Answer is C: EBS is not highly available
upvoted 17 times

 **Ello2023** 10 months, 2 weeks ago

EBS is Highly Available as it stores in multi AZ and S3 is regional.
upvoted 1 times

 **oguz11** 10 months, 1 week 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 8 times

 **FNJ1111** 11 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

 **JayBee65** 11 months, 2 weeks ago

Yes it is!
upvoted 1 times

 **xdkonorek2** Most Recent 3 weeks, 4 days 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

✉ **David_Ang** 1 month, 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** 1 month, 3 weeks ago

confused between EBS and S3, both are HA, but location?

upvoted 1 times

✉ **joshik** 2 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** 2 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** 3 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** 4 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** 4 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** 5 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** 6 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 2 times

✉ **bgsanata** 6 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** 6 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

✉ **Rahulbit34** 7 months ago

C make sense. as its asking for least operational overhead
upvoted 1 times

✉️  **channn** 7 months, 3 weeks ago

Selected Answer: C

- A. manual put <> near real time
- C. chooses as S3 is highly available
- D: only for that EC2

upvoted 1 times

✉️  **gx2222** 7 months, 4 weeks ago

Selected Answer: C

To meet the requirements of securely downloading, encrypting, decrypting, and storing certificates with minimal operational overhead, you can use AWS Key Management Service (KMS) and Amazon S3.

Here's how this solution would work:

Store the security certificates in an S3 bucket with Server-Side Encryption enabled.

Create a KMS Customer Master Key (CMK) for encrypting and decrypting the certificates.

Grant permission to the EC2 instance to access the CMK.

Have the application running on the EC2 instance retrieve the security certificates from the S3 bucket.

Use the KMS API to encrypt and decrypt the certificates as needed.

Store the encrypted certificates in another S3 bucket with Server-Side Encryption enabled.

This solution provides a highly secure way to encrypt and decrypt certificates and store them in highly available storage with minimal operational overhead. AWS KMS handles the encryption and decryption of data, while S3 provides highly available storage for the encrypted data. The only operational overhead involved is setting up the KMS CMK and S3 buckets, which is a one-time setup task.

upvoted 2 times

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 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 11 times

≡  **Shrestwt** 7 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 9 times

≡  **ronin201**  1 month 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

≡  **Ruffyit** 1 month ago

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-example-private-subnets-nat.html>

upvoted 1 times

≡  **Guru4Cloud** 3 months, 2 weeks 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 2 times

≡  **james2033** 4 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** 5 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 4 times

 **Jeeva28** 6 months, 1 week ago

NAT Gateway will be created Public Subnet and Provide access to Private Subnet

upvoted 1 times

 **cheese929** 7 months ago

Selected Answer: A

A is correct.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-example-private-subnets-nat.html>

upvoted 1 times

 **Heric** 7 months, 2 weeks ago

Selected Answer: A

Now NAT Instances is avoided by AWS. Then choose the NAT Gateway

upvoted 3 times

 **alexiscloud** 8 months ago

A: NAT Gateway

upvoted 1 times

 **Rudraman** 8 months, 1 week ago

Selected Answer: A

NAT Gateway - AWS-managed NAT, higher bandwidth, high availability, no administration

upvoted 1 times

 **RODCCN** 9 months 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** 9 months ago

Refer:

<https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-scenarios.html#public-nat-gateway-overview>

Should be A.

upvoted 1 times

 **erik29** 10 months, 4 weeks ago

aaaaaa

upvoted 1 times

 **techhb** 11 months ago

Selected Answer: A

Networking 101, A is only right option

upvoted 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 4 times

 **career360guru** 11 months, 2 weeks ago

Option A

NAT gateway needs to be configured within each VPC's in Public Subnet.

upvoted 1 times

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

BE (53%)	AB (42%)	4%
----------	----------	----

✉️  **123jh10** Highly Voted 1 year, 1 month 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 41 times

✉️  **Iconique** 2 months, 1 week 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 2 times

✉️  **attila9778** 1 year ago

Can someone explain why A is correct?
 EFS is spread across Availability Zones in a region, as per <https://aws.amazon.com/blogs/gametech/gearbox-entertainment-goes-remote-with-aws-and-perforce/>
 My question then is whether it makes sense to launch EC2 instances in the *same Availability Zone as the EFS file system* ?

upvoted 6 times

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

However, launching the EC2 instance in the same AZ as the EFS file system can provide some performance benefits, such as reduced network latency and improved throughput. Therefore, it may be a best practice to launch the EC2 instance in the same AZ as the EFS file system if performance is a concern.

upvoted 2 times

✉️  **BlueVolcano1** 10 months, 1 week ago

Yes exactly, that's why A doesn't make sense. I voted for B and E.

upvoted 4 times

✉️  **Lalo** 9 months, 2 weeks ago

CORRECT ANSWER: B&E

Steps 4 &5

https://aws.amazon.com/datasync/getting-started/?nc1=h_ls

upvoted 9 times

✉️  **RBSK** 11 months, 2 weeks ago

will A,B work without E?

upvoted 3 times

✉️  **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 29 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 11 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 7 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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

 **MiniYang** Most Recent  1 week 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 2 times

 **t0nx** 1 week 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 1 times

 **xdkonorek2** 3 weeks, 4 days 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** 2 months, 2 weeks ago

Selected Answer: BD

BE is the correct answer
upvoted 1 times

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

<https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-associate-saa-c03/view/11/#>
upvoted 1 times

✉ **Raggz** 3 months, 1 week ago

Selected Answer: AE

A. Launch the EC2 instance into the same Availability Zone as the EFS file system and E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.
These two steps in combination should be taken to automate this task. Launching the EC2 instance into the same Availability Zone as the EFS file system ensures that the instance has low latency access to the file system. AWS DataSync can then be used to automate the transfer of data from the on-premises SFTP server to the EFS file system on the EC2 instance. DataSync is an easy-to-use data transfer service that simplifies, automates, and accelerates moving large amounts of data into and out of AWS services such as Amazon S3, Amazon Elastic File System (Amazon EFS), and Amazon FSx for Windows File Server. The other options are not relevant or do not provide an automated solution for migrating the data center to AWS.

This is AI response, Is this correct?

upvoted 1 times

✉ **Abdou1604** 3 months, 2 weeks ago

C is good , Amazon CloudFront is a content delivery network (CDN) service that helps distribute content globally with low latency and high data transfer speeds. By configuring your website to use CloudFront, your website's traffic can be distributed across multiple edge locations around the world. This not only improves user experience by reducing latency but also provides protection against DDoS attacks. CloudFront is designed to absorb and mitigate DDoS attacks by distributing traffic across its network of edge locations.

upvoted 1 times

✉ **james2033** 4 months, 1 week ago

Selected Answer: BE

Keyword "AWS DataSync" . Choose B and E, where has this keyword. NFS stands for "Network File System". SFTP stands for "Secure Fiel Transfer Protocol". AWS DataSync <https://aws.amazon.com/datasync/> , it is suitable for migration data from on-premises to AWS cloud.
upvoted 1 times

✉ **cookieMr** 5 months, 1 week ago

Selected Answer: BE

B. By installing an AWS DataSync agent in the on-premises data center, the architect can establish a secure connection between the on-premises environment and AWS.

E. Once the DataSync agent is installed, the solutions architect should configure it to create a suitable location configuration that specifies the source location as the on-premises SFTP server and the target location as the EFS. AWS DataSync will handle the secure and efficient transfer of the data from the on-premises server to the EC2 using EFS.

A. Launching EC2 into the same AZ as the EFS is not directly related to automating the migration task.

C. Creating a secondary EBS on the EC2 for the data is not necessary when using EFS. EFS provides a scalable, fully managed NFS-based file system that can be mounted directly on the EC2, eliminating the need for separate EBS.

D. It would require manual intervention and could be error-prone, especially for large amounts of data.

upvoted 2 times

✉ **Anmol_1010** 5 months, 1 week ago

Efs is launched in same region so.answer is option AB

upvoted 1 times

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

Selected Answer: BE

B: DataSync to copy the data automatically
E: DataSync discovery job to identify how / where to store your data automatically
<https://docs.aws.amazon.com/datasync/latest/userguide/getting-started-discovery-job.html>
upvoted 1 times

✉ **antropaws** 6 months ago

Selected Answer: BE

A is irrelevant given the scenario.
upvoted 1 times

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

Selected Answer: BE

Datasync configuration are required

upvoted 1 times

✉  **shinejh0528** 7 months ago

Selected Answer: BE

A : same AZ? why?

upvoted 1 times

✉  **kruasan** 7 months, 1 week ago

Selected Answer: BE

B* To access your self-managed on-premises or cloud storage, you need an AWS DataSync agent that's associated with your AWS account.
<https://docs.aws.amazon.com/datasync/latest/userguide/configure-agent.html>

E* A location is a storage system or service that AWS DataSync reads from or writes to. Each DataSync transfer has a source and destination location.

<https://docs.aws.amazon.com/datasync/latest/userguide/configure-agent.html>

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 34 times

✉  **cookieMr** Highly Voted 5 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 6 times

✉  **Ruffyit** Most Recent 1 month ago

<https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html>

upvoted 1 times

✉  **Guru4Cloud** 3 months, 2 weeks 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** 7 months ago

Selected Answer: A

Job bookmark to make sure that the glue job will not process already processed files.

upvoted 1 times

✉  **Heric** 7 months, 2 weeks 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** 8 months 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** 11 months ago

Delete files in S3 freely is not good. so B is not correct,

upvoted 1 times

✉️ **techhb** 11 months ago

Selected Answer: A

A is correct

upvoted 1 times

✉️ **Buruguduystunstugudunstuy** 11 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** 11 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

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

Selected Answer: A

It's obviously A. Bookmarks serve this purpose

upvoted 1 times

✉️ **Wpcorgan** 1 year ago

A is correct

upvoted 2 times

✉️ **LeGlopier** 1 year, 1 month ago

Selected Answer: A

A

<https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html>

upvoted 3 times

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*

AC (83%) Other

✉  **alvarez100**  1 year, 1 month 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 24 times

✉  **attila9778** 1 year 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 19 times

✉  **Buruguduystunstugudunstuy**  11 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 9 times

✉  **xdkonorek2**  3 weeks, 4 days ago

Selected Answer: AC

A - use aws shield advanced for DDoS protection, but it cannot be used with EC2 instace 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** 1 month ago

DDoS attack will choose the AWS Shield Advanced

Cloudfront have attached the WAF

upvoted 1 times

✉  **Devsin2000** 2 months 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

✉  **TariqKipkemei** 3 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

✉  **mtnayer** 3 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

✉  **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: AC

Cloud front supports SHIELD ADVANCED integration
upvoted 1 times

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

Cloud front supports SHIELD ADVANCED integration
upvoted 1 times

✉  **Aash24** 4 months, 3 weeks ago

Selected Answer: D

D should be the one here
upvoted 3 times

✉  **cookieMr** 5 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 2 times

✉  **Heric** 7 months, 2 weeks ago

Selected Answer: AC

Key word:
DDoS attack will choose the AWS Shield Advanced
Cloudfront have attached the WAF
upvoted 2 times

✉  **jdr75** 7 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

✉  **Khushna** 9 months, 1 week ago

Selected Answer: AC

DDos is better with shield and Cloudfront also provide protection for ddos
upvoted 1 times

✉  **CloudForFun** 11 months, 1 week 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** 11 months, 2 weeks ago

A and C as your will need to configure Cloudfront to activate AWS Advance Shield
upvoted 1 times

 **ishitamodi4** 11 months, 2 weeks ago

AC, AWS Shield Advanced is available globally on all Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 edge locations worldwide
upvoted 1 times

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 (98%)

123jh10 Highly Voted 1 year, 1 month 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 26 times

Buruguduystunstugudunstuy Highly Voted 11 months, 1 week 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 14 times

Buruguduystunstugudunstuy 11 months, 1 week 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 11 times

MiniYang Most Recent 1 week 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 1 times

Evonne_HY 2 months, 2 weeks 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 2 months, 1 week 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 3 months, 2 weeks 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** 4 months, 2 weeks ago

D

* is BIG NO. And we are talking about policy --> hence D

upvoted 2 times

✉️ **cookieMr** 5 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** 6 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** 6 months, 4 weeks ago

Since its for Lamda which is a resource, resource policy is the trick

upvoted 2 times

✉️ **bdp123** 9 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/eventbridge/latest/userguide/resource-based-policies-eventbridge.html#lambda-permissions>

upvoted 1 times

✉️ **gustavtd** 11 months ago

Selected Answer: D

The definition scope of D is the smallest, so is it

upvoted 1 times

✉️ **techhb** 11 months ago

Selected Answer: D

events.amazonaws.com is principal for eventbridge

upvoted 1 times

✉️ **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉️ **wly_al** 11 months, 2 weeks ago

least privilege meant the role cannot be "*". answer B only mention lambda. so the answer was D

upvoted 1 times

✉️ **ocbn3wby** 1 year 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

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

D (90%)	10%
---------	-----

✉️  **123jh10** Highly Voted 1 year, 1 month 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 15 times

✉️  **vadiminski_a** 11 months, 2 weeks ago

In addition you cannot log key usage in B, for A I am not certain

upvoted 1 times

✉️  **ocbn3wby** 1 year ago

Thank you for the explanation.

upvoted 1 times

✉️  **rcttryk** Most Recent 1 day, 13 hours 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

✉️  **Guru4Cloud** 3 months, 2 weeks 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 2 times

✉️  **cookieMr** 5 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 4 times

✉️  **SilentMilli** 10 months, 3 weeks 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** 11 months ago

Selected Answer: B

Amazon 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

✉ **Burugduystunstugudunstuy** 11 months, 1 week 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 1 times

✉ **Burugduystunstugudunstuy** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉ **Berny** 11 months, 2 weeks 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** 11 months, 3 weeks 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** 11 months, 1 week 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 ago

Selected Answer: D

Agree Also, SSE-S3 cannot be audited.

upvoted 2 times

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

B (49%)	D (42%)	9%
---------	---------	----

✉  **ArielSchivo**  1 year, 1 month 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 68 times

✉  **bullrem** 10 months, 1 week 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 5 times

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

B might work but D works better. B requires 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 Kinesis flexible API (<https://aws.amazon.com/documentation-overview/kinesis-data-analytics/>)

upvoted 4 times

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

Also by using kinesis the analytics platform will have a storing buffer to take & process data through the kinesis API. The lambda approach in the B scenario is too wide and leaves many loose ends.

upvoted 2 times

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

You are right, but it clearly says "store data".
AWS Lambda don't store data, Kinesis does.

upvoted 4 times

✉  **ces26015** 10 months, 1 week ago

I don't understand the use of a lambda function here, maybe if there would be a need to transform the data, can you explain?

upvoted 4 times

✉  **Six_Fingered_Jose**  1 year, 1 month ago

Selected Answer: D

I don't 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 44 times

✉  **JackLo** 2 months, 2 weeks ago

B is more appropriate than D because the question contains to retrieve, Kinesis doesn't have such function, Lambda can set custom function as you like

upvoted 1 times

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

B might work but D works better. B requires 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. API supports integration with several languages.

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 1 times

✉ **MutiverseAgent** 4 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 1 times

✉ **aadityaravi8** 5 months ago

100% agree
upvoted 1 times

✉ **JiyuKim** 9 months, 3 weeks ago

But KDA also cannot store data.
upvoted 2 times

✉ **vipyodha** 5 months, 1 week ago

kda can store data with retention period
upvoted 1 times

✉ **xdkonorek2** Most Recent ⓘ 3 weeks, 3 days 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 possiblity to read a data point from it
https://docs.aws.amazon.com/kinesisanalytics/latest/dev/API_Operations.html

upvoted 1 times

✉ **slimen** 3 weeks, 5 days ago

Selected Answer: B

the do have an analytic platform, adding keneses = more money + more operational overhead

upvoted 1 times

✉ **ZZNZ** 1 month, 2 weeks ago

Selected Answer: B

"The company wants to use these data points in its existing analytics platform"

upvoted 1 times

✉ **tom_cruise** 1 month, 2 weeks ago

Selected Answer: D

If you choose the lambda function, where does it pull data from?

upvoted 1 times

✉ **slimen** 3 weeks, 5 days ago

the data is being sent to API gateway using REST
API GW will send data to Lambda
Lambda wills end data to the existing analytic platform

they have an analytic platform already, Kenises is not needed

upvoted 1 times

✉ **MOSHE** 1 month, 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** 1 month, 3 weeks ago

Selected Answer: D

i think the answer is D because of the storing data requirement

upvoted 1 times

✉ **vijaykamal** 2 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

 **rushiwaman95** 2 months ago

tracking = real time
upvoted 1 times

 **chandu7024** 2 months, 1 week ago

It should be D.
upvoted 1 times

 **kambarami** 2 months, 3 weeks ago

Answer is D.
Amazon Kinesis Data Streams is a serverless streaming data service that simplifies the capture, processing, and storage of data streams at any scale.
Kinesis Data Firehose.
upvoted 1 times

 **sonyaws** 3 months ago

Selected Answer: B

Correction required in question: Which action meets these requirements for sorting(*not storing) and retrieving location data?

- Lambda function does the sorting and retrieving
 - API Gateway exposes a RestAPI to call the Lambda function
- upvoted 1 times

 **Stevey** 3 months, 1 week ago

Selected Answer: D

D because a storage solution is required.
B. Lamda is not a storage solution.
upvoted 2 times

 **karloscetina007** 3 months, 2 weeks ago

Selected Answer: D

D is the correct answer. Lambda can not store the infotmation for analysis, instead API gateway and Kinesis could do that years ago.
upvoted 2 times

 **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: D

The best option is to use Amazon API Gateway with Amazon Kinesis Data Analytics.

Amazon API Gateway provides a REST API that can be used to ingest and retrieve the location data points. Kinesis Data Analytics can then process and analyze those data streams in real-time. The results can be queried through the API Gateway, meeting the requirements.
upvoted 2 times

 **ack1** 3 months, 3 weeks ago

Selected Answer: D

D is right answer
upvoted 2 times

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

A (61%)

D (36%)

✉  **romko** Highly Voted  1 year 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 64 times

✉  **Evonne_HY** 2 months, 1 week ago

RDS event notification is supporting object deletion. What's more, it is saying the listing will be removed rather than update, so D is correct.
Here's the link for event notification categories link:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.ListingCategories.html
upvoted 1 times

✉  **BartoszGolebiowski24** 1 month ago

RDS event notification does not send an event when a record is deleted. RDS event notifications are used to provide notification when an Amazon RDS event occurs.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_Events.overview.html
upvoted 1 times

✉  **ruqui** 6 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 13 times

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

Wow, great find romko. Didn't realize that Event notification doesn't notify when the data is changed, it notifies when major changes at DB level occur like settings etc
upvoted 1 times

✉  **nauman001** 8 months ago

Listing the Amazon RDS event notification categories.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.ListingCategories.html:
upvoted 1 times

✉  **ksolovoyov** Highly Voted  10 months, 4 weeks 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 8 times

✉  **BlueVolcano1** 10 months, 1 week 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** 10 months, 1 week 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

✉ **Fizbo** Most Recent 1 week 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** 3 weeks, 3 days 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** 3 weeks, 5 days 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 won't send to multiple targets at the same time

is you go for 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 2 times

✉ **liux99** 3 weeks, 6 days 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 weeks ago

In my opinion, there is no complete solution provided, whether it is d or a

upvoted 1 times

✉ **tom_cruise** 4 weeks, 1 day 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

✉ **lqw** 1 month, 2 weeks ago

Selected Answer: D

1 SNS to multiple SQS, each SQS has a subscriber application...

upvoted 2 times

✉ **tom_cruise** 1 month, 2 weeks ago

Selected Answer: C

A is wrong because once the message in SQS consumed by one target, it is gone. What about the rest targets? D is wrong, fan out to multiple SQS queues does not make sense. It can be done by the SNS.

upvoted 3 times

✉ **David_Ang** 1 month, 2 weeks ago

Selected Answer: A

In option C and D from the original question, the use of Amazon SNS and Amazon SQS together might not be necessary, and it could introduce complexity. These options involve sending RDS event notifications to SNS topics and then fanning out to multiple SQS queues. While this approach can work, it adds an additional layer of complexity and might not be the most straightforward solution for the use case described.

Option A, on the other hand, directly uses AWS Lambda functions triggered by RDS updates to send data to an SQS queue. It simplifies the architecture and is often more straightforward for scenarios where you need to process and send data to multiple consumers when a database is updated.

so "A" is correct.

upvoted 1 times

✉ **Amitabha09** 1 month, 3 weeks ago

The correct answer 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 is the most scalable and reliable way to send the data to multiple target systems. It also decouples the database from the target systems, which makes the system more resilient to failures.

Amazon RDS event notifications allow you to publish events to Amazon SNS topics when certain events occur in your RDS database. For example, you can publish an event when a new record is inserted, updated, or deleted.

upvoted 3 times

✉ **rlaisqls** 2 months ago

Selected Answer: D

I think D is more recommended by AWS than C.

It should be send data to multiple consumer, A is definitely not.

<https://docs.aws.amazon.com/sns/latest/dg/sns-sqs-as-subscriber.html>

upvoted 4 times

✉ **mtmayer** 3 months, 1 week ago

Selected Answer: D

..... data must be sent to multiple target systems. = SNS

upvoted 3 times

✉ **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: A

There is RDS Fanout to SNS, but not specifically for DB level events (write, reads, etc).

It can fan out events at instance level (turn on, restart, update), cluster level (added to cluster, removed from cluster, etc). But not at DB level.

More detailed event list here:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.Messages.html

Correct answer is A

upvoted 1 times

✉ **cookieMr** 4 months, 2 weeks ago

Selected Answer: D

Fanout -> SNS + SQS

upvoted 3 times

✉ **aadityaravi8** 5 months ago

Answer should be C

When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems - it can be done through SQS polling option, as soon as it is processed, it will be removed and won't be picked up by another node of lambda for further processing. i.e Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics

upvoted 4 times

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 (82%)

B (18%)

 **123jh10** Highly Voted 1 year, 1 month 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 26 times

 **PassNow1234** 11 months, 1 week 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** Highly Voted 1 year, 1 month ago

typo -- 10 delete the objects => TO delete the objects
 upvoted 13 times

 **oddnoises** 2 months ago

they were trying to speak in binary lol
 upvoted 2 times

 **Abitek007** Most Recent 1 month, 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** 3 months 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 1 times

 **Guru4Cloud** 3 months, 2 weeks 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** 4 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** 6 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** 9 months ago

Selected Answer: D

The correct answer is D.

upvoted 1 times

 **Whericanstart** 9 months 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** 3 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** 9 months, 2 weeks 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** 9 months, 2 weeks 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** 10 months, 3 weeks 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** 4 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** 10 months, 3 weeks 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** 11 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** 11 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

 **Silvestr** 11 months, 1 week ago

Selected Answer: B

Correct answer : B

Retention mode - Governance:

- Most users can't overwrite or delete an object version or alter its lock settings
- Some users have special permissions to change the retention or delete the object

upvoted 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Selected Answer: B

To meet the requirements specified in the question, the solution architect should choose Option 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.

S3 Object Lock is a feature of Amazon S3 that allows you to apply a retention period to objects in your bucket, during which time the objects cannot be deleted or overwritten. By enabling versioning on the bucket, you can ensure that all versions of an object are retained, including any deletions or overwrites. By setting a retention period of 100 years, you can ensure that the objects remain unchangeable for a long time.

By using governance mode as the default retention mode for new objects, you can ensure that the retention period is applied to all new objects that are uploaded to the bucket. This will prevent the objects from being deleted or overwritten until the retention period expires.

upvoted 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Why other options are wrong

Option A (creating an S3 Glacier vault and applying a WORM vault lock policy) would not meet the requirement to prevent the objects from being changed, because S3 Glacier is a storage class for long-term data archival and does not support read-write operations.

Option C (using CloudTrail to track API events and restoring modified objects from backup versions) would not prevent the objects from being changed in the first place.

Option D (adding a legal hold and the s3:PutObjectLegalHold permission to IAM policies) would not meet the requirement to prevent the objects from being changed for a nonspecific amount of time.

