

A company is developing a marketing communications service that targets mobile app users. The company needs to send confirmation messages with Short Message Service (SMS) to its users. The users must be able to reply to the SMS messages. The company must store the responses for a year for analysis.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon Connect contact flow to send the SMS messages. Use AWS Lambda to process the responses.
- B. Build an Amazon Pinpoint journey. Configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving.
- C. Use Amazon Simple Queue Service (Amazon SQS) to distribute the SMS messages. Use AWS Lambda to process the responses.
- D. Create an Amazon Simple Notification Service (Amazon SNS) FIFO topic. Subscribe an Amazon Kinesis data stream to the SNS topic for analysis and archiving.

Correct Answer: A

Community vote distribution

B (83%)

Other

 **whoob** 2 months ago

base function of AWS Pinpoint

upvoted 1 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: B

Marketing communications = Amazon Pinpoint

upvoted 2 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: B

B. AWS Pinpoint is for Marketing communications.

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: B

By using Pinpoint, the company can effectively send SMS messages to its mobile app users. Additionally, Pinpoint allows the configuration of journeys, which enable the tracking and management of user interactions. The events generated during the journey, including user responses to SMS, can be captured and sent to an Kinesis data stream. This data stream can then be used for analysis and archiving purposes.

A. Creating an Amazon Connect contact flow is primarily focused on customer support and engagement, and it lacks the capability to store and process SMS responses for analysis.

C. Using SQS is a message queuing service and is not specifically designed for handling SMS responses or capturing them for analysis.

D. Creating an SNS FIFO topic and subscribing a Kinesis data stream is not the most appropriate solution for capturing and storing SMS responses, as SNS is primarily used for message publishing and distribution.

In summary, option B is the best choice as it leverages Pinpoint to send SMS messages and captures user responses for analysis and archiving using an Kinesis data stream.

upvoted 4 times

 **Bmarodi** 5 months, 2 weeks ago

Selected Answer: B

Option B is correct answer: link: <https://aws.amazon.com/pinpoint/>, and video under the link.

upvoted 2 times

 **studynoplay** 6 months, 2 weeks ago

Selected Answer: B

Two-Way Messaging

Receive SMS messages from your customers and reply back to them in a chat-like interactive experience. With Amazon Pinpoint, you can create automatic responses when customers send you messages that contain certain keywords.

upvoted 1 times

 **CLOUDUMASTER** 7 months ago

Based on my research Kinesis stream is real time data ingestion, and also stores only event data and not the actual people responses, furthermore there is no requirement to have real time data streaming. That is probably why I am hesitating agree here with everyone on B and rather choose A.

upvoted 1 times

 **jayce5** 7 months ago

Selected Answer: B
The answer is B. AWS Pinpoint is for Marketing communications.
AWS Connect is for Contact center.

upvoted 1 times

 **jaswantn** 7 months ago

Selected Answer: A
According to the following link I would choose Option A.
<https://docs.aws.amazon.com/connect/latest/adminguide/web-and-mobile-chat.html>

upvoted 1 times

 **smartegnine** 5 months, 3 weeks ago

no no, there is no SMS, note the question stated all activities through SMS, also Amazon connect flow most likely working on web application UI, but if you see question clearly, this is receiving and sending SMS not through application UI (Web/Mobile App). So for those reason we choose B

upvoted 1 times

 **ProfXsamson** 10 months ago

Selected Answer: B
Amazon Pinpoint is a flexible, scalable and fully managed push notification and SMS service for mobile apps.

upvoted 3 times

 **Foucault** 10 months, 1 week ago

It's B, see following link <https://docs.aws.amazon.com/pinpoint/latest/developerguide/event-streams.html>

upvoted 2 times

 **LuckyAro** 10 months, 2 weeks ago

Selected Answer: B
<https://aws.amazon.com/pinpoint/product-details/sms/>
Two-Way Messaging:
Receive SMS messages from your customers and reply back to them in a chat-like interactive experience. With Amazon Pinpoint, you can create automatic responses when customers send you messages that contain certain keywords. You can even use Amazon Lex to create conversational bots.
A majority of mobile phone users read incoming SMS messages almost immediately after receiving them. If you need to be able to provide your customers with urgent or important information, SMS messaging may be the right solution for you.

You can use Amazon Pinpoint to create targeted groups of customers, and then send them campaign-based messages. You can also use Amazon Pinpoint to send direct messages, such as appointment confirmations, order updates, and one-time passwords.

upvoted 2 times

 **DavidNamy** 10 months, 3 weeks ago

Selected Answer: D
D:
Amazon Simple Notification Service (SNS) is a fully managed messaging service that enables you to send and receive SMS messages in a cost-effective and highly scalable way. By creating an SNS FIFO topic, you can ensure that the SMS messages are delivered to your users in the order they were sent and that the SMS responses are processed and stored in the same order. You can also configure your SNS FIFO topic to publish SMS responses to an Amazon Kinesis data stream, which will allow you to store and analyze the responses for a year.

Amazon