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Legal holds are used to prevent objects that are subject to legal or compliance requirements from being deleted or overwritten, even if their retention period has expired. While legal holds can be useful for preventing the accidental deletion of important objects, they do not prevent the objects from being changed. S3 Object Lock can be used to prevent objects from being deleted or overwritten for a specified retention period, but a legal hold does not provide this capability.

In addition, the s3:PutObjectLegalHold permission allows users to place a legal hold on an object, but it does not prevent the object from being changed. To prevent the objects from being changed for a nonspecific amount of time, the solution architect should use S3 Object Lock and set a longer retention period on the objects.

upvoted 3 times

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

BD (50%)

CD (48%)

 **Buruguduystunstugudunstuy** Highly Voted  11 months, 1 week 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 33 times

 **jdr75** 7 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 5 times

 **EricYu2023** 7 months, 2 weeks ago

Presigned URL can be use for upload.

upvoted 3 times

 **PoisonBlack** 7 months ago

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

upvoted 3 times

 **AF_1221** 7 months ago

preassigned URL is for upload or download for temporary time and for specific users outside the company

upvoted 2 times

 **AF_1221** 7 months ago

but for temporary purpose not for permanent

upvoted 3 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 3 times

 **MutiverseAgent** 4 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** 9 months, 2 weeks 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 3 times

 **fkie4** Highly Voted  8 months, 3 weeks 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 17 times

 **slimen** Most Recent  3 weeks, 5 days ago

Selected Answer: BD

pre-signed URL is temporary

decoupling meas preventing server from uplaoding and doing the resizing at the same time
so separating the processing into 2 parts (uplaod, then notify, then resize) is considered decoupling

upvoted 1 times

 **xplusfb** 1 month, 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** 2 months, 1 week ago

Selected Answer: CD

CD is correct

upvoted 1 times

 **numark** 2 months, 3 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 2 times

 **MarcusLEK** 2 months, 3 weeks ago

Selected Answer: BD

while technically its possible to upload with pre-signed urls, its 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 3 times

 **judyda** 2 months, 3 weeks ago

Selected Answer: CD

https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/PresignedUrlUploadObject.html

upvoted 1 times

 **KawtarZ** 3 months ago

C is not correct. the pre-signed urls are for download only, not upload.

upvoted 1 times

 **Iconique** 2 months, 1 week ago

wrong, they both for upload/download.

upvoted 2 times

 **TariqKipkemei** 3 months 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** 3 weeks, 5 days ago

pre-signed URL is temporary

decoupling meas preventing server from uplaoding and doing the resizing at the same time

so separating the processing into 2 parts (uplaod, then notify, then resize) is considered decoupling

upvoted 1 times

✉  **mtmayer** 3 months, 1 week ago

Selected Answer: CD

CD is much more efficient.

upvoted 1 times

✉  **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: BD

Correct answers are BD

upvoted 1 times

✉  **ofdengiz** 4 months, 1 week ago

Selected Answer: CD

I'll go with C,D

B still involves the EC2 instances handling the image uploads and resizing, which does not improve website performance and increases coupling within the application.

upvoted 1 times

✉  **sosda** 4 months, 2 weeks ago

Selected Answer: BD

presign url is not operational efficient

upvoted 1 times

✉  **vini15** 4 months, 2 weeks ago

I will go with B and D. Pre signed URL is temporary thing.

A presigned URL remains valid for the period of time specified when the URL is generated. If you create a presigned URL with the Amazon S3 console, the expiration time can be set between 1 minute and 12 hours. If you use the AWS CLI or AWS SDKs, the expiration time can be set as high as 7 days.

upvoted 1 times

✉  **Kostya** 5 months, 2 weeks ago

Selected Answer: BD

Correct answers are BD

upvoted 1 times

✉  **omoakin** 6 months, 1 week ago

BC BC BC

upvoted 1 times

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 (97%)

✉️  **123jh10** Highly Voted 1 year, 1 month 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 15 times

✉️  **Ruffyit** Most Recent 1 month 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 1 times

✉️  **prabhjot** 1 month, 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

✉️  **TariqKipkemei** 3 months ago

Selected Answer: D

HIGHEST availability. Definitely option D.

upvoted 1 times

✉️  **Guru4Cloud** 3 months, 2 weeks 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 1 times

✉️  **Guru4Cloud** 3 months, 2 weeks 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** 4 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** 4 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** 5 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** 5 months, 2 weeks ago

Selected Answer: D

Correct answer D

upvoted 1 times

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

Auto scaling and Multi-AZ enabled for high availability.

upvoted 1 times

 **Erbug** 8 months, 2 weeks 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** 10 months, 1 week ago

Selected Answer: D

D as the Auto Scaling group offer the highest availability between all solutions

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 2 times

 **Wpcorgan** 1 year ago

D is correct

upvoted 1 times

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, 1 month 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 14 times

✉️  **cosmiccliff**  3 weeks, 5 days 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** 1 month 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** 3 months ago

Selected Answer: A

LEAST operational overhead = AWS Fargate
upvoted 1 times

✉️  **Guru4Cloud** 3 months, 2 weeks 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** 3 months, 2 weeks 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** 4 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** 4 months, 2 weeks ago

A

Fargate, ECS, ASG, ALB....What else one will need for a nice sleep?

upvoted 2 times

✉ **cookieMr** 5 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** 6 months, 1 week 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** 6 months, 3 weeks ago

Selected Answer: A

Least Operational Overhead = Serverless

upvoted 1 times

✉ **airraid2010** 8 months, 2 weeks 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** 9 months, 3 weeks ago

A is correct

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 11 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 2 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: A

Option A has minimum operational overhead and almost no application code changes.

upvoted 1 times

✉ **Wpcorgan** 1 year ago

A is correct

upvoted 1 times

✉ **Six_Fingered_Jose** 1 year, 1 month 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

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 (69%)

D (31%)

✉️  **123jh10**  1 year, 1 month 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 45 times

✉️  **remand** 10 months 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 6 times

✉️  **jdr75** 7 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 2 times

✉️  **goodmail**  10 months, 2 weeks 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 10 times

✉️  **Shalen**  2 days 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 over head " hence C would be reinventing the weel

upvoted 1 times

✉️  **slimen** 3 weeks, 5 days 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 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** 1 month, 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 support compute resources

upvoted 3 times

 **TariqKipkemei** 3 months 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** 3 weeks, 5 days 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** 3 months, 2 weeks 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** 4 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 1 times

 **small_zipgenius** 4 months, 4 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** 4 months, 3 weeks ago

D answer says Snowball Edge STORAGE Optimized, which supports 80TB. 39.5TB is for the Snowball Edge COMPUTE Optimized.

upvoted 2 times

 **live_reply_developers** 5 months 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** 4 months, 3 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** 5 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** 4 months, 3 weeks ago

My thoughts exactly. I think people are misunderstanding CONFIG for OPERATION overhead.

upvoted 1 times

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

Selected Answer: C

Correctly answer is C.

"The data center does not have any available network bandwidth for additional workloads."

upvoted 1 times

✉️  **KMohsoe** 6 months, 2 weeks ago

Option is C.

"The data center does not have any available network bandwidth for additional workloads."

D is new EC instance is need to created. So I choose option C.

upvoted 1 times

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

Selected Answer: C

LEAST operational overhead = Serverless = Glue

upvoted 3 times

✉️  **SkyZeroZx** 7 months ago

Selected Answer: D

Exist " A custom application in the company's data center runs a weekly data transformation job"

Because existing previous app rebuild with Glue is more effort

Ans D

upvoted 1 times

✉️  **darn** 7 months, 1 week ago

Selected Answer: C

D is far too manual, lots of overhead

upvoted 2 times

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** Highly Voted 1 year, 1 month ago

Selected Answer: C

Do not store images in databases ;)... correct answer should be C

upvoted 32 times

✉️  **cookieMr** Highly Voted 5 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 5 times

✉️  **aptx4869** Most Recent 1 month ago

Selected Answer: C

Images (Object) should go in S3 and metadata should go in database (DynamoDB)

upvoted 1 times

✉️  **Ruffyit** 1 month 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** 1 month ago

Selected Answer: C

Solution C

upvoted 1 times

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

Selected Answer: C

A does not store data.

upvoted 1 times

✉  **TariqKipkemei** 3 months ago

Selected Answer: C

I stopped at option C

upvoted 1 times

✉  **sand444** 3 months ago

Selected Answer: C

c is correct

upvoted 1 times

✉  **Abdou1604** 3 months, 1 week ago

DynamoDB can technically store images as binary data (BLOBs)

upvoted 1 times

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

Selected Answer: C

Why one would store photos in DB

upvoted 2 times

✉  **MNotABot** 4 months, 2 weeks ago

This one is in exam

upvoted 5 times

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

Selected Answer: C

Option C is the best.

upvoted 1 times

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

Selected Answer: C

C is the correct answer, A can't store images in DB

upvoted 1 times

✉  **cheese929** 7 months ago

Selected Answer: C

Go for C which is able to scale

upvoted 1 times

✉  **TheAbsoluteTruth** 8 months 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** 5 months, 1 week ago

Si Señor Siarra!

upvoted 1 times

✉  **TheAbsoluteTruth** 8 months ago

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 1 times

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** Highly Voted 5 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 7 times

 **Ruffyit** Most Recent 1 month 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** 3 months 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** 3 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** 11 months, 1 week ago

Selected Answer: C

According to the well-designed framework, option C is the safest and most efficient option.

upvoted 3 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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** 10 months, 3 weeks 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

 **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **ocbn3wby** 1 year 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 ago

C is correct

upvoted 1 times

 **Jtic** 1 year ago

Selected Answer: C

Use VPC endpoint

upvoted 1 times

 **Jtic** 1 year ago

Selected Answer: C

User VPC endpoint and make the EC2 private

upvoted 1 times

 **Jtic** 1 year ago

Use VPC endpoint

upvoted 1 times

 **backbencher2022** 1 year 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

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

AD (81%)

Other

 **palermo777** Highly Voted 1 year, 1 month 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 27 times

 **Six_Fingered_Jose** Highly Voted 1 year, 1 month 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 5 times

 **Lalo** 5 months, 3 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

 **aussiehoa** 6 months, 3 weeks ago

does not need to have any dynamic content available
upvoted 1 times

 **David_Ang** Most Recent 1 month, 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** 1 month, 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** 3 months 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 1 times

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

Selected Answer: AD

AD

A for enhanced security D for static content

upvoted 1 times

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

Selected Answer: AD

LEAST operational overhead = Serverless

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

upvoted 2 times

✉ **angolateoria** 7 months ago

AD misses the operational part, how can the app work without a lambda function, an EC2 instance or something?

upvoted 1 times

✉ **darn** 7 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** 7 months, 3 weeks ago

Selected Answer: AD

A for enhanced security

D for static content

upvoted 2 times

✉ **Erbug** 8 months, 2 weeks 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** 9 months, 1 week ago

I vote A & C for the reason being least operational overhead.

upvoted 1 times

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

Selected Answer: AD

Here a perfect explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>

upvoted 2 times

✉ **Abdel42** 10 months ago

Selected Answer: AD

Simple and secure

upvoted 1 times

✉ **remand** 10 months, 2 weeks 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** 11 months, 1 week 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** 11 months, 1 week 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

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

A (65%)

C (33%)

  Six_Fingered_Jose  1 year, 1 month 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 69 times

  Zerotn3 11 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 9 months, 2 weeks ago

that is not true, you can stream logs from CloudWatch Logs directly to OpenSearch

upvoted 5 times

  HayLLIHuK 11 months ago

Zerotn3 is right! There should be a Lambda for writing into ES

upvoted 1 times

  UWSFish 1 year, 1 month ago

Great link. Convinced me

upvoted 5 times

  Buruguduystunstugudunstuy  11 months, 1 week 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 16 times

  Lalo 5 months, 3 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

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 10 months ago

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 1 times

 **Marco_St** Most Recent 1 week 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 weeks, 1 day ago

Selected Answer: C

You need real time buffer like Kinesis, otherwise you are going to lose data.

upvoted 1 times

 **mhka1988** 1 month, 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** 1 month, 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 1 times

 **tom_cruise** 1 month, 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** 1 month, 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 1 times

 **JKevin778** 2 months ago

Selected Answer: C

100% C.

CloudWatch logs cannot be sent 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** 2 months, 2 weeks ago

Selected Answer: C

The answer is C

upvoted 1 times

 **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: C

C is the correct answer.

Using Kinesis Data Firehose will allow near real-time delivery of the CloudWatch logs to Amazon Elasticsearch Service with the least operational overhead compared to the other options.

Firehose can be configured to automatically ingest data from CloudWatch Logs into Elasticsearch without needing to run Lambda functions or install agents on the application servers. This makes it the most operationally simple way to meet the stated requirements.

upvoted 1 times

 **npraveen** 4 months, 1 week ago

Selected Answer: C

Near Real Time: Cloud watch logs --> Subscription Filter --> Kinesis data fire house --> S3

Real Time: Cloud watch logs --> Subscription Filter --> Lambda --> S3

upvoted 2 times

 **Cloudnative9990** 4 months, 2 weeks ago

We need to consider the "least operation overhead" and with that said Cloudwatch log Group and OpenSearch is already existing in the system and needs integration. Kinesis is preferable for near real time streaming but it will be additional overhead..Hence answer should be A

upvoted 2 times

 **bala_s** 4 months, 3 weeks ago

Answer is A . The question says near real time and not real time

You can also use a CloudWatch Logs subscription to stream log data in near real time to an Amazon OpenSearch Service cluster. For more information, see Streaming CloudWatch Logs data to Amazon OpenSearch Service.

upvoted 1 times

 **bigboi23** 4 months, 3 weeks ago

Selected Answer: C

OPTION C

You can use subscriptions to get access to a real-time feed of log events from CloudWatch Logs and have it delivered to other services such as an Amazon Kinesis stream, an Amazon Kinesis Data Firehose stream, or AWS Lambda for custom processing, analysis, or loading to other systems.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html>

upvoted 1 times

 **cookieMr** 5 months, 1 week ago

By configuring a CloudWatch Logs subscription, you can stream the logs from CloudWatch Logs to Amazon OpenSearch Service in near-real-time. This solution requires minimal operational overhead as it leverages the built-in functionality of CloudWatch Logs and Amazon OpenSearch Service for log streaming and indexing.

Option B (Creating an AWS Lambda function) would involve additional development effort and maintenance of a custom Lambda function to write the logs to Amazon OpenSearch Service.

Option C (Creating an Amazon Kinesis Data Firehose delivery stream) introduces an additional service (Kinesis Data Firehose) that may not be necessary for this specific requirement, adding unnecessary complexity.

Option D (Installing and configuring Amazon Kinesis Agent) also introduces additional overhead in terms of manual installation and configuration on each application server, which may not be needed if the logs are already stored in CloudWatch Logs.

In summary, option A is the correct choice as it provides a straightforward and efficient way to stream logs from CloudWatch Logs to Amazon OpenSearch Service with minimal operational overhead.

upvoted 3 times

 **srijrao** 5 months, 1 week ago

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html>

upvoted 1 times

 **konieczny69** 5 months, 2 weeks ago

Selected Answer: C

I vote for C.

Solution A add unnecessary hop

upvoted 1 times

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

D (94%) 6%

✉️  **Azure55** 4 weeks ago

Selected Answer: D

the cost of S3<EFS<EBS

upvoted 2 times

✉️  **awashenko** 1 month, 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 1 times

✉️  **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: D

MOST cost-effective = S3 (unless explicitly stated in the requirements)

upvoted 1 times

✉️  **cookieMr** 5 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 3 times

✉️  **Jeeva28** 6 months, 1 week 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** 6 months, 1 week ago

EFS and S3 meet the requirements but S3 is a better option because it is cheaper.

upvoted 1 times

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

Selected Answer: D

MOST cost-effective = S3 (unless explicitly stated in the requirements)

upvoted 2 times

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

Selected Answer: D

S3 is the cheapest and most scalable.
upvoted 1 times

 **jdr75** 7 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** 7 months, 4 weeks ago

EFS is a good option but expensive alongside S3 and customer concerned about cost - thus: S3 (D)
upvoted 2 times

 **frenzoid** 8 months, 1 week ago

I wonder why people choose S3, yet S3 max capacity is 5TB 😕.
upvoted 1 times

 **frenzoid** 8 months, 1 week ago

My bad, the 5TB limit is for individual files. S3 has virtually unlimited storage capacity.
upvoted 6 times

 **Help2023** 9 months, 1 week 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** 10 months, 2 weeks 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** 10 months, 3 weeks 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** 11 months ago

Selected Answer: D

Is there anything cheaper than S3?
upvoted 3 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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

 **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

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 (74%)

A (26%)

✉  **Gil80**  1 year 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 25 times

✉  **slimen** 3 weeks, 5 days ago

they didn't mention multiple accounts! only 2 regions

upvoted 1 times

✉  **Nigma**  1 year 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 15 times

✉  **JayBee65** 11 months, 1 week 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

✉  **slimen**  3 weeks, 5 days ago

Selected Answer: A

the question mentioned 2 regions not 2 accounts

WAF is more suitable here with less effort than Firewall Manager!

upvoted 1 times

✉  **cosmiccliff** 3 weeks, 5 days 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** 1 month 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

✉  **Abitek007** 1 month, 2 weeks ago

Selected Answer: A

you can as well use Firewall Manager, but the question says least operational overhead
upvoted 1 times

✉ **Valder21** 2 months, 4 weeks ago

Selected Answer: A

SQL injection, cross-site scripting = WAF
upvoted 1 times

✉ **Hassao0** 3 months ago

A is Right Option
<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-aws-waf.html>
upvoted 1 times

✉ **Guru4Cloud** 3 months, 2 weeks 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

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

Selected Answer: A

awf setting is region specific
upvoted 1 times

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

Selected Answer: B

if you want to manage protection accross accounts and resources then use AWS firewall manager. AWS WAF protect against web attacks like sql-injection and cross-site scripting
upvoted 1 times

✉ **cookieMr** 5 months, 1 week ago

Selected Answer: B

B. By setting up AWS Firewall Manager, you can centrally configure AWS WAF rules, which can be applied to multiple AWS accounts and Regions. This allows for efficient management and enforcement of security rules across accounts without the need for separate configuration in each individual Region.

Option A (Setting up AWS WAF with Regional web ACLs) requires setting up and managing AWS WAF in each Region separately, which increases administrative effort.

Option C (Setting up AWS Shield with Regional web ACLs) primarily focuses on DDoS protection and may not provide the same level of protection against SQL injection and cross-site scripting attacks as AWS WAF.

Option D (Setting up AWS Shield in one Region) provides DDoS protection but does not directly address protection against SQL injection and cross-site scripting attacks.

In summary, option B offers the most efficient and centralized approach by leveraging AWS Firewall Manager to configure AWS WAF rules across multiple Regions, minimizing administrative effort while ensuring protection against SQL injection and cross-site scripting attacks.

upvoted 1 times

✉ **omoakin** 6 months, 1 week ago

AAAAAAAAAAA
upvoted 2 times

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

Crazy community voting !
Correct answer is => A : AWS Firewall Manager security policies are region specific. Each Firewall Manager policy can only include resources available in that specified AWS Region.
upvoted 3 times

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

You can say that again. I will go with A as well
upvoted 1 times

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

B is the correct answer..
Among the options provided, option B offers the least amount of administrative effort to protect the API Gateway managed REST APIs from SQL injection and cross-site scripting attacks across multiple accounts.

AWS Firewall Manager allows you to centrally configure and manage AWS WAF rules across multiple accounts and resources. By setting up AWS Firewall Manager in both the us-east-1 and ap-southeast-2 Regions, you can apply consistent WAF rules to the API Gateway instances in those regions without the need to individually configure WAF rules for each API Gateway.

upvoted 1 times

 **TheAbsoluteTruth** 8 months ago

Selected Answer: B

La opción A proporciona protección contra inyecciones SQL y secuencias de comandos entre sitios utilizando AWS WAF, que es una solución de firewall de aplicaciones web. Sin embargo, esta opción requiere que se configure AWS WAF en cada región individualmente y se asocie una lista de control de acceso web (ACL) con una etapa de API. Esto puede resultar en un esfuerzo administrativo significativo si hay varias regiones y etapas de API que se deben proteger.

La opción B es una solución centralizada que utiliza AWS Firewall Manager para administrar las reglas de AWS WAF en múltiples regiones. Con esta opción, es posible configurar las reglas de AWS WAF en una sola ubicación y aplicarlas a todas las regiones relevantes de manera uniforme. Esta solución puede reducir significativamente el esfuerzo administrativo en comparación con la opción A.

upvoted 4 times

 **sezer** 8 months ago

Prerequisites for using AWS Firewall Manager

Your account must be a member of AWS Organizations

Your account must be the AWS Firewall Manager administrator

You must have AWS Config enabled for your accounts and Regions

To manage AWS Network Firewall or Route 53 resolver DNS Firewall, the AWS Organizations management account must enable AWS Resource Access Manager (AWS RAM).

can anybody explain me least Administration efficiency

i will go with A

if i am wrong anybody correct me

upvoted 1 times

 **jdr75** 7 months, 3 weeks ago

When they said "LEAST amount of administrative effort" they ignore the "transition costs" associated to get the final scenario. Only takes account the administration effort supposing all the migration task & prerequisites were done.

So B is probably, BEST.

upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/>

upvoted 1 times

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

B (73%)	A (23%)	4%
---------	---------	----

 **dokaedu** Highly Voted 1 year, 1 month ago

B is the correct one for self managed 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 13 times

 **MutiverseAgent** 4 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 2 times

 **MutiverseAgent** 4 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** 1 month, 1 week ago

Why I need replace NLB to ALB?

upvoted 1 times

 **LeGlopier** Highly Voted 1 year, 1 month ago

Selected Answer: B

for me it is B

upvoted 10 times

 **Masakichen** Most Recent 5 days, 17 hours 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 1 times

 **Ruffyit** 1 month 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** 1 month, 2 weeks ago

Selected Answer: B

Key: route traffic to all the EC2 instances
upvoted 2 times

 **Hassao** 3 months 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 2 times

 **Guru4Cloud** 3 months, 2 weeks 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** 4 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** 5 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** 5 months, 3 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 1 times

 **studynoplay** 6 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** 6 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** 7 months ago

Using self managed DNS - other three options talking about Route 53 so B can only B answer

upvoted 1 times

 **tonyexim** 7 months ago

I think both answer A and B is solutions
upvoted 1 times

 **EricYu2023** 7 months, 2 weeks ago

Selected Answer: B

The first half of Option A seems right. "Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs.", however, for the second part "Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin." , it's totally useless. Route 53 can use geolocation routing directly route request to the NLBs

upvoted 2 times

 **Musti35** 7 months, 2 weeks ago

Selected Answer: B

https://docs.aws.amazon.com/global-accelerator/?icmpid=docs_homepage_networking
explanation:

AWS Global Accelerator Documentation

AWS Global Accelerator is a network layer service in which you create accelerators to improve the security, availability, and performance of your applications for local and global users. Depending on the type of accelerator that you choose, you can gain additional benefits, such as improving availability or mapping users to specific destination endpoints.

upvoted 1 times

 **saransh_001** 8 months ago

Selected Answer: B

option A although mentions geolocation routing and would allow the company to route traffic based on the location of the user. However, the company has already implemented a self-managed DNS solution and wants to use NLBs for load balancing, so it may not be feasible for them to switch to Route 53 and CloudFront.

upvoted 1 times

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 (78%)

C (20%)

✉  **123jh10**  1 year, 1 month 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 42 times

✉  **JoeGuan** 3 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 1 times

✉  **Guru4Cloud** 3 months, 2 weeks ago

In simple terms, you double it the effort of your work and spending money by creating unnecessary snapshots... so A is the best choice

upvoted 1 times

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

How can A guarantee future encryption?

upvoted 2 times

✉  **Smart** 4 months, 1 week ago

Once DB is encrypted, newer snapshots and read replicas will also be encrypted.

upvoted 3 times

✉  **tom_cruise**  4 weeks, 1 day ago

Selected Answer: A

What's wrong with C is: "Copy the snapshots and enable encryption"

upvoted 1 times

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

Selected Answer: A

key: snapshots

upvoted 1 times

✉  **AntonioMinolfi** 1 month, 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%20it.)

ore.

upvoted 1 times

 **TMabs** 1 month, 3 weeks ago

A makes sence
upvoted 1 times

 **cookieMr** 5 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.
 - C. Copying snapshots to an encrypted S3 bucket only encrypts the snapshots, but does not address the encryption of the DB instance.
 - D. 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** 1 month 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** 6 months, 1 week 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]** 7 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

 **kruasan** 7 months, 1 week 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** 7 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 one as all you need is the latest snapshot.
upvoted 2 times

 **JoeGuan** 3 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** 7 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** 8 months, 1 week ago

Selected Answer: C
Encryption is enabled during the Copy process itself.
<https://repost.aws/knowledge-center/encrypt-rds-snapshots>
upvoted 1 times

 **Bang3R** 8 months, 1 week 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** 7 months, 3 weeks ago

BUT you can't restore encrypted snapshot to an existing DB instance. Only a 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 an existing one.

The RDB engine understands that restoring from an encrypted snapshot is to create an encrypted NEW database.

upvoted 2 times

 **TungPham** 8 months, 3 weeks 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** 8 months, 1 week 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** 9 months, 2 weeks 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

 **CaoMengde09** 9 months, 3 weeks ago

It's A for the following reasons :

--> To restore an Encrypted DB Instance from an encrypted snapshot we'll need to replace the old one - as we cannot enable encryption on an existing DB Instance

--> We have both Snap/Db Instance encrypted moving forward since all the daily Backups on an already encrypted DB Instance would be encrypted

upvoted 1 times

 **sassy2023** 10 months ago

Selected Answer: C

C is right

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.

Tools used to enable encryption:

AWS KMS key for encryption – When you create an encrypted DB instance, you can choose a customer managed key or the AWS managed key for Amazon RDS to encrypt your DB instance. If you don't specify the key identifier for a customer managed key, Amazon RDS uses the AWS managed key for your new DB instance. Amazon RDS creates an AWS managed key for Amazon RDS for your AWS account.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>

upvoted 2 times

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 Highly Voted 1 year, 1 month 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 18 times

ocbn3wby 1 year ago

Most documented answers. Thank you, 123jhl0.

upvoted 3 times

Ruffyit Most Recent 1 month 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 3 months, 2 weeks 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 5 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 7 months ago**Selected Answer: B**

B is correct.

upvoted 1 times

Buruguduystunstugudunstuy 11 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 4 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **Wpcorgan** 1 year ago

B is correct

upvoted 1 times

 **Wpcorgan** 1 year ago

B is correct

upvoted 1 times

 **Jtic** 1 year 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

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

D (95%) 5%

 **123jh10** Highly Voted 1 year, 1 month 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 15 times

 **Buruguduystunstugudunstuy** Highly Voted 11 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 10 times

 **Ruffyt** Most Recent 1 month 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 1 times

 **Guru4Cloud** 3 months, 2 weeks 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** 5 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** 9 months, 3 weeks ago

Selected Answer: A

Why is A wrong?

upvoted 2 times

 **xdkonorek2** 3 weeks, 2 days ago

ec2 instances still would be responsible for decrypting traffic and it wouldn't solve load issue

upvoted 1 times

 **Yadav_Sanjay** 7 months ago

Company uses its own SSL certificate. Option A says.. Create a SSL certificate in ACM

upvoted 2 times

 **remand** 10 months, 2 weeks 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** 11 months, 2 weeks ago

Selected Answer: D

Option D to offload the SSL encryption workload

upvoted 1 times

 **Aamee** 11 months, 3 weeks 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 ago

D is correct

upvoted 1 times

 **Six_Fingered_Jose** 1 year, 1 month ago

Selected Answer: D

agree with D

upvoted 1 times

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** Highly Voted 1 year 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 13 times

 **Evangelia** Highly Voted 1 year, 1 month ago

spot instances

upvoted 5 times

 **Ruffyit** Most Recent 1 month 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 1 times

 **tom_cruise** 1 month, 2 weeks ago

Selected Answer: A

key: can be started and stopped at any given time with no negative impact

upvoted 1 times

 **AbhilashDyadav** 1 month, 3 weeks ago

Selected Answer: A

Spot can do that

upvoted 1 times

 **Guru4Cloud** 3 months, 2 weeks 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** 5 months, 1 week 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** 5 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

✉ **alexiscloud** 8 months ago

Answer A:

typically takes upwards of 60 minutes total to complete.

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 11 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** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

✉ **Wpcorgan** 1 year ago

A is correct

upvoted 1 times

✉ **SimonPark** 1 year, 1 month ago

Selected Answer: A

A is the answer

upvoted 1 times

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.
- 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.

Correct Answer: CE

Community vote distribution

AD (54%)	A (21%)	AB (21%)	2%
----------	---------	----------	----

 **mabotega**  1 year 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 23 times

 **oguzbeliren** 4 months ago

D allows public internet access which is not desired. The answer is not d.

The most accurate answers are AB

upvoted 1 times

 **smd_** 7 months 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** 6 months, 1 week ago

B option wrong! NAT gateways must be created in public subnets!!

upvoted 6 times

 **x33** 2 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** 1 month, 1 week ago

NAT Gateway can't be used by EC2 instance in the same subnet (only from other subnets)

upvoted 3 times

 **AbhiJo** 1 year ago

We will require 2 private subnets, D does mention 1 subnet

upvoted 3 times

 **HayLLIHuK**  11 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 18 times

 **darn** 7 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

 **rlamberti** Most Recent 1 month, 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 1 times

 **RNess** 1 month, 1 week ago

Selected Answer: AD

AE

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

upvoted 1 times

 **tom_cruise** 1 month, 2 weeks ago

Selected Answer: AD

AE. There are two Ds, the last option should be E.

upvoted 1 times

 **tungnguyenduy** 3 months, 3 weeks ago

Selected Answer: AB

AB. should not be exposed to the public internet => private subnet

upvoted 1 times

 **ayrus1992** 4 months, 2 weeks ago

Selected Answer: C

CE

Highly Available and Secure

upvoted 1 times

 **bahaa_shaker** 3 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 ur answer

C is wrong answer b/c 1000000%

its A and D

upvoted 1 times

 **omerap12** 5 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** 5 months, 1 week 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** 5 months, 2 weeks ago

Selected Answer: AD

Second D so like E.

upvoted 1 times

 **fishy_resolver** 5 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** 6 months ago

Selected Answer: AD

AD because 2 NAT gateways in 2 public subnets in 2 AZs.

upvoted 2 times

 **bgsanata** 6 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** 6 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** 7 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** 7 months, 1 week 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

 **kruasan** 7 months, 1 week ago

Selected Answer: AB

In option B, an Application Load Balancer (ALB) is deployed in the private subnets, and two NAT gateways are configured across two Availability Zones to provide internet access to the instances in the private subnets. This allows the web tier to be accessed publicly through the ALB while still keeping the instances in private subnets. The NAT gateways act as a proxy between the instances and the internet, allowing only necessary traffic to pass through while blocking all other inbound traffic. This configuration provides additional security to the application by keeping the instances in private subnets and minimizing the exposure of the infrastructure to the public internet

upvoted 2 times

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

B (74%)	C (16%)	9%
---------	---------	----

✉  **rjam**  1 year 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 11 times

✉  **Abdou1604** 3 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

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

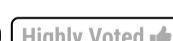
Just to clarify, my previous comment is about how answer B) might be correct and the MOST cheapest option under the correct configuration.

upvoted 1 times

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

Sorry, I meant answer C) might be correct

upvoted 1 times

✉  **Tela0**  1 year 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

✉  **Ruffyit**  1 month 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** 1 month, 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** 2 months, 4 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 1 times

✉ **cookieMr** 5 months, 1 week 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 1 times

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

Why not D

upvoted 2 times

✉ **RNess** 1 month, 1 week ago

"Data from the most recent 2 years must be highly available and immediately retrievable."

upvoted 1 times

✉ **RNess** 1 month, 1 week ago

Additionally,
S3 Standard Availability = 99.99%
S3 One Zone-IA Availability = 99.5%
upvoted 1 times

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

Selected Answer: B

B is the only one possible.
upvoted 1 times

✉ **rushlav** 7 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** 9 months, 3 weeks ago

It's pretty straight forward.

S3 Standard answers for High Availability/Immediate retrieval for 2 years. S3 Intelligent Tiering 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** 10 months ago

C appears to be appropriate - good case for intelligent tiering
upvoted 1 times

✉ **Robrobtutu** 7 months, 2 weeks 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

✉ **Sdraju** 8 months, 4 weeks 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

✉ **DaveNL** 10 months, 2 weeks 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** 11 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

 **Zerotn3** 11 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

 **hahahumble** 10 months, 2 weeks 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

 **Ello2023** 10 months, 2 weeks 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

 **Ifrad** 10 months, 3 weeks 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

 **k1kavi1** 11 months, 1 week ago

Selected Answer: B

B looks correct

upvoted 2 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **lapaki** 11 months, 3 weeks ago

Selected Answer: B

B. Most correct

upvoted 2 times

 **Cizzla7049** 1 year ago

Selected Answer: C

<https://aws.amazon.com/blogs/aws/s3-intelligent-tiering-adds-archive-access-tiers/>

upvoted 1 times

 **JayBee65** 11 months, 1 week ago

From your link "We added S3 Intelligent-Tiering to Amazon Amazon S3 to solve the problem of using the right storage class and optimizing costs when access patterns are irregular.". But access patterns are not irregular, they are clearly stated on the question, so this is not required.

upvoted 3 times

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

D (73%)

A (28%)

✉  **Sauran** Highly Voted 1 year, 1 month 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 24 times

✉  **michellemeloc** 7 months ago

Update: i3en.metal and i3en.24xlarge = 8 x 7500 GB (60TB)

upvoted 2 times

✉  **ishitamodi4** 11 months, 2 weeks 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** 11 months, 1 week 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** 11 months, 1 week 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** 6 months 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 1 times

✉  **Six_Fingered_Jose** Highly Voted 1 year, 1 month ago

Selected Answer: D

agree with D, since it is only used for video processing instance store should be the fastest here (being ephemeral shouldnt be an issue because they are moving the data to S3 after processing)

upvoted 7 times

✉  **Marco_St** Most Recent 6 days, 11 hours 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** 2 weeks, 5 days 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 1 times

✉ **Azure55** 4 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

✉ **tom_cruise** 4 weeks, 1 day 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

✉ **Ruffyit** 1 month ago

We are talkimng about storage here and EC2 instance store in not a viable solution for for a storage.

upvoted 1 times

✉ **aptx4869** 1 month 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

✉ **David_Ang** 1 month, 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

✉ **BrijMohan08** 2 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

✉ **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: D

The best set of services to meet the storage requirements are:

D) Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

The rationale is:

EC2 instance store provides the highest performance storage for I/O intensive video processing.

S3 provides durable, scalable object storage for the media content library.

Glacier provides the lowest cost archival storage for media no longer in active use.

EBS volumes don't offer the IOPS needed for video processing.

EFS file storage isn't as durable or cost effective for large media libraries as S3.

By matching each storage need with the optimal storage service - EC2, S3, Glacier - this combination meets the performance, durability, and cost requirements for each storage use case.

upvoted 6 times

✉ **JummyFash** 3 months, 2 weeks ago

Option B suggests using Amazon EFS for durable data storage. While Amazon EFS is a managed file storage service, it may not provide the same level of performance and cost-effectiveness as Amazon EBS for maximum I/O performance.

Options C and D suggest using Amazon EC2 instance store, which is ephemeral storage that is directly attached to an EC2 instance. While it can provide high I/O performance, it is not as durable as Amazon EBS or Amazon S3 and does not meet the durability requirements for long-term data storage.

Therefore, option A is the most suitable recommendation to meet the specified storage requirements for the media company.

upvoted 1 times

✉ **vikashverma93** 4 months, 2 weeks ago

A because we need at least 10TB of storage (Persistent) with max I/O, as instance storage is not persistent so that is why it is out of picture, otherwise answer should be D

upvoted 1 times

✉  **MNotABot** 4 months, 2 weeks ago

D

I will go for D as here we need max I/O:

Amazon EC2 Instance Store is suited for temporary storage needs where high performance and low latency are critical. Amazon EBS, on the other hand, is ideal for long-term data storage with better durability and accessibility features.

upvoted 1 times

✉  **cookieMr** 5 months, 1 week ago

Selected Answer: D

Option D is the recommended solution. Amazon EC2 instance store provides maximum performance for video processing, offering local, high-speed storage that is directly attached to the EC2 instances. Amazon S3 is suitable for durable data storage, providing the required capacity of 300 TB for storing media content. Amazon S3 Glacier serves as a cost-effective solution for archival storage, meeting the requirement of 900 TB of archival media storage.

Option A suggests using Amazon EBS for maximum performance, but it may not deliver the same level of performance as instance store for I/O-intensive workloads.

Option B recommends Amazon EFS for durable data storage, but it may not provide the required performance for video processing.

Option C suggests using Amazon EC2 instance store for maximum performance and Amazon EFS for durable data storage, but instance store may not offer the durability and scalability required for the storage needs of the media company.

upvoted 2 times

✉  **antropaws** 6 months ago

Selected Answer: A

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

✉  **manuelemg2007** 4 months, 1 week ago

The instance i4g has capacity 15TB

<https://aws.amazon.com/es/ec2/instance-types/>

upvoted 1 times

✉  **mell1222** 7 months ago

Selected Answer: D

In terms of speed, instance store can generally offer higher I/O performance and lower latency than EBS, due to the fact that it is physically attached to the host. However, the performance of EBS can be optimized based on the specific use case, by selecting the appropriate volume type, size, and configuration.

upvoted 3 times

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 (74%)

A (24%)

✉  **bgsanata**  6 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 11 times

✉  **MutiverseAgent** 4 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 4 times

✉  **Lalo** 5 months, 4 weeks ago

USING SPOT INSTANCES WITH EKS

https://ec2spotworkshops.com/using_ec2_spot_instances_with_eks.html

upvoted 2 times

✉  **ruqui** 6 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 3 times

✉  **MutiverseAgent** 4 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**  8 months, 3 weeks 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 7 times

✉  **pipici**  2 weeks, 1 day ago

Selected Answer: A

A has less operational overhead

upvoted 1 times

✉  **xdkonorek2** 3 weeks, 2 days ago

Selected Answer: B

running containers without container service like EKS introduce huge operational effort

upvoted 1 times

✉  **David_Ang** 1 month, 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 3 times

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

Selected Answer: B

It is a lot of work to manage docker environment on ec2 instance by yourself.

upvoted 2 times

poponpo 1 month, 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 2 months ago

Selected Answer: A

reponse A

upvoted 1 times

TariqKipkemei 2 months, 4 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 3 times

Guru4Cloud 3 months, 2 weeks 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 5 months 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 5 months, 1 week 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 3 times

Abrar2022 6 months, 1 week 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 8 months 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 8 months ago

B: Sport instance save cost

upvoted 1 times

 **bgsanata** 8 months, 3 weeks ago

Selected Answer: D

The answer should be D. Spot instance is not good option at all. The question say "...can tolerate disruptions" this doesn't mean it can run at random time intervals.

upvoted 1 times

 **Lalo** 5 months, 4 weeks ago

USING SPOT INSTANCES WITH EKS

https://ec2spotworkshops.com/using_ec2_spot_instances_with_eks.html

upvoted 1 times

 **Robrobtutu** 7 months, 2 weeks ago

Spot instances are the correct option for this case.

upvoted 1 times

 **Sdraju** 8 months, 4 weeks ago

Selected Answer: B

Spot instances for cost optimisation and Kubernetes for container management

upvoted 1 times

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*

AE (96%) 4%

✉️  **ArielSchivo**  1 year ago

Selected Answer: AE

I would say A and E since Aurora and Fargate are serverless (less operational overhead).
upvoted 8 times

✉️  **baba365** 2 months, 2 weeks ago

There's a difference between Amazon Aurora and Amazon Aurora Serverless
upvoted 1 times

✉️  **Ruffyit**  1 month ago

I would say A and E since Aurora and Fargate are serverless (less operational overhead)
upvoted 1 times

✉️  **TariqKipkemei** 2 months, 4 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 2 times

✉️  **Guru4Cloud** 3 months, 2 weeks 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** 5 months, 1 week 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** 6 months, 3 weeks ago

Selected Answer: AE

Improve the application's infrastructure = Modernize Infrastructure = Least Operational Overhead = Serverless
upvoted 1 times

 **Robrobtutu** 7 months, 2 weeks ago

Selected Answer: AE

A and E are the best options.
upvoted 1 times

 **bgsanata** 8 months, 3 weeks ago

Selected Answer: AE

A and E
upvoted 1 times

 **rapatajones** 10 months, 1 week ago

Selected Answer: AE

a e.....
upvoted 1 times

 **goodmail** 10 months, 2 weeks 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** 10 months, 4 weeks ago

Selected Answer: AE

Yes, go for A and E since thes two ressources are serverless.
upvoted 2 times

 **Buruguduystunstugudunstuy** 11 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** 11 months, 1 week ago

A and E are obvious choices.
upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: AE

Option A and E
upvoted 1 times

 **SilentMilli** 11 months, 2 weeks ago

Selected Answer: AE

A and E
upvoted 1 times

 **333666999** 11 months, 2 weeks ago

Selected Answer: CE

C not A. and E
upvoted 1 times

 **Wpcorgan** 1 year ago

A and E
upvoted 1 times

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  11 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 8 times

✉️  **Ruffyit** Most Recent  1 month ago

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>
upvoted 1 times

✉️  **tom_cruise** 1 month, 2 weeks ago**Selected Answer: B**

target tracking policy = maintain
upvoted 2 times

✉️  **youdelin** 1 month, 3 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 1 times

✉️  **TariqKipkemei** 2 months, 4 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** 3 months, 2 weeks 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 2 times

✉️  **cookieMr** 5 months, 1 week 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 7 months, 2 weeks ago

Selected Answer: B

B of course.

upvoted 1 times

aba2s 10 months, 4 weeks 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 11 months, 1 week ago

Selected Answer: B

target tracking - CPU at 40%

upvoted 2 times

career360guru 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

Wpcorgan 1 year ago

B is correct

upvoted 1 times

ArielSchivo 1 year 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 ago

B

CPU utilization = target tracking

upvoted 2 times

SimonPark 1 year, 1 month ago

Selected Answer: B

B is the answer

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 27 times

✉  **SimonPark** 1 year, 1 month ago

Thanks it convinces me

upvoted 1 times

✉  **xdkonorek2** Most Recent 3 weeks, 2 days 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 1 times

✉  **tom_cruise** 1 month, 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

✉  **Guru4Cloud** 3 months, 2 weeks 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 4 times

✉  **cookieMr** 5 months, 1 week 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** 6 months 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** 11 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 3 times

✉  **career360guru** 11 months, 2 weeks ago

Selected Answer: D

D is the right answer

upvoted 1 times

✉  **gloritown** 11 months, 2 weeks ago

Selected Answer: D

D is correct but instead of OAI using OAC would be better since OAI is legacy

upvoted 3 times

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

Thanks, I didn't know about OAC.

upvoted 1 times

✉  **Wpcorgan** 1 year ago

D is correct

upvoted 1 times

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

A (94%) 3%

 **G3**  10 months ago

Selected Answer: A

Historical reports = Static content = S3
upvoted 15 times

 **dokaedu**  1 year, 1 month 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

 **TariqKipkemei**  2 months, 3 weeks ago

Selected Answer: A

Global, cost-effective, serverless, low latency = CloudFront with S3
Static content = S3
upvoted 3 times

 **Guru4Cloud** 3 months, 2 weeks ago

Selected Answer: A

Historical reports = Static content = S3
upvoted 2 times

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

Very good explanations!
upvoted 1 times

 **Buruguduystunstugudunstuy** 11 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/s3/>

upvoted 3 times

✉  **techhb** 11 months, 1 week ago

A is correct

upvoted 1 times

✉  **career360guru** 11 months, 2 weeks 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 ago

A is correct

upvoted 1 times

✉  **sdasdawa** 1 year 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 ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/27935-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

✉  **samplerunk** 1 year 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 ago

Selected Answer: C

load balancing + scalability + cost effective

upvoted 1 times

✉  **MyNameIsJulien** 1 year ago

Selected Answer: B

I think the answer is B

upvoted 1 times

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

C (50%)	A (43%)	7%
---------	---------	----

✉️  **ArielSchivo**  1 year 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 24 times

✉️  **KalarAzar** 5 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 14 times

✉️  **brushek**  1 year, 1 month 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 15 times

✉️  **bhgt** 2 months ago

how it is C when the read replica is not meant for DR
upvoted 1 times

✉️  **wsdasdasdqwdaw** 1 month ago

If the source DB instance fails, you can promote your Read Replica to a standalone source server.
upvoted 2 times

✉️  **rcptryk**  5 days, 8 hours ago

Selected Answer: C

RDS custom support read replica
<https://aws.amazon.com/blogs/database/build-high-availability-for-amazon-rds-custom-for-oracle-using-read-replicas/>
upvoted 1 times

✉️  **merajk** 6 days, 23 hours ago

Selected Answer: C

The shared responsibility model of RDS Custom provides OS shell-level access and database administrator access
upvoted 1 times

✉️  **emd** 1 week ago

Selected Answer: C

C - RDS Custom has access to underlying OS. RDS Custom can create read replicas. <https://aws.amazon.com/blogs/aws/amazon-rds-custom-for-oracle-new-control-capabilities-in-database-environment/>
upvoted 1 times

✉️  **Azure55** 4 weeks ago

Selected Answer: A

here is why answer is A not C:

- 1) DR replication is better than read replica as DR
 - 2) EC2 offer more underlying database's OS than RDS Custom
- upvoted 2 times

✉ **Ruffyit** 1 month ago

C . Underlying OS
upvoted 2 times

✉ **aptx4869** 1 month ago

Selected Answer: C
Keyword: Underlying OS
upvoted 1 times

✉ **wsdadasdqwdaw** 1 month ago

Very tricky but I think it is C not A.
The access to the OS is clear both options have it and
The explanation that if the source DB instance fails, you can promote your Read Replica to a standalone source server is quite enough for this scenario.

upvoted 1 times

✉ **sheji** 1 month ago

Why is the answer not B?
Amazon RDS for Oracle cross-Region automated backups, which include both snapshots as well as archived redo logs, you may attain cost-effective cross-Region DR with low Recovery Point Objective (RPO) and reduced Recovery Time Objective (RTO) compared to the self-managed scripting.
<https://aws.amazon.com/blogs/database/managed-disaster-recovery-with-amazon-rds-for-oracle-cross-region-automated-backups-part-1/>
upvoted 2 times

✉ **ACloud_Guru15** 1 month ago

for people who is supporting answer A, can you please explain how DR can be achieved by this method?
upvoted 1 times

✉ **sweetheatmn** 1 month, 1 week ago

Selected Answer: A
I Go with A because C is not applicable for both regions
1- Cross region replication is not available for RDS custom
2- Read replica is not meant for DR
upvoted 3 times

✉ **sweetheatmn** 1 month, 1 week ago

I Go with A because C is not applicable for both regions
1- Cross region replication is not available for RDS custom
2- Read replica is not meant for DR
ATEF
upvoted 2 times

✉ **rlamberti** 1 month, 1 week ago

Selected Answer: A
Maintain access to the database's underlying operating system.
Cross-region replication for DR
Must be EC2.
upvoted 2 times

✉ **tom_cruise** 1 month, 2 weeks ago

Selected Answer: C
"You can create Oracle replicas for RDS Custom for Oracle DB instances."
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/custom-rr.html>
upvoted 2 times

✉ **clark777** 2 months ago

Selected Answer: A
1.maintain access to the database's underlying operating system.
2.can't create cross-Region replicas in RDS Custom
upvoted 3 times

✉ **BrijMohan08** 2 months, 1 week ago

Selected Answer: A
EC2 - to maintain the underlying OS
upvoted 3 times

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

A (52%)

C (48%)

✉️  **123jh10**  1 year, 1 month 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 47 times

✉️  **MutiverseAgent** 4 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** 2 weeks, 5 days 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 1 times

✉️  **markw92** 5 months, 2 weeks ago

See comment from Nicknameinvalid below. You get your answer.

upvoted 1 times

✉️  **dokaedu**  1 year, 1 month 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 22 times

✉️  **AKBM7829** 3 months ago

But in server side encryption Multi Region Keys is not possible which leaves to Option C

upvoted 1 times

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

Both answers A & C can be possible from the certificate perspective because in both regions will be certificates to encrypt/decrypt, SSE-KMS and SSE-S3 respectively. But the difference is that replication works for new objects and not existing ones, so that leaves answer A as the only right option.

upvoted 1 times

✉️  **Chiznitz** 2 weeks, 5 days 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 1 times

✉ **ruqui** 6 months, 1 week ago

If you want to use the cost argument: SSE-S3 is free so it's cheaper than any other encryption solution (all of the others have a cost), so the answer should be C

upvoted 1 times

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

Replication does not work for existing objects, only for new ones.

upvoted 1 times

✉ **s50600822** 6 months, 3 weeks ago

Don't know what "kays" are, could they be a trap?

upvoted 1 times

✉ **Bmarodi** 5 months, 3 weeks ago

Kays = keys, mistype i think.

upvoted 1 times

✉ **sofodofo** Most Recent 1 month 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** 1 month, 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** 1 month, 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

✉ **DamyanG** 1 month, 4 weeks ago

Selected Answer: C

Answer C I think

upvoted 1 times

✉ **JKevin778** 2 months ago

Selected Answer: C

Athena to query from S3.

SSE-S3 is least operation overhead than SSE-KMS
so, C.

upvoted 2 times

✉ **hieulam** 2 months, 1 week ago

Selected Answer: A

The question should be A.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-what-is-isnot-replicated.html#:~:text=Objects%20created%20after%20you%20add%20a%20replication%20configuration>.

upvoted 1 times

✉ **XCheng** 2 months, 2 weeks ago

C

https://docs.aws.amazon.com/zh_cn/AmazonS3/latest/userguide/bucket-encryption.html#bucket-encryption-replication

upvoted 1 times

✉ **frankie270299** 2 months, 3 weeks ago

Selected Answer: C

i think C is correct answer,i asked chatgpt

upvoted 1 times

 **TariqKipkemei** 2 months, 3 weeks ago

Selected Answer: A

Technically both A and C will work, but there is a requirement for 'LEAST operational overhead'.

Multi-Region keys are a flexible and powerful solution for many common data security scenarios such as this:

Global data management

Businesses that operate globally need globally distributed data that is available consistently across AWS Regions. You can create multi-Region keys in all Regions where your data resides, then use the keys as though they were a single-Region key without the latency of a cross-Region call or the cost of re-encrypting data under a different key in each Region.

upvoted 4 times

 **Jeyaluxshan** 3 months ago

If you use S3 managed encryption key , it will apply to newly uploaded objects, not to existing objects. C & D is wrong. which state use existing bucket.

Athena is to query in S3 so no need of RDS. B is wrong.

Correct Answer is A - use KMS key

upvoted 3 times

 **AKBM7829** 3 months ago

C is right Answer

upvoted 1 times

 **sohailn** 3 months, 2 weeks ago

C is the best answer because encrypted s3 replication is not as simple,

if you have an unencrypted data or encrypted with sse-s3 it will replicate by default.

if you have encrypted sse-c client side encryption it will not replicate at all because you need to access the key all the time.

if you encrypted with sse-kms by default it will not encrypt from source to target by default you'll need to perform additional steps and we can't use KMS-Multi key because aws s3 still consider it independent key, so you must first need to decrypt the data in source bucket and re-encrypt in target bucket this solution is 100% true as per stephen udemy instructor.

upvoted 1 times

 **GC2023** 3 months, 2 weeks ago

Please remember that enabling encryption on a bucket does not retroactively encrypt existing objects. You would need to perform a copy operation to re-upload existing objects with encryption enabled if you want to ensure that all objects are encrypted (from chatGPT)

upvoted 1 times

 **Fielies23** 3 months, 3 weeks ago

As a side note, if a bucket already exists and you enable replication, you CAN actually now also replicate the existing object in the bucket with "Amazon S3 Batch Replication".

<https://aws.amazon.com/blogs/aws/new-replicate-existing-objects-with-amazon-s3-batch-replication/#:~:text=S3%20Replication%20is%20fully,or%20multiple%20destination%20buckets.>

upvoted 2 times

 **RupeC** 4 months, 1 week ago

Selected Answer: C

A and C are valid, but C has less overhead and the key management is also serverless.

upvoted 2 times

 **fuzzycr** 4 months, 2 weeks ago

Selected Answer: A

without any changes to your client applications

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 26 times

 **remand** Highly Voted 10 months, 2 weeks 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 7 times

 **RNess** Most Recent 1 month, 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** 2 months, 3 weeks ago

Selected Answer: D

option D is correct

upvoted 1 times

 **Guru4Cloud** 3 months, 2 weeks 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 1 times

cookieMr 5 months, 1 week 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 2 times

Abrar2022 6 months ago

VPC Endpoint (Target Service) - for specific services (not accessing whole vpc)

VPC Peering - (accessing whole VPC)

upvoted 3 times

Abrar2022 6 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 6 months, 1 week ago

Selected Answer: D

Option D, but seems that it is vise versa. Customer needs to create Privatelink and and you VPC endpoint to connect to Privatelink

upvoted 1 times

studynoplay 6 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 9 months, 1 week ago

Selected Answer: D

D. Here you are the one initiating the connection

upvoted 1 times

devonwho 10 months 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 10 months 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 11 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** 11 months ago

AWS PrivateLink documentation: <https://docs.aws.amazon.com/vpclink/latest/userguide/what-is-vpclink.html>

upvoted 1 times

 **techhb** 11 months, 1 week ago

D is right, if requirement was to be ok with public internet then option C was ok.

upvoted 1 times

 **k1kavi1** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: D

D is the right answer

upvoted 1 times

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

AC (89%)	11%
----------	-----

 **123jh10**  1 year, 1 month 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 23 times

 **gustavtd**  11 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 6 times

 **LuckyAro** 10 months, 2 weeks ago

You nailed it !

upvoted 1 times

 **Amitabha09**  1 month, 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** 1 month, 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 1 times

 **TariqKipkemei** 2 months, 3 weeks ago

Selected Answer: AC

Create an AWS Database Migration Service (AWS DMS) replication server then create an ongoing replication task

upvoted 2 times

 **Guru4Cloud** 3 months, 2 weeks 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** 4 months, 2 weeks 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** 5 months, 1 week 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** 5 months, 3 weeks ago

Answer is CD. Postgresql to Aurora Postgresql needed SCT.
<https://aws.amazon.com/ko/dms/schema-conversion-tool/>

upvoted 1 times

✉ **Bmarodi** 5 months, 3 weeks ago

Selected Answer: AC

Option A & C are the right answer.

upvoted 1 times

✉ **kruasan** 7 months, 1 week 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** 8 months, 1 week 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** 8 months, 1 week 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

✉ **G3** 10 months ago

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-postgresql-database-to-aurora-postgresql.html>

This link talks about using DMS . I saw the other link pointing to SCT - not sure which one is correct

upvoted 1 times

✉ **aba2s** 10 months, 4 weeks ago

Selected Answer: CD

DMS for database migration
SCT for having the same scheme

upvoted 3 times

✉ **Help2023** 9 months, 2 weeks ago

The source and destination are both MySQL so schema is not needed.

upvoted 3 times

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

Selected Answer: AC

AWS Database Migration Service (AWS DMS)
upvoted 1 times

✉ **bamishr** 11 months ago

A. Create an ongoing replication task: An ongoing replication task can be used to continuously replicate data from the on-premises database to the Aurora database. This will ensure that the Aurora database remains in sync with the on-premises database.

D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT): The AWS SCT can be used to convert the schema of the on-premises database to a format that is compatible with Aurora. This will ensure that the data can be properly migrated and that the Aurora database can be used with the same applications and queries as the on-premises database.

upvoted 2 times

 Help2023 9 months, 2 weeks ago

The source and destination are both MySQL so schema is not needed.

upvoted 1 times

 Buruguduystunstugudunstuy 11 months ago

Selected Answer: AC

To meet the requirements of maintaining an online and accessible on-premises database while migrating to Amazon Aurora PostgreSQL and keeping the databases synchronized, a solutions architect should take the following actions:

Option A. Create an ongoing replication task. This will allow the architect to continuously replicate data from the on-premises database to the Aurora database.

Option C. Create an AWS Database Migration Service (AWS DMS) replication server. This will allow the architect to use AWS DMS to migrate data from the on-premises database to the Aurora database. AWS DMS can also be used to continuously replicate data between the two databases to keep them synchronized.

upvoted 3 times

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

B (87%) 13%

✉️  **123jh10**  1 year, 1 month 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**  5 months, 1 week 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 5 times

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

Selected Answer: B

distribution list is the way to go
upvoted 1 times

✉️  **Guru4Cloud** 3 months, 2 weeks 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** 5 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 workflowso it is D

upvoted 1 times

✉️  **fishy_resolver** 5 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** 6 months 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** 7 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 1 times

✉️ **jdr75** 7 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** 8 months 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** 7 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** 8 months, 1 week 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** 11 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** 11 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

✉️ **Buruguduystunstugudunstuy** 11 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** 10 months, 1 week 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** 11 months, 1 week ago

B makes more sense

upvoted 1 times

 **Sahilbhai** 11 months, 2 weeks ago

answer b is makes more sense

upvoted 1 times

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** Highly Voted  1 year, 1 month 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 19 times

✉  **EKA_CloudGod** 12 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, 1 month 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 2 times

✉  **chandu7024** Most Recent 2 months, 1 week ago

Agree with B

upvoted 1 times

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

Selected Answer: B

B offers high availability and low operational overheads.
upvoted 1 times

✉  **Guru4Cloud** 3 months, 2 weeks 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 3 times

 **MNotABot** 4 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** 5 months, 1 week 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** 9 months ago

Selected Answer: B

B for me.

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 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 4 times

 **techhb** 11 months, 1 week ago

Selected Answer: B

B is right all explanations below are correct

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B is right answer

upvoted 1 times

 **Wpcorgan** 1 year ago

B for me

upvoted 1 times

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

D (73%)	B (21%)	4%
---------	---------	----

 Six_Fingered_Jose Highly Voted 1 year, 1 month 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 21 times

 Abdou1604 1 month, 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

 vipyodha 5 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 7 times

 123jh10 Highly Voted 1 year, 1 month 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

 vipyodha 5 months, 1 week ago

but B is not least operational overhead , D is least operational overhead

upvoted 1 times

 LuckyAro 10 months, 2 weeks ago

Nowhere in the question did they mention that other files were unrelated to reporting

"The reporting team wants to move the files automatically to analysis S3 bucket as the files enter the initial S3 bucket" where did it say they were unrelated files ? except for conjecture.

upvoted 6 times

 **jdr75** 7 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 and cheaper than use Lambda. So the answer is D.

upvoted 2 times

 **JayBee65** 11 months, 1 week 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 5 times

 **Marco_St** Most Recent 5 days, 12 hours 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** 1 month, 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 3 times

 **vijaykamal** 2 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** 2 months, 3 weeks ago

Selected Answer: D

D provide the least operational overhead
upvoted 1 times

 **Guru4Cloud** 3 months, 2 weeks 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:

S3 replication automatically copies new objects to analysis bucket
EventBridge allows easily adding multiple targets for events
No custom Lambda function needed for copying objects
Leverages managed services for event processing

upvoted 3 times

 **MutiverseAgent** 4 months, 2 weeks 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** 5 months, 1 week 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** 6 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 5 times

✉ **eendee** 7 months, 3 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 4 times

✉ **kraken21** 8 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** 8 months, 2 weeks ago

only one destination type can be specified for each event notification in S3 event notifications

upvoted 1 times

✉ **gmehra** 8 months, 3 weeks 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

✉ **markw92** 5 months, 2 weeks 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

✉ **Kaireny54** 8 months 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

✉ **Steve_4542636** 8 months, 4 weeks 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** 10 months, 1 week 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 straightforward, while 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

✉ **AHUI** 10 months, 2 weeks ago

Ans : D

S3 event notification can only send notifications to SQS. SNS and Lambda, BUT not SageMaker
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html>

S3 event notification can send notifications to SNS, SQS and Lambda, but not SageMaker

upvoted 8 times

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, 1 month 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 15 times

aba2s Highly Voted 10 months, 4 weeks ago

Selected Answer: AC

Compute Savings Plans can be used for EC2 instances and Fargate. Whereas EC2 Savings Plans support EC2 only.

upvoted 6 times

TariqKipkemei Most Recent 2 months, 3 weeks ago

Selected Answer: AC

Compute Savings Plans can also apply to Fargate and Lambda Usage.

upvoted 1 times

AKBM7829 3 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 1 month, 2 weeks ago

Spot instances can auto scale so Spot instance is correct.

upvoted 1 times

Guru4Cloud 3 months, 2 weeks 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 1 times

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

EC2 instance Savings Plans are not applied to Fargate or Lambda

upvoted 1 times

 **Noviiice** 8 months, 2 weeks ago

Why not B?

upvoted 1 times

 **SkyZeroZx** 8 months 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** 11 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 1 times

 **AKBM7829** 3 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** 1 month, 2 weeks ago

Spot instances can auto scale so Spot is still correct.

upvoted 1 times

 **techhb** 11 months, 1 week ago

Selected Answer: AC

Too obvious answer.

upvoted 1 times

 **berks** 11 months, 1 week ago

Selected Answer: AC

AC

can be interrupted at any time => spot

upvoted 2 times

 **TECHNOWARRIOR** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

 **rjam** 1 year ago

its A and C . <https://www.densify.com/finops/aws-savings-plan>

upvoted 1 times

 **bunnychip** 1 year, 1 month ago

Selected Answer: AC

api is not EC2.need to use compute savings plan

upvoted 4 times

 **Chunslı** 1 year, 1 month 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

 **Yadav_Sanjay** 7 months ago

I Agree

upvoted 1 times

 **capepenguin** 1 year, 1 month ago

Isn't the EC2 Instance Savings Plan not applicable to Fargate and Lambda?

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 6 times

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 (29%)

 **huiy** Highly Voted 1 year, 1 month 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 24 times

 **MutiverseAgent** 4 months, 2 weeks 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

 **Six_Fingered_Jose** Highly Voted 1 year, 1 month 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 10 times

 **Abdou1604** 1 month, 3 weeks ago

What about accross the word :)

upvoted 1 times

 **Mahadeva** 10 months, 3 weeks ago

CloudFront does not cache dynamic content. But Latency can be still low for dynamic content because the traffic is on the AWS global network which is faster than the internet.

upvoted 6 times

 **Joxtat** 10 months, 2 weeks ago

Amazon CloudFront speeds up distribution of your static and dynamic web content, such as .html, .css, .php, image, and media files. When users request your content, CloudFront delivers it through a worldwide network of edge locations that provide low latency and high performance.

upvoted 4 times

 **Onimole** 1 year ago

Cf works for both static and dynamic content

upvoted 8 times

 **Aamee** 12 months ago

Can you pls. provide a ref. link from where this info. got extracted?
upvoted 1 times

 **manuelemg2007** 4 months ago

this is link <https://aws.amazon.com/es/blogs/aws-spanish/cloudfront-para-la-distribucion-de-contenido-estatico-y-dinamico/>
upvoted 1 times

 **AZ_Master** Most Recent 1 week, 3 days ago

Selected Answer: B

Those are personalized content - where CloudFront could not help much.
upvoted 2 times

 **David_Ang** 1 month, 1 week ago

Selected Answer: A

"A" because cloud front is more efficient
upvoted 1 times

 **Wayne23Fang** 1 month, 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** 2 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 1 times

 **TariqKipkemei** 2 months, 3 weeks ago

Selected Answer: A

CloudFront to the rescue....whoosh
upvoted 2 times

 **Guru4Cloud** 3 months, 2 weeks 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** 3 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** 4 months, 2 weeks 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 2 times

 **MutiverseAgent** 4 months, 2 weeks 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** 5 months, 1 week 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** 6 months 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

 **antropaws** 6 months ago

Selected Answer: A

A is correct. CF distributes the content globally. Why not deploy the application in 4 or 5 regions instead of 2? It's an arbitrary choice, that's one of the reasons why B and D are not a solid solution.

upvoted 1 times

 **Bmarodi** 6 months, 1 week ago

Selected Answer: A

I go for option A, CF uses edge locations to speed up S3 content, both static and dynamic, hence A is right ans.

upvoted 1 times

 **bgsanata** 6 months, 1 week ago

Selected Answer: B

I would say B.

2 regions is always better if you aim for better distribution of the traffic. This will split the amount of request sent to the Single EC2 instance by half => indirectly improve latency.

It's true that CloudFront improves latency but it's hard to say if this will be true for ALL users. Having second region will definitely improve the performance for the users with less latency atm.

upvoted 1 times

 **cheese929** 7 months ago

Selected Answer: A

A is correct. Cloudfront can serve both static and dynamic content fast.

<https://aws.amazon.com/cloudfront/dynamic-content/>

upvoted 2 times

 **kevinkn** 7 months ago

Selected Answer: B

the lowest latency (option B) is not always equal to the closest resource (option D). And the requirement asks for lowest latency

upvoted 1 times

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** Highly Voted 1 year, 1 month 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 59 times

 **stepman** 11 months, 3 weeks 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 5 times

 **praveenas400** 10 months, 4 weeks ago

Explained very well. ty

upvoted 2 times

 **iCcma** 1 year ago

Thank you, your explanation helped me to better understand even the answer of question 29

upvoted 3 times

 **Buruguduystunstugudunstuy** Highly Voted 11 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 5 times

 **Buruguduystunstugudunstuy** 11 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 2 times

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

Selected Answer: C

UDP, static IP = Global Accelerator and Network Load Balancer
upvoted 1 times

✉ **Guru4Cloud** 3 months, 2 weeks 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** 5 months, 1 week 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** 6 months ago

aws global accelerator provides static IP addresses.

upvoted 1 times

✉ **Bmarodi** 6 months, 1 week ago

Selected Answer: C

My choice is option C, due to the followings: Amazon Global accelerator route the 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** 8 months ago

Answer : C
CloudFront : Doesn't support static IP addresses
ALB : Doesn't support UDP
upvoted 1 times

✉ **Devsin2000** 8 months, 3 weeks ago

C - <https://aws.amazon.com/global-accelerator/>
upvoted 1 times

✉ **SilentMilli** 10 months, 3 weeks 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** 11 months, 1 week ago

Selected Answer: C

C is obvious choice here.

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: C

C as Global Accelerator is the best choice for UDP based traffic needing static IP address.

upvoted 1 times

✉ **Certified101** 11 months, 2 weeks ago

Selected Answer: C

c correct

upvoted 1 times

✉ **Qjb8m9h** 11 months, 3 weeks 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 ago

C is correct

upvoted 1 times

 **PS_R** 1 year ago

Selected Answer: C

Cloud Fronts supports both Static and Dynamic and Global Accelerator means low latency over UDP

upvoted 1 times

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

D (80%)	B (16%)	5%
---------	---------	----

✉  **Ken701** Highly Voted 1 year, 1 month ago

I think the answer here is "D" because usually when you see terms like "monolithic" the answer will likely refer to microservices.
upvoted 27 times

✉  **Bevemo** Highly Voted 1 year 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 13 times

✉  **TariqKipkemei** Most Recent 2 months, 3 weeks ago

Selected Answer: D

'Non-monolithic', 'smaller applications', 'minimized operational overhead' all screaming 'microservices'.
upvoted 1 times

✉  **Guru4Cloud** 3 months, 2 weeks 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 3 times

✉  **MM_Korvinus** 3 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 7 times

✉  **Fielies23** 3 months, 3 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

✉  **cookieMr** 5 months, 1 week 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** 6 months 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** 6 months, 3 weeks ago

Selected Answer: D

monolithic = microservices = ECS

upvoted 4 times

 **C_M_M** 7 months, 2 weeks 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** 8 months, 3 weeks 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

 **aws4myself** 10 months, 1 week 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

 **SilentMilli** 10 months, 3 weeks ago

Selected Answer: D

To meet the requirement of breaking the application into smaller applications that can be managed by different teams, while minimizing operational overhead and providing high scalability, the best solution would be to host the applications on Amazon Elastic Container Service (Amazon ECS). Amazon ECS is a fully managed container orchestration service that makes it easy to run, scale, and maintain containerized applications. Additionally, setting up an Application Load Balancer with Amazon ECS as the target will allow the company to easily scale the application as needed. Option D, "Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target," is the correct answer.

upvoted 1 times

 **Zerotn3** 11 months ago

Selected Answer: D

. Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target.

Hosting the application on Amazon ECS would allow the company to break the monolithic application into smaller, more manageable applications that can be managed by different teams. Amazon ECS is a fully managed container orchestration service that makes it easy to deploy, run, and scale containerized applications. By setting up an Application Load Balancer with Amazon ECS as the target, the company can ensure that the solution is highly scalable and minimizes operational overhead.

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months ago

Selected Answer: D

The correct answer is Option D. To meet the requirements, the company should host the application on Amazon Elastic Container Service (Amazon ECS) and set up an Application Load Balancer with Amazon ECS as the target.

Option A is not a valid solution because AWS Lambda is not suitable for hosting long-running applications.

Option B is not a valid solution because AWS Amplify is a framework for building, deploying, and managing web applications, not a hosting solution.

Option C is not a valid solution because Amazon EC2 instances are not fully managed container orchestration services. The company will need to manage the EC2 instances, which will increase operational overhead.

upvoted 4 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: D

It can be C or D depending on how easy it would be to containerize the application. If application needs persistent local data store then C would be a better choice.

Also from the usecase description it is not clear whether application is http based application or not though all options uses ALB only so we can safely assume that this is http based application only.

upvoted 2 times

 **career360guru** 11 months, 1 week ago

After reading this question again A will be minimum operational overhead.

D has higher operational overhead as D will have operational overhead of scaling EC2 servers up/down for running ECS containers.

upvoted 1 times

 **Wpcorgan** 1 year ago

D is correct

upvoted 1 times

 **backbencher2022** 1 year ago

Selected Answer: D

I think D is the right choice as they want application to be managed by different people which could be enabled by breaking it into different containers

upvoted 1 times

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%)

 **TariqKipkemei** 2 months, 3 weeks ago

Selected Answer: B

Migrate the monthly reporting to an Aurora Replica
upvoted 1 times

 **Guru4Cloud** 3 months, 2 weeks 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 1 times

 **cd93** 3 months, 2 weeks 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 1 times

 **cd93** 3 months, 2 weeks 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 2 times

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

 **Abrar2022** 6 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** 6 months, 1 week ago

Selected Answer: B

Option B is right answer.

upvoted 1 times

 **studynoplay** 6 months, 3 weeks ago

Finally a question where there are no controversies
upvoted 3 times

 **SilentMilli** 10 months, 3 weeks 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

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 3 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 5 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

B is the best option

upvoted 2 times

 **sanket1990** 11 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

 **Wpcorgan** 1 year ago

B is correct

upvoted 1 times

 **backbencher2022** 1 year ago

Selected Answer: B

ReadIOPS issue inclining towards Read Replica as the most cost effective solution here

upvoted 4 times

 **rjam** 1 year ago

Answer B

upvoted 2 times

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

D (69%)	A (27%)	4%
---------	---------	----

✉️  **genny**  7 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 8 times

✉️  **AZ_Master** 1 week, 3 days 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 1 times

✉️  **Konb**  6 months, 4 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 7 times

✉️  **pbpally** 6 months, 3 weeks ago

Yup. Got me too. I picked A, saw D, and then reread the "scale seamlessly" part. D is correct.

upvoted 3 times

✉️  **xdkonorek2**  3 weeks, 1 day 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** 2 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

 **TariqKipkemei** 2 months, 3 weeks ago

Selected Answer: D

Scale seamlessly = Autoscaling group, Amazon Aurora MySQL DB instance

Cost effective = Spot Fleet

upvoted 2 times

 **Guru4Cloud** 3 months, 2 weeks 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 2 times

 **cookieMr** 5 months, 1 week 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** 7 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** 8 months, 1 week 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** 9 months, 3 weeks 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** 10 months, 1 week 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** 10 months, 2 weeks 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** 11 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** 9 months, 2 weeks 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** 4 months, 1 week ago

Super bit of info. Thanks
upvoted 1 times

 **Zerotn3** 11 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** 11 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 2 times

 **techhb** 11 months, 1 week ago

D ,as only this has auto scaling
upvoted 1 times

 **Sahilbhai** 11 months, 1 week ago

ANSWER IS D
upvoted 1 times

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

B (53%)	C (35%)	11%
---------	---------	-----

✉  **rob74**  1 year 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 14 times

✉  **Qjb8m9h**  11 months, 3 weeks 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 8 times

✉  **VladanO**  17 hours 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** 1 day, 11 hours 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-](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 1 times

✉  **Marco_St** 4 days 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 1 times

✉  **Juliez** 3 weeks, 5 days 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 1 times

✉  **StudyAllNite** 4 weeks, 1 day 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

✉  **ACloud_Guru15** 1 month 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

✉ **rexix7368** 1 month ago

Selected Answer: C

C is most cost effective option for running not 7x24 loads

upvoted 3 times

✉ **Wayne23Fang** 1 month, 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** 2 months ago

Selected Answer: C

For 8 hours/day on demand works best

upvoted 2 times

✉ **Azure55** 4 weeks ago

and Application usage is moderate and steady overnight!

upvoted 1 times

✉ **TariqKipkemei** 2 months, 3 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** 2 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

✉ **Guru4Cloud** 3 months, 2 weeks 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 2 times

✉ **toussyn** 4 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

✉ **cookieMr** 5 months, 1 week ago

Selected Answer: B

B is correct because it combines the use of Reserved Instances and Spot Instances to minimize EC2 costs while ensuring availability. Reserved Instances provide cost savings for the baseline level of usage during the heavy usage period, while Spot Instances are utilized for any additional capacity needed during peak times, taking advantage of their cost-effectiveness.

A is incorrect because relying solely on Spot Instances for the entire workload can result in potential interruptions and instability during peak usage periods.

C is incorrect because using On-Demand Instances for the baseline level of usage does not provide the cost savings and long-term commitment benefits that Reserved Instances offer.

D is incorrect because using Dedicated Instances for the baseline level of usage incurs additional costs without significant benefits for this scenario. Dedicated Instances are typically used for compliance or regulatory requirements rather than cost optimization.

upvoted 2 times

 **Bmarodi** 5 months, 3 weeks ago

Selected Answer: B
A company runs a stateless web application in production. This means that the application can be stopped and restarted again.

upvoted 1 times

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 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 8 times

tdkumberland 1 year ago

AWS BackUp costs something, setting up S3 LCP doesn't.

upvoted 3 times

TariqKipkemei Most Recent 2 months, 3 weeks ago**Selected Answer: B**

S3 Lifecycle policies to the rescue

upvoted 1 times

cookieMr 5 months, 1 week 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 2 times

Mamiololo 10 months, 2 weeks ago

B is correct..

upvoted 1 times

Buruguduystunstugudunstuy 11 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 11 months, 2 weeks 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 ago

B is correct
upvoted 1 times

 **ArielSchivo** 1 year ago

Selected Answer: B
S3 + Glacier is the most cost effective.
upvoted 3 times

 **Bevemo** 1 year 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** 12 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 ago

Selected Answer: B
<https://www.examtopics.com/discussions/amazon/view/80772-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

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

D (85%)

C (15%)

✉️  **bunnychip** Highly Voted 1 year, 1 month ago

Selected Answer: D

ensure that all notifications are eventually processed
upvoted 11 times

✉️  **Guru4Cloud** Most Recent 3 months, 2 weeks 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 1 times

✉️  **Help2023** 9 months, 2 weeks ago

Selected Answer: D

This is why <https://docs.aws.amazon.com/sns/latest/dg/sns-message-delivery-retries.html>
upvoted 3 times

✉️  **CaoMengde09** 9 months, 3 weeks 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 3 times

✉️  **CaoMengde09** 9 months, 3 weeks 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** 10 months, 3 weeks 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** 11 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** 11 months, 1 week ago

Selected Answer: D

Option D to ensure that all notifications are eventually processed you need to use SQS.
upvoted 2 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C is right option.
SNS does not have any "On Failure" delivery destination. One needs to configure dead-letter queue and configure SQS to read from there. So given this option D is incorrect.
upvoted 2 times

 **JayBee65** 11 months, 1 week 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 4 times

 **NikaCZ** 11 months, 2 weeks ago

Selected Answer: D

Is correct.

upvoted 1 times

 **NikaCZ** 11 months, 2 weeks ago

If you want to ensure that all notifications are eventually processed you need to use SQS.

upvoted 1 times

 **Wajif** 12 months ago

Selected Answer: D

C isn't specific. Hence D

upvoted 1 times

 **LeGlopier** 1 year ago

Selected Answer: C

"on-failure destination" doesn't exist, only dead letter queue exists.
that's why I am leaning for C

upvoted 1 times

 **Wajif** 12 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 1 times

 **Wpcorgan** 1 year ago

D is correct

upvoted 1 times

 **ds0321** 1 year ago

Selected Answer: D

D is the answer

upvoted 1 times

 **ArielSchivo** 1 year 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, 1 month ago

Selected Answer: D

imho, D is the answer

upvoted 1 times

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%)

 **Guru4Cloud** 3 months, 2 weeks 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** 5 months, 1 week 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 3 times

 **cheese929** 7 months ago

Selected Answer: A

A is correct. Use FIFO to process in the specific order required

upvoted 2 times

 **WhericanIstart** 9 months ago

Selected Answer: A

Option A is correct...data is processed in the correct order

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 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 3 times

 **techhb** 11 months, 1 week ago

Only A is right option here.
upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: A

Option A is the best option.
upvoted 2 times

 **elect096** 11 months, 2 weeks ago

Selected Answer: A

"The data is written in a specific order that must be maintained throughout processing" --> FIFO
upvoted 4 times

 **NikacZ** 11 months, 2 weeks ago

Selected Answer: A

specific order = FIFO
upvoted 1 times

 **k1kavi1** 11 months, 2 weeks ago

Selected Answer: A

A is correct
upvoted 1 times

 **david76x** 11 months, 3 weeks ago

Selected Answer: A

Definitely A
upvoted 1 times

 **Wpcorgan** 1 year ago

A is correct
upvoted 1 times

 **ArielSchivo** 1 year ago

Selected Answer: A

FIFO means order, so Option A.
upvoted 4 times

 **rjam** 1 year ago

Order --- means FIFO option A
upvoted 3 times

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, 1 month 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 22 times

 **Modulopi**  2 months 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** 2 months, 3 weeks ago

Selected Answer: A

Composite alarms was designed to handle this scenario.

upvoted 1 times

 **Guru4Cloud** 3 months, 2 weeks 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 2 times

 **cookieMr** 5 months, 1 week 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 4 times

 **Abrar2022** 6 months ago

The composite alarm goes into ALARM state only if all conditions of the rule are met.

upvoted 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 2 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 2 weeks ago

A is correct answer

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **Qjb8m9h** 11 months, 3 weeks 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 ago

A is correct

upvoted 1 times

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

AC (69%)	14%	Other
----------	-----	-------

 **Six_Fingered_Jose** Highly Voted 1 year, 1 month 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 15 times

 **rjam** Highly Voted 1 year ago

<https://aws.amazon.com/blogs/aws/new-for-aws-control-tower-region-deny-and-guardrails-to-help-you-meet-data-residency-requirements/>

*Disallow internet access for an Amazon VPC instance managed by a customer

upvoted 9 times

 **rjam** 1 year ago

Option A and C

upvoted 2 times

 **rjam** 1 year ago

*You can use data-residency guardrails to control resources in any AWS Region.

upvoted 1 times

 **BrijMohan08** Most Recent 2 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** 2 months, 3 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** 3 months, 2 weeks 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 2 times

 **cookieMr** 5 months, 1 week 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 7 times

✉ **Abrar2022** 5 months, 3 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 1 times

✉ **hicham0101** 7 months, 1 week 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** 7 months, 3 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** 6 months, 4 weeks ago

I just checked, now it's supported!!!

upvoted 2 times

✉ **notacert** 7 months, 3 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

✉ **datz** 7 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** 7 months, 1 week ago

False, Control Tower is in Osaka NorthEast 3

<https://docs.aws.amazon.com/controltower/latest/userguide/region-how.html>

upvoted 2 times

✉ **Kaireny54** 8 months 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/controltower.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

✉ **Bmarodi** 6 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

✉ **darn** 7 months, 1 week ago

same page you posted:

ap-northeast-3 Asia Pacific (Osaka) 2023-04-20 <https://aws.amazon.com/controltower>

upvoted 1 times

✉ **darn** 7 months, 1 week ago

False, Control Tower is in Osaka NorthEast 3

<https://docs.aws.amazon.com/controltower/latest/userguide/region-how.html>

upvoted 1 times

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

What's wrong with B?

upvoted 2 times

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

Selected Answer: CE

A - CANNOT BE!!! AWS Control Tower is not available in ap-northeast-3! Check your consolle.

upvoted 4 times

✉️ **moaaz86** 9 months, 1 week 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** 1 month 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** 9 months, 3 weeks 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

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

D (80%)	A (20%)
---------	---------

✉️  **study_aws1** Highly Voted 1 year 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 29 times

✉️  **123jh10** Highly Voted 1 year, 1 month 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

✉️  **ArielSchivo** 1 year ago

Option A refers to Session Manager, not State Manager as you pointed, so it is wrong. Option D is valid.

upvoted 8 times

✉️  **Bevemo** 1 year ago

Agree A, free to use state manager within limits, and don't need to code or manage lambda.

upvoted 1 times

✉️  **Kien048** 1 year, 1 month ago

Look like State manager and Session manager use for difference purpose even both in same dashboard console.

upvoted 1 times

✉️  **Kien048** 1 year, 1 month ago

And ofcause, D is working, so if A also right, the question is wrong.

upvoted 3 times

✉️  **Ruffyit** Most Recent 2 days, 2 hours 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 1 times

✉️  **TariqKipkemei** 2 months, 3 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 1 times

👤 **lemur88** 3 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** 3 months, 2 weeks 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 2 times

👤 **cookieMr** 5 months, 1 week 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 2 times

👤 **Siva007** 6 months, 1 week ago

Selected Answer: D

I got this question in real exam!

upvoted 3 times

👤 **srijrao** 5 months, 1 week 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** 6 months, 3 weeks ago

State Manager, a capability of AWS Systems Manager

upvoted 1 times

👤 **Ankit_EC_ran** 7 months, 1 week ago

Selected Answer: D

Option D is correct

upvoted 2 times

👤 **Musti35** 7 months, 2 weeks 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 2 times

👤 **test_devops_aws** 8 months, 2 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/systems-manager-automation-runbooks/latest/userguide/automation-ref-rds.html>
upvoted 1 times

👤 **aba2s** 10 months, 4 weeks 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** 11 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

 **jupa** 11 months, 1 week ago

Selected Answer: D

Its D. confirmed via others exam test pages

upvoted 2 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D is the best option. Session Manager access can not be used to start and stop DB instances. It is used for the Brower based SSH access to instances.

upvoted 2 times

 **ArielSchivo** 1 year ago

Selected Answer: D

Option D is the one. Option A could be as well if it referred to State Manager instead of Session Manager.

upvoted 5 times

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

D (63%)

B (37%)

✉  **rjam**  1 year 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 33 times

✉  **MutiverseAgent** 4 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** 4 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

✉  **zeronine75**  1 year 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 11 times

✉  **Wajif** 12 months ago

S3 Intelligent tiering is used when the access frequency is not known. I think 128KB is a deflector.

upvoted 7 times

✉  **ruqui** 6 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 2 times

✉  **FNJ1111** 11 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 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 4 times

✉ **javitech83** 11 months, 3 weeks 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** 11 months, 3 weeks ago

oh sorry it states objects are bigger than 128 KB. B is correct

upvoted 1 times

✉ **Ruffyit** Most Recent 2 days, 1 hour 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** 3 weeks, 1 day 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** 1 month, 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

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

Selected Answer: D

Not B because Intelligent-tiering = unkown patterns

upvoted 1 times

✉ **Guru4Cloud** 3 months, 2 weeks 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 1 times

✉ **Smart** 4 months, 1 week 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 2 times

✉ **MutiverseAgent** 4 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 1 times

✉ **MutiverseAgent** 4 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 1 times

✉ **vini15** 4 months, 2 weeks ago

should be D

upvoted 1 times

✉ **cookieMr** 5 months, 1 week 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

✉ **kelvintoy93** 5 months, 3 weeks ago

Selected Answer: D

128kB is a 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 dont 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 1 times

✉ **kelvintoy93** 5 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** 6 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

✉ **Abrar2022** 6 months ago

In the question it mentions that the files are stored in S3 Standard. So you need to transition them from S3 standard using S3 Lifecycle policy that moves the objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.

upvoted 1 times

✉ **ccmc** 6 months, 3 weeks ago

Selected Answer: B

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. -- means some most accessed files are can be more than 90 days old. so should go with intelligent tiering as the patterns are unpredictable

upvoted 1 times

✉ **cheese929** 7 months ago

Selected Answer: B

Answer should be B.

S3 Standard and S3 Intelligent - Tiering are both \$0.023 per GB per month.

However S3 Standard - Infrequent Access is \$0.0125 per GB while S3 Intelligent - Tiering Archive Access Tier is \$0.0036 per GB. S3 Intelligent - Tiering Deep Archive Access Tier is even cheaper at \$0.00099 per GB. Thus the answer is B.

upvoted 1 times

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

B (86%)

14%

 **elmogy** Highly Voted 6 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 20 times

 **Qjb8m9h** Highly Voted 1 year 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 19 times

 **abhishek2021** 6 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

 **Zerotn3** 11 months ago

How about: The repository must allow a few scientists to add new files

upvoted 1 times

 **JayBee65** 10 months, 4 weeks ago

Adding is not the same as changing :)

upvoted 7 times

 **Ruffyt** Most Recent 2 days, 1 hour 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 1 times

 **TariqKipkemei** 2 months, 3 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** 3 months, 2 weeks 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

 **MutiverseAgent** 4 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** 5 months, 1 week 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** 6 months, 1 week ago

Am I the only one to worry about leap years ?

upvoted 1 times

 **cheese929** 7 months 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** 7 months, 1 week ago

Selected Answer: B

its B, legal hold has no retention

upvoted 3 times

 **Shrestwt** 7 months, 1 week ago

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

upvoted 1 times

 **jaswantn** 8 months 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** 10 months 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** 10 months, 4 weeks ago

Selected Answer: B

users can have the ability to modify or delete any files in the repository ==> Compliance Mode

upvoted 1 times

 **aba2s** 10 months, 3 weeks ago

users cannot have the ability to modify or delete any files in the repository ==> Compliance Mode

upvoted 3 times

 **Zerotn3** 11 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** 7 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

 **techhb** 11 months, 1 week ago

Selected Answer: B

No users can have the ability to modify or delete any files in the repository. hence it must be compliance mode.

upvoted 2 times

 **lazzyoung** 11 months, 1 week ago

Selected Answer: B

Answer is B

Compliance:

- Object versions can't be overwritten or deleted by any user, including the root user
- Objects retention modes can't be changed, and retention periods can't be shortened

Governance:

- Most users can't overwrite or delete an object version or alter its lock settings
- Some users have special permissions to change the retention or delete the object

upvoted 3 times

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** Highly Voted 1 year ago

key :caching
Option C
upvoted 11 times

✉  **TariqKipkemei** Most Recent 2 months, 3 weeks ago

Selected Answer: C

Amazon CloudFront to the rescue
upvoted 1 times

✉  **Guru4Cloud** 3 months, 2 weeks 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 3 times

✉  **cookieMr** 5 months, 1 week 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.
- C. 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

✉  **jackky3123213** 5 months, 2 weeks ago

Global Accelerator does not support Edge Caching
upvoted 1 times

✉  **Bmarodi** 6 months, 1 week ago

Selected Answer: C

Option C is correct answer.
upvoted 1 times

✉  **warioverde** 8 months, 1 week 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** 9 months, 2 weeks ago

Selected Answer: C

C correto

upvoted 1 times

✉  **ProfXsamson** 10 months ago

C, Caching == Edge location == CloudFront

upvoted 2 times

✉  **career360guru** 11 months, 2 weeks ago

Selected Answer: C

C right answer

upvoted 2 times

✉  **k1kavi1** 11 months, 2 weeks ago

Selected Answer: C

Agreed

upvoted 1 times

✉  **Wpcorgan** 1 year ago

C is correct

upvoted 1 times

✉  **MyNameIsJulien** 1 year ago

Selected Answer: C

Answer is C

upvoted 1 times

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

AE (84%) Other

 **Wazhija**  1 year, 1 month ago

Selected Answer: AE

I believe AE makes the most sense
upvoted 10 times

 **Six_Fingered_Jose**  1 year, 1 month ago

Selected Answer: AE

yeah AE makes sense, only E is working with S3 here and questions wants them to be in S3
upvoted 8 times

 **Guru4Cloud**  3 months, 2 weeks 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 5 times

 **Mia2009687** 4 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** 5 months, 1 week ago

@Golcha once the data comes from different sources then you use GLUE
upvoted 1 times

 **Jeeva28** 6 months ago

Selected Answer: AC

Less Overhead with option AC .No need to manage
upvoted 1 times

 **Golcha** 7 months, 2 weeks ago

Selected Answer: AC

No specific use case for GLUE
upvoted 1 times

 **TTaws** 5 months, 1 week ago

once the data comes from different sources then you use GLUE

upvoted 1 times

✉ **TECHNOWARRIOR** 7 months, 3 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 2 times

✉ **TECHNOWARRIOR** 7 months, 3 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 2 times

✉ **jramos** 7 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** 7 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** 9 months, 3 weeks ago

Can anyone please explain me why B cannot be an answer?

upvoted 3 times

✉ **Shrestwt** 7 months, 1 week ago

Kinesis Data Analytics is designed for continuous queries rather than one-time queries.

upvoted 4 times

✉ **ashishvineetlk** 10 months, 1 week 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** 9 months, 1 week ago

I will do "A" as well.

upvoted 1 times

✉ **ProfXsamson** 10 months ago

A would probably be the best answer. Sq extended client library is for Java apps.

upvoted 1 times

✉ **bullrem** 10 months, 1 week ago

Selected Answer: DE

I believe DE makes the most sense

upvoted 1 times

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

Selected Answer: AE

stored in s3 -> data lake -> athena (process the SQL parquet format)-> quicksight visualize

upvoted 4 times

✉ **Zerotn3** 11 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** 10 months, 4 weeks 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 2 times

✉  **jainparag1** 10 months, 1 week ago

Absolutely, querying data is after staging and so Athena fits perfectly.

upvoted 1 times

✉  **techhb** 11 months, 1 week ago

Selected Answer: AE

C can work it out ,but has additional overhead.

upvoted 2 times

✉  **career360guru** 11 months, 2 weeks ago

Selected Answer: AE

A and E

upvoted 2 times

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

DE (79%)

AD (19%)

✉  **JayBee65**  10 months, 4 weeks 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 27 times

✉  **aadityaravi8** 4 months, 3 weeks ago

100% agree

upvoted 4 times

✉  **kmaneith**  1 year ago

Selected Answer: DE

dude trust me

upvoted 18 times

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

<https://medium.com/@darekhale91/how-to-pass-amazon-saa-c03-exam-dumps-2023-583619ddbcc8>

upvoted 1 times

✉  **Priyanshugpt486** 2 months, 1 week ago

hehe... hehe

upvoted 1 times

✉  **JayBee65** 10 months, 4 weeks ago

No, please show your reasoning, you may be wrong. Remember, no one thinks they are wrong, but some always are :)

upvoted 13 times

✉  **Ruffyit**  1 day, 21 hours 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** 1 month, 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** 2 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** 2 months, 3 weeks ago

Selected Answer: DE

DE makes more sense

upvoted 1 times

✉ **Guru4Cloud** 3 months, 2 weeks 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** 8 months, 1 week ago

Selected Answer: AD

Automated backup is limited 35 days

upvoted 3 times

✉ **Training4aBetterLife** 10 months, 1 week 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** 10 months, 1 week 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** 11 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** 11 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

✉ **awashenko** 1 month, 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

✉ **JayBee65** 10 months, 4 weeks ago

I think a lifecycle policy would only keep backups for 35 days

upvoted 3 times

✉ **techhb** 11 months, 1 week ago

Selected Answer: DE

D and E only

upvoted 2 times

✉ **Chirantan** 11 months, 1 week ago

AD

is correct as you can keep backup of snapshot indifferently.

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: DE

D and E

upvoted 2 times

✉  **Qjb8m9h** 11 months, 2 weeks 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** 11 months, 3 weeks 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** 11 months, 3 weeks 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

✉  **Heyang** 11 months, 3 weeks ago

Selected Answer: AD

no more than 35 days

upvoted 4 times

✉  **kmluy73** 11 months, 3 weeks ago

https://aws.amazon.com/about-aws/whats-new/2020/06/amazon-aurora-snapshots-can-be-managed-via-aws-backup/?nc1=h_ls AWS Backup

upvoted 3 times

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

A (56%) B (44%)

✉  **Nigma** Highly Voted 1 year 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 27 times

✉  **Ruffyit** Most Recent 1 day, 21 hours 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 1 times

✉  **mhka1988** 1 month, 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** 1 month, 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

✉  **awashenko** 1 month, 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 1 times

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

chatgpt went with cloudfront on this question, so answer A
upvoted 3 times

✉ **coolkidsclubvip** 3 months 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** 3 months, 2 weeks 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 1 times

✉ **Chan1010** 4 months, 1 week ago

Selected Answer: B

Global Accelerator good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP
upvoted 1 times

✉ **fageroff** 1 month ago

a video streaming is udp traffic
upvoted 1 times

✉ **cookieMr** 5 months, 1 week ago

Amazon CloudFront is a content delivery network (CDN) that can deliver both real-time and on-demand streaming. It caches content at edge locations worldwide, providing low-latency delivery to a global audience.

B. AWS Global Accelerator: Global Accelerator is more suitable for non-HTTP use cases or when static IP addresses are required.
C. Amazon Route 53: Route 53 is a DNS service and not designed specifically for streaming video.
D. Amazon S3 Transfer Acceleration: S3 Transfer Acceleration improves upload speeds to Amazon S3 but does not directly enhance streaming performance.

upvoted 2 times

✉ **Jeeva28** 6 months ago

Selected Answer: A

Serve video on demand or live streaming video
CloudFront offers several options for streaming your media to global viewers—both pre-recorded files and live events.

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 1 times

✉ **Kumaran1508** 6 months ago

Selected Answer: B

I vote for B. Global Accelerator.
CloudFront Video on Demand is specifically designed for delivering on-demand video content, meaning pre-recorded videos that can be streamed or downloaded. It is not suitable for streaming real-time videos or live video broadcasts.
Global Accelerator helps in reducing network hops between the user and AWS making real-time streams smoother.

upvoted 3 times

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

Selected Answer: B

To get the benefit of CloudFront video needs to be cached, so requests should be frequent. On demand video - I vote for B
upvoted 1 times

✉ **warioverde** 8 months, 1 week ago

How can Cloudfront help with real-time use case?
upvoted 2 times

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

Amazon CloudFront
upvoted 1 times

✉ **aba2s** 10 months, 4 weeks 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>

upvoted 2 times

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

AC (71%)

CE (29%)

 **jdr75** Highly Voted 7 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 7 times

 **Ruffyit** Most Recent 1 day, 21 hours 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** 1 month, 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 3 times

 **TariqKipkemei** 2 months, 3 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** 3 months, 2 weeks 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** 4 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** 4 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** 4 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** 5 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** 9 months 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** 9 months 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** 9 months 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** 10 months, 1 week ago

Selected Answer: AC

A/C for security to prevent anonymous access

upvoted 3 times

👤 **JayBee65** 10 months, 4 weeks ago

I'm thinking A and C

A - the API is publicly accessible but there is nothing to stop the company requiring users to register for access.

B - you can do this with Lambda, AWS Network Firewall and Amazon GuardDuty, see <https://aws.amazon.com/blogs/security/automatically-block-suspicious-traffic-with-aws-network-firewall-and-amazon-guardduty/>, but these components are not mentioned

C - a WAF is the logical choice with its bot detection capabilities

D - a private API is only accessible within a VPC, so this would not work

E - would be even more work than A

upvoted 3 times

👤 **HayLLIHuK** 10 months, 4 weeks ago

Selected Answer: AC

<https://www.examtopics.com/discussions/amazon/view/61082-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

👤 **techhb** 11 months ago

Selected Answer: AC

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>
<https://medium.com/@tshemku/aws-waf-vs-firewall-manager-vs-shield-vs-shield-advanced-4c86911e94c6>
upvoted 2 times

 **SoluAWS** 11 months, 1 week ago

I do not agree with A as it mentioned the application is publically accessible. "A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda". If this is public how can we ensure that genuine user?

I will go with CD
upvoted 3 times

 **techhb** 11 months, 1 week ago

Selected Answer: AC

A and C ,C is obvious ,however A is the only other which seems to put quota 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

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

C (83%) B (17%)

✉  **babaxoxo** Highly Voted 1 year ago

Selected Answer: C

Ans C:

Cost-effective solution with milliseconds of retrieval -> it should be s3 standard
upvoted 8 times

✉  **xdkonorek2** Most Recent 3 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** 3 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 2 times

✉  **Its_SaKar** 2 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 1 times

✉  **TariqKipkemei** 2 months, 3 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** 3 months ago

Selected Answer: C

ANS - C

upvoted 1 times

 **Guru4Cloud** 3 months, 2 weeks 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** 4 months ago

Selected Answer: C

<https://aws.amazon.com/s3/storage-classes/glacier/instant-retrieval/>

upvoted 1 times

 **cookieMr** 5 months, 1 week 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** 5 months, 3 weeks ago

Selected Answer: B

<https://aws.amazon.com/s3/storage-classes/glacier/instant-retrieval/>

upvoted 3 times

 **KZM** 9 months, 2 weeks 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** 10 months, 3 weeks 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/amazon-glacier/latest/dev/introduction.html>

upvoted 3 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **lapaki** 11 months, 3 weeks ago

Selected Answer: C

JSON is object notation. S3 stores objects.

upvoted 1 times

 **hpipit** 12 months ago

Selected Answer: C

c IS correct

upvoted 1 times

 **Wpcorgan** 1 year ago

C is correct

upvoted 1 times

 **sdasdawa** 1 year 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** 12 months ago

ElasticSearch is a search service, the question states here about the backup service reqd. for the DR scenario.

upvoted 3 times

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

B (94%)	6%
---------	----

✉  **babaxoxo**  1 year ago

Selected Answer: B

solution should remove operation overhead -> s3 -> lambda -> aurora
upvoted 11 times

✉  **markw92** 5 months, 2 weeks 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** 2 months ago

sql database, not sql server
upvoted 1 times

✉  **Zerotn3**  11 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

✉  **David_Ang**  1 month, 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 make for this
upvoted 1 times

✉  **Mandar15** 2 months ago

Selected Answer: B

B is correc
upvoted 1 times

✉  **TariqKipkemei** 2 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** 3 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** 4 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** 5 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 2 times

 **Bmarodi** 6 months, 1 week ago

Selected Answer: B

Keywords here are : "maximizes scalability and minimizes operational overhead, hence option B is correct answer.

upvoted 1 times

 **channn** 7 months, 3 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

 **perception** 9 months 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** 9 months, 1 week ago

B is the best option. <https://aws.amazon.com/rds/aurora/>

upvoted 1 times

 **mp165** 11 months ago

Selected Answer: B

agree...B is the best option S3, Lambda , Aurora.

upvoted 1 times

 **techhb** 11 months, 1 week 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** 11 months, 2 weeks 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** 11 months, 1 week 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

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **Phinx** 1 year ago

Selected Answer: B

D is incorrect because using ECS entails a lot of admin overhead. so B is the correct one.

upvoted 1 times

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** Highly Voted 11 months, 3 weeks ago

Selected Answer: A

If you see HPC and Linux both in the question.. Pick Amazon FSx for Lustre
upvoted 22 times

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

yeap, you're right!
upvoted 2 times

✉  **aba2s** Highly Voted 10 months, 4 weeks 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 7 times

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

Selected Answer: A

HPC workloads running on Linux = Amazon FSx for Lustre
upvoted 1 times

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

High performance - Lustre
upvoted 1 times

✉  **Guru4Cloud** 3 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** 5 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** 6 months, 1 week ago

Selected Answer: A

Option A is right answer.

upvoted 1 times

✉ **kerin** 9 months, 1 week 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** 10 months, 4 weeks ago

Selected Answer: A

Amazon FSx for Lustre integrated with Amazon S3

upvoted 1 times

✉ **techhb** 11 months, 1 week ago

Selected Answer: A

A is right choice here.

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: A

Option A is the best high performance storage with integration to S3

upvoted 1 times

✉ **wly_al** 11 months, 2 weeks 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** 11 months, 3 weeks 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 ago

A is correct

upvoted 1 times

✉ **BENICE** 1 year ago

A - for HPC "Amazon FSx for Lustre" and long-term persistence "S3"

upvoted 1 times

✉ **rjam** 1 year ago

Amazon FSx for Lustre:

- HPC optimized distributed file system, millions of IOPS
- Backed by S3

upvoted 3 times

✉ **rjam** 1 year ago

Answer A

upvoted 1 times

✉ **babaxoxo** 1 year ago

Selected Answer: A

FSx Lustre integrated with S3

upvoted 1 times

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** Highly Voted 1 year ago

Selected Answer: A

AWS Fargate

upvoted 11 times

 **ACloud_Guru15** Most Recent 1 month ago

Selected Answer: A

ECR+ECS+Fargate = Less overhead

upvoted 1 times

 **Sindokuhlep** 1 month ago

Selected Answer: A

Fargate

upvoted 1 times

 **TariqKipkemei** 2 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** 3 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 1 times

 **MikeDu** 3 months, 2 weeks ago

Selected Answer: A

AWF Fargate should be the best choice

upvoted 1 times

 **aadityaravi8** 4 months, 3 weeks ago

A is the right answer undoubtedly.

upvoted 1 times

 **cookieMr** 5 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** 4 months, 2 weeks ago

Nice explanations!

upvoted 1 times

 **Bmarodi** 6 months, 1 week ago

Selected Answer: A

ECS + Fargate satisfy requirements, hence option A is the best solution.

upvoted 1 times

 **studynoplay** 6 months, 2 weeks ago

Selected Answer: A

minimize operational overhead = Serverless

Fargate is Serverless

upvoted 1 times

 **NoInNothing** 7 months, 2 weeks ago

Selected Answer: A

Correct is "A"

upvoted 1 times

 **jaswantn** 7 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

 **SkyZeroZx** 7 months, 4 weeks ago

Selected Answer: A

A

Why ?

Because fargate provisioned on demand resource

upvoted 2 times

 **CheckpointMaster** 11 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** 11 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **alect096** 11 months, 2 weeks ago

Selected Answer: A

"minimizes operational overhead" --> Fargate is serverless

upvoted 2 times

 **Shasha1** 11 months, 3 weeks ago

A

AWS Fargate is a serverless experience for user applications, allowing the user to concentrate on building applications instead of configuring and managing servers. Fargate also automates resource management, allowing users to easily scale their applications in response to demand.

upvoted 1 times

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

C (88%) 12%

 **aba2s** Highly Voted 10 months, 4 weeks 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 9 times

 **TariqKipkemei** Most Recent 2 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 2 times

 **Guru4Cloud** 3 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** 4 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** 5 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 3 times

✉ **Bmarodi** 4 months, 2 weeks ago

Nice explanations always, thanks a lot!

upvoted 1 times

✉ **Bmarodi** 3 months, 2 weeks ago

Nice explanations always, thanks a lot

upvoted 1 times

✉ **Jeeva28** 6 months ago

Selected Answer: C

Answer C, In Question if Keyword have Processing Failed >> SQS

upvoted 1 times

✉ **Bmarodi** 6 months, 1 week 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** 6 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** 6 months, 2 weeks ago

Selected Answer: C

operationally efficient = Serverless

SQS is serverless

upvoted 1 times

✉ **studynoplay** 6 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** 7 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** 4 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** 9 months ago

SQS has a limit 12h for visibility time out

upvoted 1 times

✉ **bullrem** 10 months, 1 week 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** 9 months 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** 7 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** 10 months ago

There's no way for kinesis to know whether the message processing failed.

upvoted 1 times

✉️ **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C.

upvoted 1 times

✉️ **ocbn3wby** 12 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

✉️ **Kapello10** 1 year ago

Selected Answer: C

Option C is the correct ans

upvoted 1 times

✉️ **Gabs90** 1 year ago

Selected Answer: C

C is correct. The B is wrong because the question ask for a way to let the two application to communicate, so the process is already done

upvoted 1 times

✉️ **TelaO** 1 year ago

Selected Answer: B

Please explain why "B" is incorrect? How does SQS process data?

"KCL helps you consume and process data from a Kinesis data stream by taking care of many of the complex tasks associated with distributed computing."

<https://docs.aws.amazon.com/streams/latest/dev/shared-throughput-kcl-consumers.html>

upvoted 2 times

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

As per question, the processing application will take messages.

"The company wants to implement an AWS service to handle messages between the two applications."

upvoted 1 times

✉️ **ocbn3wby** 12 months ago

The processing is done at the 2nd application level.

This seems to be the job of Dead Letter Q

upvoted 1 times

✉️ **KADSM** 1 year ago

Kinesis may not be having message retry - there is no way for kinesis to know whether the message processing failed. message can be there till their retention period.

upvoted 4 times

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

D (57%)

B (43%)

✉  **Nigma**  1 year ago

Answer D. Use an OAI to lockdown CloudFront to S3 origin & enable WAF on CF distribution

upvoted 25 times

✉  **FNJ1111** 11 months ago

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/> confirms use of OAI (and option D).

upvoted 9 times

✉  **cookieMr**  5 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 6 times

✉  **bogobob** 2 weeks, 6 days 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

✉  **wearrexdzw3123**  2 weeks, 6 days 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** 3 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** 1 month, 1 week 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 4 times

✉  **fageroff** 1 month 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** 1 month, 3 weeks ago

Selected Answer: B

voting B because of inspecting traffic

upvoted 1 times

 **javiems** 2 months 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 2 times

 **vijaykamal** 2 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 1 times

 **JKevin778** 2 months ago

Selected Answer: D

<https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html>

D

upvoted 1 times

 **BrijMohan08** 2 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** 2 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

 **mtnmayer** 3 months, 1 week ago

Selected Answer: D

D for me.

upvoted 2 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

This option meets the requirements by:

Using CloudFront with an S3 origin to store the static website

Configuring CloudFront to forward requests to AWS WAF first for inspection before fetching content from S3

This allows AWS WAF to inspect all traffic to the website per the security policy

upvoted 1 times

 **Willnotsin** 4 months ago

Answer D

upvoted 2 times

 **Nazmul123** 4 months ago

D

CloudFront's Origin Access Identity (OAI) is a special CloudFront user that you can associate with your distribution. By applying an OAI to your S3 bucket, you're able to securely lock down all direct access to your S3 files and require all requests to come through CloudFront.

Amazon Web Application Firewall (WAF) is a security feature that helps protect your resources against common exploits. You can configure AWS WAF directly on your CloudFront distribution to inspect incoming requests to your web application.

upvoted 2 times

 **sosda** 4 months, 2 weeks ago

Selected Answer: D

WAF associated with cloudfront on creation/distribution. No need to forward request to WAF
upvoted 2 times

Dhaysindhu 5 months ago

Selected Answer: B

I vote for B!

Option D is not correct, OAI in CloudFront and restricting access to the S3 bucket does not ensure that all website traffic is inspected by AWS WAF.
upvoted 1 times

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** Highly Voted 11 months, 1 week 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 7 times

 **TariqKipkemei** Most Recent 2 months, 2 weeks ago

Selected Answer: D

Global users = Amazon CloudFront

upvoted 1 times

 **Guru4Cloud** 3 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** 5 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 3 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **k1kavi1** 11 months, 2 weeks ago

Selected Answer: D

Agreed

upvoted 1 times

 **Sahilbhai** 11 months, 3 weeks ago

answer is D agree with Shasha1

upvoted 1 times

 **Shasha1** 11 months, 3 weeks 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 ago

D is correct

upvoted 2 times

 **Nigma** 1 year ago

D

Static content on S3 and hence Cloudfront is the best way

upvoted 2 times

 **Pamban** 1 year ago

Selected Answer: D

D is the correct answer

upvoted 2 times

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

D (52%) C (47%)

✉  **HayLLIHuK** Highly Voted 10 months, 4 weeks ago

Selected Answer: C

"without any downtime" - Reserved Instances for the baseline capacity
 "MOST cost-effectively" - Spot Instances to handle additional capacity
 upvoted 20 times

✉  **kraken21** 8 months ago

How can you have baseline capacity when your message volume is unpredictable and often has intermittent traffic?
 upvoted 2 times

✉  **MutiverseAgent** 4 months, 1 week ago

For this reason I think correct answer is A
 upvoted 1 times

✉  **Macadam** 2 weeks, 1 day ago

Spot instances cannot be an option as it is unreliable and the question requires the messages to be continuously processed
 upvoted 1 times

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

Dude, read the question, cost consideration was not mentioned in the question.
 upvoted 1 times

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

Dude, read the question, "Which solution meets these requirements MOST cost-effectively?"
 upvoted 18 times

✉  **MrSaint** 7 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 3 times

✉  **kraken21** 7 months, 4 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** 2 months, 3 weeks ago

Intermediate data stored in SQS queue so once free then it take data and process.
 upvoted 1 times

✉  **taer** Highly Voted 1 year ago

Selected Answer: D

D is the correct answer
 upvoted 20 times

✉  **Drayen25** 9 months, 3 weeks ago

C is correct, read for cost effectiveness

upvoted 5 times

 **diabloexodia** 4 months, 2 weeks ago

AWS has stopped issuing spot instances so i think C

upvoted 1 times

 **diabloexodia** 4 months, 2 weeks ago

so i think C is incorrect*. the Correct ans is D.

upvoted 1 times

 **sezer** 8 months ago

if you cannot find enough spot instance you will have downtime

you cannot always find spot instance

upvoted 9 times

 **Kumaran1508** 6 months ago

Why downtime when there are baseline reserved instances?

upvoted 2 times

 **Sutariya** 2 months, 3 weeks ago

Baseline reserved instances and ondemand Spot instance is cost saver

upvoted 1 times

 **Marco_St** Most Recent 3 days, 18 hours 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** 1 week, 2 days ago

Selected Answer: D

spot instance is not reliable solution

upvoted 1 times

 **Richi0907** 1 week, 3 days ago

Selected Answer: C

cccccccccc

upvoted 1 times

 **Alex1atd** 3 weeks, 6 days ago

Selected Answer: D

NO Downtime != spot instance

Yes, C is cheaper, but you could have downtime. The request is to be Cost-effective, but also no downtime. To accomplish both, the answer is D (it will cost more than C, this is for sure, but you will have no downtime)

upvoted 2 times

 **wsdasdasdqwdaw** 1 month ago

C is more effective than D but it is not possible because of the last requirement "This application should continually process messages without any downtime." So spot instances are out of the games as well as C option. The correct one is option D

upvoted 3 times

 **rlamberti** 1 month, 1 week ago

Selected Answer: D

"process messages without any downtime"

Spot instances can be terminated anytime, so C is not an option.

Answer is D.

upvoted 2 times

 **awashenko** 1 month, 2 weeks ago

Selected Answer: D

I commented on a few post arguing for C but I spent 20 mins just thinking about this question. Its tricky because your weighing the cost and downtime perspective. The reason I now think its D is because there is a chance you might not get a spot instance when you get an influx of data over the amount of your reserve. In this case, you would have downtime as there arent any spot instances available and you have more data than the reserve can handle. So I think D is the correct answer with On-Demand.

upvoted 1 times

 **Ramdi1** 1 month, 3 weeks ago

Selected Answer: C

C is correct, it is not just relying on the spot instance, when the instance become available it can be added back in.

upvoted 1 times

 **mildewCake** 2 months ago

Selected Answer: D

D: On-demand instances would always be available, whereas Spot (C) would not.
upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

without any downtime = NO Spot Instances
upvoted 3 times

 **awashenko** 1 month, 2 weeks ago

The reserve instances would cover for this. There still shouldnt be downtime.

I think Spot instance is correct. The only issue I could possibly see here is if you got a massive influx of data coming in and couldnt get any spot instances. I'm not sure if thats ever been an issue though.

upvoted 1 times

 **daniel33** 2 months, 2 weeks ago

Selected Answer: D

D is the answer - the question states "should continually process messages without any downtime".
So, spot instances can offer up to 90% discount but quickly get interrupted.
upvoted 1 times

 **TariqKipkemei** 2 months, 2 weeks ago

Selected Answer: D

'This application should continually process messages without any downtime'.
With spot instances there are chances of downtime.
On-demand will handle the peak times with no downtime.
upvoted 1 times

 **Valder21** 2 months, 3 weeks ago

Selected Answer: D

without any downtime=no spot instances
upvoted 1 times

 **coolkidsclubvip** 3 months ago

Selected Answer: C

C has no downtime either
upvoted 1 times

 **AKBM7829** 3 months ago

D is correct answer
Keyword: unpredictable and often has intermittent traffic is ON-Demand
upvoted 1 times

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** Highly Voted 1 year 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 13 times

✉️  **cookieMr** Highly Voted 5 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 7 times

✉️  **awashenko** 1 month, 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

✉️  **mach2022** Most Recent 4 weeks ago

is D because of Deeznuts

upvoted 1 times

✉️  **xplusfb** 1 month, 1 week ago

Selected Answer: D

Its very clear question answer is D

upvoted 1 times

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

Selected Answer: D

<https://medium.com/@darekhale91/how-to-pass-amazon-saa-c03-exam-dumps-2023-583619ddbcc8>

upvoted 1 times

✉️  **TariqKipkemei** 2 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** 3 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** 6 months, 1 week 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** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **Wpcorgan** 1 year ago

D iscorrect

upvoted 1 times

 **babaxoxo** 1 year ago

an organization and requires single point place to manage permissions

upvoted 2 times

 **goatbernard** 1 year ago

Selected Answer: D

SCP for organization

upvoted 3 times

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** Highly Voted 6 months, 2 weeks ago

What's going on, suddenly the questions are so easy
upvoted 6 times

 **Sutariya** 4 months ago

Its due to confidence level going up after experience.
upvoted 3 times

 **awashenko** Most Recent 1 month, 2 weeks ago

Selected Answer: C
When you see DDOS immediately think Shield
upvoted 2 times

 **TariqKipkemei** 2 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** 3 months, 1 week ago

Selected Answer: C
Enable AWS Shield Advanced to prevent attacks.
upvoted 1 times

 **cookieMr** 5 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** 11 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** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: C

C is right answer

upvoted 1 times

 **Wpcorgan** 1 year ago

C is correct

upvoted 1 times

 **goatbernard** 1 year ago

Selected Answer: C

AWS Shield Advanced

upvoted 3 times

 **Nigma** 1 year ago

DDOS = AWS Shield

upvoted 4 times

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 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 18 times

 **Guru4Cloud**  3 months, 1 week ago

Selected Answer: C

C. Configure AWS WAF on the Application Load Balancer in a VPC

upvoted 1 times

 **Sutariya** 4 months ago

We can use AWS WAF to configure access control rule to access from specific location.

upvoted 1 times

 **cookieMr** 5 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** 6 months ago

Configure AWS WAF for Geo Match Policy

upvoted 1 times

 **aba2s** 10 months, 3 weeks 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** 11 months, 1 week 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

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 11 months, 2 weeks ago

Selected Answer: C

OptionC. Configure WAF for Geo Match Policy

upvoted 1 times

Wpcorgan 1 year ago

C is correct

upvoted 1 times

mricee9 1 year 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 ago

C. WAF with ALB is the right option

upvoted 1 times

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 (95%)	5%
---------	----

 **bullrem** Highly Voted 10 months, 1 week 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 17 times

 **paniya93** Most Recent 1 month, 4 weeks ago

Selected Answer: B

in 002 answer is B. Why is that?

upvoted 1 times

 **vijaykamal** 2 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** 2 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 1 times

 **TariqKipkemei** 2 months, 2 weeks ago

Selected Answer: B

scalable and elastic = serverless = API gateway and AWS Lambda

upvoted 1 times

 **Guru4Cloud** 3 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 1 times

✉  **cookieMr** 5 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** 6 months, 1 week ago

Selected Answer: B

Option B is the solution that is scalable and elastic, hence this meets requirements.

upvoted 1 times

✉  **jayce5** 7 months, 1 week 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** 10 months ago

B. Serverless option wins over EC2

upvoted 4 times

✉  **sona21** 11 months, 1 week ago

Lambda is serverless is scalable so answer should be B.

upvoted 2 times

✉  **Buruguduystunstugudunstuy** 11 months, 1 week 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

✉  **markw92** 5 months, 2 weeks 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 1 times

✉  **Buruguduystunstugudunstuy** 11 months, 1 week 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** 10 months, 3 weeks 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 2 times

✉  **JayBee65** 10 months, 3 weeks ago

Sorry, it should say "Therefore D is wrong, and B is possible."

upvoted 2 times

✉  **BENICE** 11 months, 2 weeks ago

B is the option

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B. Though D is also possible B is more scalable as Lambda will autoscale to meet the dynamic load.

upvoted 4 times

 **Gil80** 11 months, 4 weeks ago

Selected Answer: B

B. Lambda scales much better

upvoted 2 times

 **Kapello10** 1 year ago

B is the correct ans

upvoted 1 times

 **Gabs90** 1 year ago

Selected Answer: B

B is correct, lambda is a better choice

upvoted 1 times

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

C (77%) B (23%)

 **Bobbybash** Highly Voted 1 year 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 32 times

 **vijaykamal** Most Recent 2 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 2 times

 **Guru4Cloud** 3 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** 4 months ago

Would the HTTPS imply that the cert was signed by a CA

upvoted 1 times

 **cookieMr** 5 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** 6 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

 **Whericanstart** 8 months, 3 weeks 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 2 times

 **bdp123** 10 months 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** 10 months ago

C, field-level encryption should be used when necessary to protect sensitive data.

upvoted 1 times

 **ayanshbhaiji** 10 months, 3 weeks ago

It should be C

upvoted 2 times

 **HayLLIHuK** 10 months, 4 weeks 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

 **kbaruu** 10 months, 4 weeks ago

Selected Answer: C

Field-Level Encryption allows you to securely upload user-submitted sensitive information to your web servers. x Signed cookie - provides access to download multiple private files (from Tutorial Dojo)

upvoted 1 times

 **Mindvision** 11 months ago

C = Answer

I concur. why? 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.

upvoted 2 times

 **Zerotn3** 11 months ago

Selected Answer: B

he correct answer is B. Configure a CloudFront signed cookie.

CloudFront signed cookies can be used to protect sensitive information by requiring users to authenticate with a signed cookie before they can access content that is served through CloudFront. This can be used to restrict access to certain applications and ensure that the sensitive information is protected throughout the entire application stack.

Option A, Configure a CloudFront signed URL, would also provide an additional layer of security by requiring users to authenticate with a signed URL before they can access content served through CloudFront. However, this option would not protect the sensitive information throughout the entire application stack.

upvoted 2 times

 **Zerotn3** 11 months ago

Option C, Configure a CloudFront field-level encryption profile, can be used to protect sensitive information that is stored in Amazon S3 and served through CloudFront. However, this option would not provide an additional layer of security for the entire application stack.

upvoted 1 times

 **JayBee65** 10 months, 3 weeks ago

CloudFront signed cookie are used to control user access to sensitive documents but that is not what is required. "Some of the information submitted by users is sensitive" This is what you are looking to protect, when it's in the system, (not when users are trying to access it and this is not mentioned in the Q).

Field-level encryption encrypts sensitive data ... This ensures sensitive data can only be decrypted and viewed by certain components or services. (q states "access to the information should be restricted to certain applications."), so C is a perfect match

upvoted 1 times

 **muhtoy** 11 months, 1 week ago

Selected Answer: B

configuring a CloudFront signed cookie is a better solution for protecting sensitive information and restricting access to certain applications throughout the entire application stack. This will allow them to restrict access to content based on the viewer's identity and ensure that the sensitive information is protected throughout the entire application stack

upvoted 1 times

 **techhb** 11 months, 1 week ago

Selected Answer: C

Option B, "Configure a CloudFront signed cookie," is not a suitable solution for this scenario because signed cookies are used to grant temporary access to specific content in your CloudFront distribution. They do not provide an additional layer of security for the sensitive information submitted by users, nor do they allow you to restrict access to certain applications.

upvoted 1 times

 **NV305** 11 months, 1 week ago

Selected Answer: B

Field-level encryption profiles, which you create in CloudFront, define the fields that you want to be encrypted.

upvoted 1 times

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

B (94%)

6%

 **Nigma** Highly Voted 1 year 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 18 times

 **rlamberti** Most Recent 1 month, 1 week 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** 2 months, 2 weeks ago

Selected Answer: B
Deploy an Amazon CloudFront web distribution in front of the S3 bucket
upvoted 1 times

 **Guru4Cloud** 3 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** 4 months, 1 week ago

Selected Answer: B
ElasticCache is for DB Cache(RDS) nor for S3
upvoted 1 times

 **cookieMr** 5 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 3 times

 **kruasan** 7 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 3 times

✉ **LuckyAro** 10 months, 2 weeks 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

✉ **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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

✉ **Bofi** 9 months 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

✉ **ocbn3wby** 10 months 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** 10 months ago

Answers are mostly correct. Only a small percentage were wrong

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

✉ **k1kavi1** 11 months, 2 weeks ago

Selected Answer: B

Agreed

upvoted 1 times

✉ **rewdboy** 1 year ago

Selected Answer: B

B is the correct answer

upvoted 1 times

✉ **Wpcorgan** 1 year ago

B is correct

upvoted 1 times

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** Highly Voted 1 year ago
B. auto scaling groups can not span multi region
upvoted 22 times

 **TariqKipkemei** Most Recent 2 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** 3 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 1 times

 **cookieMr** 5 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 4 times

 **techhb** 11 months, 1 week ago
B. auto scaling groups cannot span multi region
upvoted 1 times

 **Buruguduystunstugudunstuy** 11 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.

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** 11 months, 2 weeks ago
Selected Answer: B
Option B
upvoted 1 times

 **k1kavi1** 11 months, 2 weeks ago

Selected Answer: B

Agreed

upvoted 1 times

 **Shasha1** 11 months, 3 weeks 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 ago

Selected Answer: B

B is rightt

upvoted 1 times

 **Wpcorgan** 1 year ago

B is correct

upvoted 1 times

 **xua81376** 1 year ago

B auto scaling i multiple AZ

upvoted 1 times

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 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/rds/proxy/>

upvoted 26 times

✉️  **babaxoxo**  1 year ago

Selected Answer: B

Issue related to opening many connections and the solution requires least code changes so B satisfies the conditions
upvoted 6 times

✉️  **TariqKipkemei**  2 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 1 times

✉️  **Guru4Cloud** 3 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** 5 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 4 times

 **obifranky** 7 months, 4 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** 10 months, 2 weeks ago

I also think the answer is B. However can RDS Proxy be used with Amazon Aurora PostgreSQL database?
upvoted 1 times

 **everfly** 9 months ago

RDS Proxy can be used with Aurora
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>
upvoted 3 times

 **gustavtd** 11 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** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 2 weeks ago

Option --- B

upvoted 1 times

 **career360guru** 11 months, 2 weeks 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** 11 months, 3 weeks 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 ago

B is correct

upvoted 1 times

 **xua81376** 1 year ago

B - Proxy to manage connections

upvoted 2 times

 **Nigma** 1 year ago

Correct B

upvoted 1 times

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** Highly Voted 1 year ago

Selected Answer: A

VPC endpoints for service in private subnets

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

upvoted 10 times

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

Selected Answer: A

VPC endpoints for service in private subnets

upvoted 1 times

 **RashiJaiswal** 4 months, 3 weeks ago

Selected Answer: A

VPC endpoint for dynamodb and S3

upvoted 1 times

 **cookieMr** 5 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 4 times

 markw92 5 months, 2 weeks 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 1 times

 dmt6263 6 months, 2 weeks ago

AAAAAAA

upvoted 1 times

 gx2222 7 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 8 months, 3 weeks 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 9 months, 2 weeks ago

private...backend Answer A

upvoted 1 times

 bdp123 10 months 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 10 months ago

ExamTopics.com should be sued for this answer tagged as Correct answer.

upvoted 4 times

 mp165 11 months ago

Selected Answer: A

A is correct. VPC end point. D exposed to the internet

upvoted 3 times

 Buruguduystunstugudunstuy 11 months, 1 week 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 11 months, 1 week 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

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** Highly Voted 11 months, 1 week 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 17 times

✉  **cookieMr** Highly Voted 5 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 8 times

✉  **TariqKipkemei** Most Recent 2 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** 6 months ago

Selected Answer: B

improve the performance efficiency of DynamoDB

upvoted 1 times

✉  **gx2222** 7 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** 8 months, 1 week ago

B-->Applications that are read-intensive==><https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.html#DAX.use-cases>

upvoted 1 times

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

Selected Answer: B

DynamoDB Accelerator, less overhead.

upvoted 2 times

✉  **wmp7039** 10 months, 2 weeks 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

✉  **Burugudystunstugudunstuy** 11 months, 1 week 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

✉  **Burugudystunstugudunstuy** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 2 times

✉  **k1kavi1** 11 months, 2 weeks ago

Selected Answer: B

Agreed

upvoted 2 times

✉  **Shasha1** 11 months, 3 weeks 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 ago

B is correct

upvoted 1 times

✉  **goatbernard** 1 year ago

Selected Answer: B

DAX is the cache for this

upvoted 1 times

✉  **nhlegend** 1 year ago

B is correct, DAX provides caching + no changes

upvoted 2 times

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 (96%) 4%

 **cookieMr** Highly Voted 5 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 5 times

 **Guru4Cloud** Most Recent 3 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** 3 months, 4 weeks ago

D would have been a great option but the question requires less manual effort. So, A is better.

upvoted 1 times

 **cheese929** 6 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 2 times

 **kruasan** 7 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** 7 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** 7 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** 11 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** 11 months ago

A is correct - you need to find a backup solution for EC2 and RDS. DLM doent work with RDS , only with snapshots.

upvoted 1 times

✉ **techhb** 11 months, 1 week 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** 11 months, 1 week 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

✉ **YogK** 6 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

✉ **HayLLIHuK** 10 months, 4 weeks 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** 11 months, 1 week 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

✉ **Kruiz29** 10 months, 2 weeks ago

This guy is giving wrong answers in detail...lol

upvoted 4 times

✉ **PassNow1234** 11 months, 1 week ago

Some of your answers are very detailed. Can you back them up with a reference?

upvoted 2 times

✉ **jwu413** 10 months ago

All of their answers are from ChatGPT

upvoted 5 times

techhb 11 months, 1 week 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

egmira 10 months, 1 week 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

PassNow1234 11 months ago

Thanks techhb

upvoted 1 times

career360guru 11 months, 2 weeks ago

Selected Answer: A

Option A as it is fully managed service with least operational overhead

upvoted 1 times

Shasha1 11 months, 3 weeks 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 ago

Selected Answer: A

Ans A with least operational overhead

upvoted 1 times

rjam 1 year ago

AWS Backup supports Supports cross-region backups

upvoted 3 times

rjam 1 year ago

Selected Answer: A

Option A

Aws back up supports , EC2, RDS

upvoted 3 times

rjam 1 year ago

AWS Backup suports Supports cross-region backups

upvoted 1 times

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

A (92%) 8%

 **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week 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 7 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 5 times

 **sdasdawa** Highly Voted 1 year ago

Selected Answer: A

Agree with A, IAM role is for services (EC2 for example)
IAM policy is more for users and groups

upvoted 6 times

 **TariqKipkemei** Most Recent 2 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** 3 months, 1 week ago

Selected Answer: A

CORRECT Option A

upvoted 1 times

 **cookieMr** 5 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** 6 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

✉ **kruasan** 7 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** 10 months, 4 weeks 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** 11 months, 2 weeks ago

A -- is correct option

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

Option A.

upvoted 1 times

✉ **k1kavi1** 11 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

✉ **Shasha1** 11 months, 3 weeks 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 ago

Selected Answer: B

i think policy

upvoted 1 times

✉ **[Removed]** 1 year 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

✉ **[Removed]** 1 year 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** 10 months, 3 weeks 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

✉ **turalmth** 11 months, 4 weeks ago

can you attach policy to ec2 directly ?

upvoted 1 times

✉ **EKA_CloudGod** 1 year 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 ago

Selected Answer: A

Attach IAM role to EC2 Instance profile

upvoted 3 times

 **goatbernard** 1 year ago

Selected Answer: B

IAM policy

upvoted 1 times

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

BC (93%)	4%
----------	----

✉  **babaxoxo**  1 year ago

Selected Answer: BC

Shield - Load Balancer, CF, Route53
AWS - CF, ALB, API Gateway

upvoted 36 times

✉  **YogK** 6 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 5 times

✉  **Ouk** 11 months, 1 week ago

Thank u U meant WAF* - CloudFormation, right? haha

upvoted 4 times

✉  **rjam**  1 year 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 6 times

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

don't agree that NLB sits before API gateway. it should be other way around

upvoted 3 times

✉  **aadityaravi8** 4 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**  3 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 2 times

✉  **Sat897** 3 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** 5 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 2 times

✉ **cheese929** 6 months, 3 weeks ago

Selected Answer: BC

B and C is correct

upvoted 1 times

✉ **kruasan** 7 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** 7 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** 10 months 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** 10 months, 1 week 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

✉ **omoakin** 6 months, 1 week ago

correct

upvoted 1 times

✉ **bullrem** 10 months, 1 week 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

✉ **bullrem** 10 months, 1 week 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** 4 months, 2 weeks ago

A is not correct as WAF doesn't support Network Load Balancer

upvoted 1 times

 **drabi** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 1 week ago

Ans:-a and C

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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 3 times

 **jwu413** 10 months ago

This guy just copies and pastes from ChatGPT.

upvoted 4 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 2 weeks ago

Option B and C

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: BC

B and C

upvoted 1 times

 **tz1** 11 months, 3 weeks ago

B & C is the answer

upvoted 1 times

 **Wpcorgan** 1 year ago

B and C

upvoted 1 times

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

A (90%)	10%
---------	-----

 **Buruguduystunstugudunstuy** Highly Voted  11 months, 1 week 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 13 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 4 times

 **TariqKipkemei** Most Recent  2 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** 3 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 2 times

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

BBBBBBBBBB

upvoted 1 times

 **Bmarodi** 6 months, 1 week ago

Selected Answer: A

SQS for decoupling a monolithic architecture, hence option A is the right answer.

upvoted 1 times

 **Madhuaws** 7 months, 4 weeks ago

it also says 'the order of results does not matter'. Option B is correct.

upvoted 1 times

 **asoli** 8 months, 2 weeks 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** 9 months ago

Selected Answer: B

it doesn't say it is one-one relationships , SNS is better

upvoted 3 times

 **markw92** 5 months, 2 weeks ago

watch out for this sentence in the question..."Data needs to process sequentially...."

upvoted 2 times

 **career360guru** 11 months, 2 weeks 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** 11 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **Shasha1** 11 months, 3 weeks 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 ago

We need decoupling so ok to use SQS

upvoted 2 times

 **BENICE** 1 year ago

Can someone explain it bit more? Not able to understand it.

upvoted 2 times

 **EKA_CloudGod** 1 year ago

As monolithic systems become too large to deal with, many enterprises are drawn to breaking them down into the microservices architectural style by means of decoupling. Amazon Simple Queue Service (Amazon SQS) is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications

upvoted 14 times

 **taer** 1 year ago

Selected Answer: A

Answer is A

upvoted 2 times

 **Nigma** 1 year ago

SQS to decouple.

upvoted 2 times

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 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 15 times

 **studynoplay** Highly Voted  6 months, 2 weeks ago

Selected Answer: B

RDS Multi-AZ = Synchronous = Disaster Recovery (DR)
Read Replica = Asynchronous = High Availability
upvoted 6 times

 **riyasara** Most Recent  1 month, 1 week 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 1 times

 **cookieMr** 5 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** 7 months, 3 weeks ago

Selected Answer: B

B
since all other answers r wrong
upvoted 2 times

 **jayce5** 8 months ago

Selected Answer: B

B
Since read replica is async.

upvoted 1 times

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

Selected Answer: C

Multi AZ is not as protected as Multi-Region Read Replica.

upvoted 1 times

✉  **JayBee65** 10 months, 3 weeks ago

I curios to know why A isn't right. Is it just that it would take more effort?

upvoted 3 times

✉  **techhb** 11 months, 1 week ago

B is correct C requires more wokr.

upvoted 1 times

✉  **BENICE** 11 months, 2 weeks ago

Option B

upvoted 1 times

✉  **bammy** 11 months, 2 weeks 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** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

✉  **Shasha1** 11 months, 3 weeks 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** 10 months, 3 weeks 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** 11 months, 1 week 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** 11 months, 3 weeks 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 ago

B is correct

upvoted 1 times

✉  **EKA_CloudGod** 1 year ago

Selected Answer: B

Option B is the correct answer:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>

upvoted 1 times

✉  **Nigma** 1 year ago

B is the answer

upvoted 2 times

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

✉  **romko**  1 year 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 39 times

✉  **klayytech** 8 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 4 times

✉  **Yadav_Sanjay** 5 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 4 times

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

That's why Dynamo DB is best suited option

upvoted 1 times

✉  **Manlikeleke**  1 year ago

please is this dump enough to pass the exam?

upvoted 11 times

✉  **LuckyAro** 9 months, 3 weeks 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 6 times

✉  **Bobbybash** 1 year ago

I HOPE SO

upvoted 8 times

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

Selected Answer: A

dynamodb is serverless

upvoted 1 times

✉  **Angryasianxd** 2 months, 2 weeks 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.

 **n0pz** 2 months, 2 weeks ago

S3 is discarded since the question says: A company is building a new dynamic ordering website,
upvoted 1 times

 **TariqKipkemei** 2 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** 2 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 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

Minimize maintenance & Patching = Serverless
S3, DynamoDB are serverless
upvoted 1 times

 **ravindrabagale** 3 months, 2 weeks ago

Minimize maintenance & Patching = Serverless services
Serverless services with no sql database is perfect combination
upvoted 1 times

 **cookieMr** 5 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** 6 months 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** 6 months ago

Key word in question "storing ordering data"
DynamoDB is perfect for storing ordering data (key-values)
upvoted 2 times

 **studynoplay** 6 months, 2 weeks ago

Selected Answer: A

Minimize maintenance & Patching = Serverless
S3, DynamoDB are serverless
upvoted 2 times

 **lucdt4** 6 months, 3 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

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 1 times

 **DavidNamy** 10 months, 3 weeks 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** 10 months 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

 **Zerotn3** 11 months ago

Selected Answer: A

A for sure ~

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

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

A (74%)

C (26%)

✉  **Gil80**  12 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 15 times

✉  **markw92** 5 months, 2 weeks 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** 1 week, 2 days 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/QU\\$aj1a6jBQ92Kp56klbZFNw/aws-lambda-to-on-premise-via-direct-connect-and-aws-privatelink](https://repost.aws/questions/QU$aj1a6jBQ92Kp56klbZFNw/aws-lambda-to-on-premise-via-direct-connect-and-aws-privatelink)

upvoted 1 times

✉  **javitech83**  11 months, 3 weeks 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 8 times

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

C says to "update the route table" not create a new connection. C is correct.

upvoted 3 times

✉  **ruqui** 5 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** 7 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

✉  **xdkonorek2**  2 weeks, 4 days 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** 3 weeks, 1 day 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

✉ **Igor** 1 month, 2 weeks ago

Answer C is correct:

<https://repost.aws/questions/QUStj1a6jBQ92Kp56klbZFNw/aws-lambda-to-on-premise-via-direct-connect-and-aws-privatelink>

upvoted 1 times

✉ **Guru4Cloud** 3 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 2 times

✉ **zjcorpuz** 4 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** 5 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** 6 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** 7 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/QUStj1a6jBQ92Kp56klbZFNw/questions/QUStj1a6jBQ92Kp56klbZFNw/aws-lambda-to-on-premise-via-direct-connect-and-aws-privatelink?>

upvoted 2 times

✉ **Jinius83** 7 months, 2 weeks ago

C

AWS -> 회사 데이터 센터로 나가는 트래픽이기 때문에

upvoted 2 times

✉ **youdelin** 1 month, 2 weeks ago

dude, english

upvoted 1 times

 **darn** 7 months, 1 week ago

english please
upvoted 4 times

 **datz** 7 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 3 times

 **datz** 7 months, 3 weeks ago

it is telling non "VPC" traffic, really wish there was edit function lol
upvoted 1 times

 **Devsin2000** 8 months, 2 weeks 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

 **bdp123** 9 months, 1 week ago

Selected Answer: A

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

upvoted 2 times

 **nickolaj** 9 months, 2 weeks ago

Selected Answer: A

The best solution to meet the requirements would be option A - Configure the Lambda function to run in the VPC with the appropriate security group.

By configuring the Lambda function to run in the VPC, the function will have access to the private subnets in the company's data center through the Direct Connect connections. Additionally, security groups can be used to control inbound and outbound traffic to and from the Lambda function, ensuring that only the necessary traffic is allowed.

upvoted 2 times

 **nickolaj** 9 months, 2 weeks ago

Option B is not ideal as it would require additional configuration and management of a VPN connection between the company's data center and AWS, which may not be necessary for the specific use case.

Option C is not recommended as updating the route tables to allow the Lambda function to access the on-premises data center through Direct Connect would allow all VPC traffic to route through the data center, which may not be desirable and could potentially create security risks.

Option D is not a viable solution for accessing resources in the on-premises data center as Elastic IP addresses are only used for outbound internet traffic from an Amazon VPC, and cannot be used to communicate with resources in an on-premises data center.

upvoted 2 times

 **Yelizaveta** 9 months, 2 weeks ago

Selected Answer: A

"All non-VPC traffic routes to the virtual private gateway." means -> there are already the appropriate routes, so no need for update the route tables.

Key phrase: "database that runs in a private subnet in the company's data center.", means: You need the appropriate security group to access the DB.

upvoted 3 times

 **LuckyAro** 10 months, 2 weeks ago

Selected Answer: A

A makes more sense to me.

upvoted 1 times

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 11 months, 1 week 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 6 times

 **Buruguduystunstugudunstuy** 11 months, 1 week 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 5 times

 **Guru4Cloud** Most Recent 2 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 1 times

 **cookieMr** 5 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** 6 months ago

<https://repost.aws/knowledge-center/ecs-fargate-access-aws-services>

upvoted 1 times

 **k1kavi1** 11 months, 1 week 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** 11 months, 1 week 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 1 times

 **BENICE** 11 months, 2 weeks ago

Option B

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B.

upvoted 2 times

 **k1kavi1** 11 months, 2 weeks ago

Selected Answer: B

Agreed

upvoted 1 times

 **lighrz** 11 months, 3 weeks ago

Selected Answer: B

B is the best answer

upvoted 1 times

 **Wpcorgan** 1 year ago

B is correct

upvoted 1 times

 **taer** 1 year ago

Selected Answer: B

The answer is B.

upvoted 1 times

 **Nigma** 1 year ago

B is the answer

upvoted 2 times

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** Highly Voted 1 year ago

Correct is B
FSx --> shared Windows file system (SMB)
EFS --> Linux NFS
upvoted 8 times

 **TariqKipkemei** Most Recent 2 months, 2 weeks ago

Selected Answer: B

Windows file system = Amazon FSx for Windows File Server
upvoted 1 times

 **Guru4Cloud** 3 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** 5 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** 6 months, 1 week ago

Selected Answer: B

Option B is right answer.
upvoted 1 times

 **k1kavi1** 11 months, 1 week 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** 11 months, 1 week 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%20Window%20Server%20platforms.>
upvoted 1 times

 **Burugduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 2 weeks ago

B - is correct

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **Wpcorgan** 1 year ago

B is correct

upvoted 1 times

 **xua81376** 1 year ago

B FSx for windows

upvoted 1 times

 **BENICE** 1 year ago

B is correct option

upvoted 1 times

 **rjam** 1 year ago

Selected Answer: B

Amazon FSx for Windows File Server

upvoted 3 times

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** Highly Voted 11 months, 1 week 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

 **TariqKipkemei** Most Recent 2 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** 3 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** 4 months ago

Selected Answer: AD

AD is the correct answer

upvoted 1 times

 **cookieMr** 5 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 2 times

 **studynoplay** 6 months, 2 weeks ago

Selected Answer: AD

little manual intervention = Serverless

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: AD

Option A&D

upvoted 1 times

 **k1kavi1** 11 months, 2 weeks ago

Selected Answer: AD

A and D

upvoted 1 times

 **Gabs90** 1 year ago

Selected Answer: AD

A and D

upvoted 1 times

 **Wpcorgan** 1 year ago

A and D

upvoted 1 times

 **BENICE** 1 year ago

A and D are the options

upvoted 1 times

 **Danny23132412141_2312** 1 year ago

AD for sure

Link: <https://www.examtopics.com/discussions/amazon/view/43729-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

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 6 months, 1 week ago

For Exam :
Whenever you see SFTP , FTP look for "Transfer" in options available
upvoted 26 times

 **Chirantan** Highly Voted 11 months, 1 week 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 12 times

 **oguzbeliren** 3 months, 4 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

 **TariqKipkemei** Most Recent 2 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** 3 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 1 times

 **oguzbeliren** 3 months, 4 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** 4 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 2 times

 **cookieMr** 5 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** 5 months ago

A is correct

upvoted 1 times

 **markw92** 5 months, 2 weeks 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 2 times

 **studynoplay** 6 months, 2 weeks ago

Selected Answer: A

minimizes operational overhead = Serverless

AWS Transfer Family is serverless

upvoted 1 times

 **Rahulbit34** 6 months, 4 weeks ago

AWS Transfer Family is compatible for SFTP<FTPS<FTP. A is the answer

upvoted 1 times

 **kruasan** 7 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** 7 months, 2 weeks ago

Selected Answer: A

A - is the correct answer.

upvoted 2 times

 **BENICE** 11 months, 2 weeks ago

A -- is the option

upvoted 3 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 3 times

 **mj98** 12 months ago

Selected Answer: A

AWS Transfer Family - SFTP

upvoted 2 times

 **Bobbybash** 1 year ago

Selected Answer: A

AAAAAAA

AWS Transfer for SFTP, a fully-managed, highly-available SFTP service. You simply create a server, set up user accounts, and associate the server

with one or more Amazon Simple Storage Service (Amazon S3) buckets
upvoted 2 times

 **Bobbybash** 1 year ago

AAAAAAA

AWS Transfer for SFTP, a fully-managed, highly-available SFTP service. You simply create a server, set up user accounts, and associate the server with one or more Amazon Simple Storage Service (Amazon S3) buckets.

upvoted 1 times

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

BD (73%)

BC (26%)

 [Removed] Highly Voted 1 year 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 19 times

 vadiminski_a 11 months, 2 weeks 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 7 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 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 6 times

 Ruffyit Most Recent 2 weeks, 5 days 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 3 weeks, 6 days 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** 1 month, 2 weeks 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 1 times

✉ **Tom123456ac** 1 month, 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 2 times

✉ **paniya93** 1 month, 3 weeks ago

Selected Answer: BC

C is more cost-effective than AWS KMS

upvoted 1 times

✉ **TariqKipkemei** 2 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 4 times

✉ **Guru4Cloud** 2 months, 2 weeks ago

B) Use S3 Object Lock compliance mode to prevent objects from being overwritten or deleted for 5 years.

D) Use AWS KMS customer managed keys for encryption, and configure automatic annual rotation.

Compliance mode provides the protection against overwriting/deletion needed for the full contract duration. And KMS customer managed keys allow automated key rotation each year.

upvoted 2 times

✉ **animefan1** 4 months, 3 weeks ago

Selected Answer: BD

compliance meets company's requirement and with Customer managed keys, user can set auto rotation

upvoted 1 times

✉ **cookieMr** 5 months ago

Selected Answer: BD

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 5 times

✉ **ruqui** 6 months, 1 week ago

Selected Answer: BD

Answer is BD. C is discarded because key rotation can't be configured by the customer

upvoted 1 times

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

Selected Answer: BD

With SSE-S3 you can NOT Configure key rotation (see the choice C last sentence)

With KMS you can configure key rotation

upvoted 2 times

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

also, SSE-S3 is default and free. The question is not about cost, it is about operational maintenance

upvoted 1 times

✉ **cheese929** 6 months, 3 weeks ago

Selected Answer: BD

My answer is B and D.

I choose D over C cos of the annual key rotation requirement.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: BD

Consider using the default aws/s3 KMS key if:

You're uploading or accessing S3 objects using AWS Identity and Access Management (IAM) principals that are in the same AWS account as the AWS KMS key.

You don't want to manage policies for the KMS key.

Consider using a customer managed key if:

You want to create, rotate, disable, or define access controls for the key.

You want to grant cross-account access to your S3 objects. You can configure the policy of a customer managed key to allow access from another account.

<https://repost.aws/knowledge-center/s3-object-encryption-keys>

upvoted 1 times

 **Ankit_EC_ran** 7 months ago

Selected Answer: BD

BD

"You cannot enable or disable key rotation for AWS owned keys. The key rotation strategy for an AWS owned key is determined by the AWS service that creates and manages the key."

This eliminates option c which says configure key rotation

upvoted 3 times

 **chibaniMed** 7 months ago

Selected Answer: BC

i choose C instead of D because this part of question "LEAST operational overhead"

AWS KMS automatically rotates AWS managed keys every year (approximately 365 days). You cannot enable or disable key rotation for AWS managed keys

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

upvoted 1 times

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

B (90%) 10%

 **Shasha1** Highly Voted 11 months, 3 weeks 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 8 times

 **oguzbeliren** 3 months, 4 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 2 times

 **cookieMr** Highly Voted 5 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 7 times

 **Po_chih** Most Recent 1 month, 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** 1 month, 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** 2 months, 2 weeks ago

Selected Answer: B

AWS Elastic Beanstalk URL swapping is the main ask of this question.

upvoted 2 times

 **Guru4Cloud** 3 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 2 times

 **oguzbeliren** 3 months, 4 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** 6 months ago

S3 is for hosting static websites not dynamic websites or applications
Beanstalk will take care of this.

upvoted 1 times

 **kruasan** 7 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** 7 months, 3 weeks ago

who needs discussion in the era the of chatGPT

upvoted 2 times

 **aadityarav18** 4 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** 9 months, 2 weeks ago

Option B as it has the minimum operational overhead

upvoted 1 times

 **maciekmaciek** 9 months, 2 weeks ago

Selected Answer: B

Blue/Green deployments <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 1 times

 **naxer82** 9 months, 3 weeks ago

Selected Answer: B

is correct

upvoted 1 times

 **gustavtd** 11 months ago

As I was told, Elastic Beanstalk is an expensive service, isn't it?

upvoted 2 times

 **HayLLIHuK** 10 months, 4 weeks ago

so what? The question doesn't require the most cost-effective solution

upvoted 8 times

 **techhb** 11 months, 1 week ago

Selected Answer: B

D includes additional overhead of installing.

upvoted 2 times

 **BENICE** 11 months, 2 weeks ago

B -- is correct answer

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Option B as it has the minimum operational overhead

upvoted 1 times

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** Highly Voted 11 months, 2 weeks ago

A is correct answer. This was in my exam
upvoted 20 times

 **Grace83** 8 months, 2 weeks ago

Did these questions help with your exam?
upvoted 3 times

 **Ruffyt** Most Recent 2 weeks, 5 days 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 1 times

 **David_Ang** 1 month ago

Selected Answer: A
"A" is correct because it does not cause problems in the primary DB
upvoted 1 times

 **TariqKipkemei** 2 months, 2 weeks ago

Selected Answer: A
reports = read replica
upvoted 2 times

 **Guru4Cloud** 3 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** 4 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 2 times

✉ **sickcow** 4 months, 4 weeks ago

Selected Answer: A

A sounds right

upvoted 1 times

✉ **rauldevilla** 5 months ago

Selected Answer: A

Using the primary instance continues with the problem

upvoted 1 times

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

Selected Answer: A

correct

upvoted 1 times

✉ **cheese929** 6 months, 3 weeks ago

Selected Answer: A

A is correct.

upvoted 1 times

✉ **kruasan** 7 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

✉ **jlin526** 7 months, 2 weeks ago

Please DM contributor access: yi.liiii520@gmail.com

upvoted 2 times

✉ **ammyboy** 7 months ago

bro i need contibutor access please

upvoted 1 times

✉ **Hung23** 7 months, 2 weeks ago

Selected Answer: A

Answer: A

upvoted 1 times

✉ **k33** 8 months, 1 week ago

Selected Answer: A

Answer : A

upvoted 1 times

✉ **PUCKER** 8 months, 1 week ago

Selected Answer: A

SUMMA SUMMA KICK ERUDHAE ! ULUKULAE NALA BHODHA ERUDHAE !

upvoted 1 times

 **idriskameni** 8 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

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 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 9 times

 **Ruffyit** Most Recent 2 weeks, 5 days 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** 1 month ago

Selected Answer: BE

another mistake from the admin, should correct this one, because we all agree

upvoted 2 times

 **vijaykamal** 2 months 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** 2 months, 2 weeks 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** 3 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 3 times

 **james2033** 4 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** 4 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** 4 months, 4 weeks ago

Selected Answer: BE

Texttract to extract the content and Athena to run sql queries on S3 data

upvoted 1 times

 **sickcow** 4 months, 4 weeks ago

Selected Answer: BE

From a DE/ML perspective Lambda + Texttract + S3 + Athena is the best way to go

upvoted 1 times

 **rauldevilla** 5 months ago

Selected Answer: BE

Transcribe is used. Transcribe is used for Speech to Text

upvoted 1 times

 **cookieMr** 5 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 Texttract 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** 5 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** 6 months, 1 week ago

Selected Answer: BE

Options B & E are correct answers.

upvoted 1 times

 **antropaws** 6 months, 2 weeks ago

Selected Answer: BE

Why CD are marked as correct??

upvoted 1 times

 **studynoplay** 6 months, 2 weeks ago

Selected Answer: BE

operational efficiency = Serverless

S3 is serverless

upvoted 1 times

 **k33** 8 months, 1 week ago

Selected Answer: BE

Answer : BE

upvoted 1 times

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

B (51%) A (49%)

✉  **leonnnn** Highly Voted 1 year ago

Selected Answer: B

Use ElastiCache to reduce reading and choose redis to ensure high availability.

upvoted 32 times

✉  **JoeGuan** 3 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 1 times

✉  **Lalo** 9 months, 1 week ago

Where is the high availability when the database fails and the cache time runs out?

The answer is a.

upvoted 17 times

✉  **ruqui** 6 months, 1 week ago

A can't be an answer because the requirement is "reduce the number of database reads"

upvoted 6 times

✉  **Mia2009687** 5 months ago

They run multiple databases

upvoted 1 times

✉  **mandragon** 6 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 1 times

✉  **channn** Highly Voted 7 months, 3 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 16 times

✉  **Marco_St** Most Recent 3 days, 11 hours ago

Selected Answer: A

ElasticCache is useful when the usecase has frequent accessing data. But this is not for sure. So read replica is more reasonable for reducing read to the primary database. So I picked A

upvoted 1 times

✉  **xdkonorek2** 2 weeks, 3 days ago

Selected Answer: A

B would be correct if data could be cacheable, not every data is and we don't have this information

A is the answer

upvoted 1 times

✉ **David_Ang** 1 month ago

Selected Answer: A

they are literally asking for reducing reading, not anything else, so is "A".

upvoted 1 times

✉ **tom_cruise** 1 month, 2 weeks ago

Selected Answer: B

Redis provides HA through replica, memcached does not.

upvoted 1 times

✉ **prabhjot** 1 month, 3 weeks ago

Option a - the ans and not Option B (as Option B (Using Amazon ElastiCache for Redis) is primarily used for caching data in memory, which can help reduce read operations on the database, but it doesn't provide high availability or replication of the database itself.)

upvoted 1 times

✉ **Ramdi1** 1 month, 3 weeks ago

Selected Answer: B

B - They want to reduce reads so no need for read replica. Redis ensure high Avail.

upvoted 1 times

✉ **mani37k** 2 months ago

Selected Answer: A

A. Add Amazon RDS read replicas.

Adding Amazon RDS read replicas is a commonly used strategy to offload read traffic from the primary database, thereby reducing the number of database reads. Read replicas provide high availability and can distribute read queries across multiple instances, improving overall read performance.

While options B and D suggest using Amazon ElastiCache for Redis or Memcached, these caching solutions are more focused on improving read performance by caching frequently accessed data, but they do not inherently reduce the number of reads on the RDS database. They can complement the solution by serving cached data, but they are not a direct way to reduce the reads on the database.

upvoted 3 times

✉ **Modulopi** 2 months ago

A for Availability

upvoted 1 times

✉ **axelrodb** 2 months, 1 week ago

Selected Answer: B

B is the correct answer since the requirement is to reduce the read which can be achieved with ElastiCache. Adding RDS read replica is only going to distribute the read requests.

With ElastiCache, read hit will occur thus achieving the goal mentioned.

upvoted 1 times

✉ **gouranga45** 2 months, 2 weeks ago

Selected Answer: A

A satisfies the given requirements

upvoted 1 times

✉ **TariqKipkemei** 2 months, 2 weeks ago

Selected Answer: A

RDS read replicas was designed specifically to handle this kind of scenario.

upvoted 1 times

✉ **kambarami** 2 months, 2 weeks ago

Answer is B

Use elastic cache to reduce the numbers of reads

upvoted 1 times

✉ **Valder21** 2 months, 3 weeks ago

Selected Answer: A

if it could be B, why not D?

upvoted 2 times

✉ **ssa03** 2 months, 4 weeks ago

Selected Answer: B

reduce reading

upvoted 1 times

✉ **skaikobad** 3 months ago

Selected Answer: B

I think B is correct.

Because it Reduce Read operation also provide High Availability

upvoted 1 times

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

A (51%)

C (49%)

✉  **Gil80**  11 months, 4 weeks 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 26 times

✉  **AAAWrekng** 1 month 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

✉  **berks** 11 months, 1 week ago

what number of class ?

upvoted 4 times

✉  **Gil80**  12 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 20 times

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

Design for region failure? may as well design for AWS failure and put replica in GCP and Azure :v
upvoted 7 times

✉  **Kp88** 4 months ago

And on-prem in multiple DCs and one in mars too :D
upvoted 7 times

✉  **cyber_bedouin** 1 month, 3 weeks ago

yep lol, even in the other questions, for HA you can use Multi-AZ
upvoted 1 times

✉  **Steve_4542636** 9 months ago

The question doesn't ask which option is the most HA. It asks what meets the requirements.
upvoted 3 times

✉  **javitech83** 11 months, 3 weeks ago

but for C you need communication between the two VPC, which increase the complexity. With a should be enough for HA
upvoted 4 times

 **xdkonorek2** Most Recent 2 weeks, 3 days ago

Selected Answer: C

since we're using EC2 and manually setting everything, what do "create cluster" mean in answer A?
you can set replication between 2 databases set up in 2 servers without any cluster, just open ports and set up replication
also spreading ec2 between regions is higher availability

upvoted 1 times

 **liux99** 3 weeks, 1 day ago

Both A and C provide HA and failover. There is a slight difference between multi-az and multi-region failover: multi-region replication is intended for DR and it is not natively supported. A is the answer.

upvoted 1 times

 **nncppp** 3 weeks, 5 days ago

Selected Answer: A

high available and cluster are key words. So answer is A

upvoted 1 times

 **Pankaj_007** 3 weeks, 6 days ago

The database must be highly available and must fail over automatically if a disruptive event occurs. --> In cluster setup failover happens automatically , so for me A is correct

upvoted 1 times

 **rlamberti** 1 month, 1 week ago

Selected Answer: A

Answer is A

Communication between regions may cause DB cluster disruption because of latency - remember that the question doesn't pointed the DB engine.
So, using two AZs will keep HA without the latency potential issue.

upvoted 2 times

 **tom_cruise** 1 month, 2 weeks ago

Selected Answer: C

DR should be in different regions.

upvoted 1 times

 **prabhjot** 1 month, 3 weeks ago

Option A is correct - and why not Option B (as Automatic fail over will be miss)

upvoted 1 times

 **prabhjot** 1 month, 3 weeks ago

nd why not Option C(as Automatic fail over will be miss)

upvoted 1 times

 **hieulam** 2 months, 1 week ago

Selected Answer: C

if a disruptive event occurs ==> Assuming that occurs in the region, not in the availability zone only, thus, C is correct.

upvoted 2 times

 **TariqKipkemei** 2 months, 2 weeks ago

Selected Answer: A

Technically, both option A and C provide HA. But I would go with A because its less complex and less costly on replication costs.

upvoted 2 times

 **kanha1996** 2 months, 3 weeks ago

A is the anser

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: 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.

The key reasons are:

Cross-region redundancy provides the highest level of availability and disaster recovery. If one entire region goes down, the database can fail over across regions.

Database replication ensures data is consistent between regions at all times.

Manual failover gives the flexibility to fail over on-demand in case of regional issues.

upvoted 3 times

 **n43u435b543ht2b** 3 months, 3 weeks ago

Selected Answer: C

A "critical application" should be protected against a regional outage. This sounds like overkill but is absolutely commonplace and used frequently for truly critical applications.

upvoted 4 times

✉️  **james2033** 4 months, 1 week ago

Selected Answer: C

Question keyword "disruptive event", "highly available", "failover automatically".

"Different Region" is least condition for against "disruptive event", not "different Availability Zone".

Typo in the question: "failover automatically", not "fail over automatically".

upvoted 3 times

✉️  **vini15** 4 months, 2 weeks ago

Should be C

Cluster share same rack(hardware) in EC2 and its a logical grouping of instances within a single Availability Zone. Hence does not provide HA.

upvoted 3 times

✉️  **sosda** 4 months, 2 weeks ago

Selected Answer: C

Cluster = single AZ = not HA

upvoted 1 times

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 (94%) 3%

 **Guru4Cloud** Highly Voted 3 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 7 times

 **pavospam** Most Recent 1 day, 22 hours ago

Selected Answer: C

it's C... 4 answers wrong I have found

upvoted 1 times

 **Ruffyit** 2 weeks, 4 days 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** 1 month 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** 2 months 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** 2 months, 2 weeks 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** 3 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** 5 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 queuing 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 queuing 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 2 times

 **pisica134** 5 months, 1 week ago

D is so unnecessary this confuses people

upvoted 1 times

 **cookieMr** 5 months ago

Thx Allmighty for voting system! Answers provided by the site (and not by community) are 20% wrong.

upvoted 4 times

 **markw92** 5 months, 2 weeks 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

 **gx2222** 7 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** 8 months, 1 week ago

Selected Answer: C

Answer : C

upvoted 1 times

 **nickolaj** 9 months, 2 weeks 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** 9 months, 2 weeks 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** 9 months, 2 weeks 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** 10 months, 2 weeks 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** 11 months, 1 week ago

Selected Answer: D

I choose D

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Selected Answer: C

To meet the requirements of the company, a solution should be implemented that can automatically process orders if a system outage occurs. Option C meets these requirements by using an Auto Scaling group and Amazon Simple Queue Service (SQS) to ensure that orders can be processed even if a system outage occurs.

In this solution, the EC2 instances are placed in an Auto Scaling group, which ensures that the number of instances can be automatically scaled up or down based on demand. The ordering system is configured to send messages to an SQS queue, which acts as a buffer and stores the messages until they can be processed by the EC2 instances. The EC2 instances are configured to consume messages from the queue and process them. If a system outage occurs, the messages in the queue will remain available and can be processed once the system is restored.

upvoted 2 times

 **techhb** 11 months, 1 week ago

Selected Answer: A

c is right

upvoted 1 times

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

D (92%)	8%
---------	----

 **Gil80** Highly Voted 12 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 28 times

 **TariqKipkemei** Most Recent 2 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 1 times

 **Guru4Cloud** 3 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** 5 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** 5 months, 1 week ago

D: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

upvoted 1 times

✉ **Abrar2022** 6 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** 6 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** 6 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** 6 months, 3 weeks ago

Selected Answer: D

Use DynamoDB TTL feature to achieve this..

upvoted 1 times

✉ **jdr75** 7 months, 3 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 eachtime 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** 10 months, 2 weeks 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** 10 months, 3 weeks 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** 11 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** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 1 week ago

Selected Answer: D

TTL does the trick
upvoted 1 times

👤 **kvenikoduru** 11 months, 1 week 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. - check this link <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

upvoted 1 times

👤 **prethesh** 11 months, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/about-aws/whats-new/2017/02/amazon-dynamodb-now-supports-automatic-item-expiration-with-time-to-live-ttl/>

upvoted 1 times

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 (97%)

 **DavidNamy** Highly Voted 10 months, 3 weeks 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 10 times

 **vijaykamal** Most Recent 2 months ago

Selected Answer: BE

DynamoDB is NoSQL - E it out
Replatform requires considerable overhead - C is out
Lambda function is for running code for short duration - A is out
Answer - BE
upvoted 2 times

 **TariqKipkemei** 2 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** 3 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** 5 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** 5 months, 2 weeks 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** 6 months, 1 week ago

Selected Answer: BE

B + E are the answers that fulfil the requirements.

upvoted 1 times

✉ **cheese929** 6 months, 3 weeks ago

Selected Answer: BE

B and E

upvoted 1 times

✉ **Nikhilcy** 7 months ago

why not C?

upvoted 2 times

✉ **AlankarJ** 5 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** 8 months, 1 week ago

Selected Answer: BE

Answer : BE

upvoted 1 times

✉ **waiyiu9981** 11 months ago

Why A is wrong?

upvoted 1 times

✉ **gustavtd** 11 months ago

Because that needs some development,

upvoted 2 times

✉ **Buruguduystunstugudunstuy** 11 months, 1 week 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 3 times

✉ **techhb** 11 months, 1 week ago

Selected Answer: BE

B&E Option ,because D is for No-Sql

upvoted 1 times

✉ **JayBee65** 10 months, 3 weeks ago

And requires additional development effort

upvoted 1 times

✉ **career360guru** 11 months, 2 weeks ago

B&E Option

upvoted 1 times

✉ **dcyberguy** 12 months ago

B- According to the AWS documentation, the simplest way to migrate .NET applications to AWS is to repack the applications using either AWS Elastic Beanstalk or Amazon EC2.

E - RDS with Oracle is a no-brainer

upvoted 3 times

 **[Removed]** 12 months ago

same as everyone else

upvoted 3 times

 **KADSM** 1 year ago

B E should be correct. Question says "Minimize development changes" - so should go for same oracle DB

upvoted 1 times

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**  11 months, 3 weeks ago

Selected Answer: D

If you see MongoDB, just go ahead and look for the answer that says DocumentDB.
upvoted 18 times

✉  **Guru4Cloud**  3 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 3 times

✉  **james2033** 4 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** 5 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** 6 months, 1 week ago

Selected Answer: D

The solution meets these requirements is option D.

upvoted 1 times

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

Selected Answer: D

minimizes operational overhead = Serverless (Fargate)
MongoDB = DocumentDB

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 2 times

✉ **dcyberguy** 12 months ago

DDDDDDDD

upvoted 1 times

✉ **Gabs90** 1 year 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 ago

Selected Answer: D

D meets the requirements

upvoted 1 times

✉ **Nigma** 1 year 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

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

B (89%) 7%

 **Buruguduystunstugudunstuy**  11 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.

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 15 times

 **TheAbsoluteTruth** 8 months ago

What bothers me is the 7 years of storage.

upvoted 4 times

 **enzomv** 10 months, 1 week 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 1 times

 **enzomv** 10 months, 1 week ago

Disregard. I meant B

upvoted 1 times

 **enzomv** 10 months, 1 week 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** 10 months, 1 week ago

Disregard. I meant Amazon Transcribe

upvoted 1 times

 **youdelin**  1 month, 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 1 times

👤 **paniya93** 1 month, 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** 2 months 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** 2 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** 3 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 1 times

👤 **Thornessen** 4 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 1 times

👤 **sickcow** 4 months, 4 weeks ago

Selected Answer: C

Transcribe and (s3) + Athena is the way to go here.

Redshift sounds like an overkill

upvoted 2 times

👤 **cookieMr** 5 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** 6 months, 1 week ago

Selected Answer: B

the solution that meets these requirements is option B.

upvoted 1 times

👤 **cheese929** 6 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

👤 **Rahulbit34** 6 months, 4 weeks ago

Amazon Transcribe is a service that convert speech into text, so B is the answer

upvoted 1 times

✉  **k33** 8 months, 1 week ago

Selected Answer: B

Answer : B

upvoted 2 times

✉  **enzomv** 10 months, 1 week ago

Selected Answer: C

<https://docs.aws.amazon.com/transcribe/latest/dg/what-is.html>

upvoted 1 times

✉  **master1004** 10 months, 3 weeks ago

The correct answer is C.

Wouldn't it be the right answer to save and analyze using Amazon Redshift, which can be used to analyze big data on data warehousing?

upvoted 2 times

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

B

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

Amazon Transcribe

Automatically convert speech to text

upvoted 1 times

✉  **techhb** 11 months, 1 week ago

Selected Answer: B

Only B

[ashttps://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-associate-saa-c03/view/7/#](https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-associate-saa-c03/view/7/#)

Rekognition - Image and Video Analysis

Transcribe - Text to speech

Translate - Translate a text-based file from a language to another language

upvoted 3 times

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 11 months, 1 week 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 6 times

 **Tom123456ac** Most Recent 1 month, 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 1 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: D

use Amazon Cognito to authorize user requests.
upvoted 1 times

 **Guru4Cloud** 2 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 1 times

 **Guru4Cloud** 3 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** 5 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** 6 months, 1 week ago

Selected Answer: D

solution will meet these requirements with the LEAST operational overhead is option D.

upvoted 1 times

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

Selected Answer: D

LEAST operational overhead = Serverless = Cognito user pool

upvoted 1 times

✉ **cheese929** 6 months, 3 weeks ago

Selected Answer: D

D is correct.

upvoted 1 times

✉ **k33** 8 months, 1 week ago

Selected Answer: D

Answer : D

upvoted 1 times

✉ **Hello4me** 8 months, 1 week ago

D is correct

upvoted 1 times

✉ **Mahadeva** 10 months, 3 weeks 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.

Please refer to this blog: <https://aws.amazon.com/blogs/security/building-fine-grained-authorization-using-amazon-cognito-api-gateway-and-iam/>
upvoted 1 times

✉ **JayBee65** 10 months, 3 weeks 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>

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

✉ **TungPham** 8 months, 3 weeks 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

✉ **Mahadeva** 10 months, 3 weeks ago

Option D: there is nothing called Cognito user pool authorizer. We only have custom Authorizer function through Lambda.

upvoted 1 times

✉ **JayBee65** 10 months, 3 weeks ago

Oh yes there is :)

upvoted 2 times

✉ **k1kavi1** 11 months, 1 week ago

Selected Answer: D

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html>
upvoted 4 times

 **MutiverseAgent** 4 months, 1 week ago

up this

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D - As company already has all the users authentication information in Cognito
upvoted 1 times

 **k1kavi1** 11 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

 **mj98** 12 months ago

API + Cognito integration - Answer D

upvoted 2 times

 **Nigma** 1 year ago

Selected Answer: D

Answer : D

Check Gabs90 link

Use the Amazon Cognito console, CLI/SDK, or API to create a user pool—or use one that's owned by another AWS account

upvoted 1 times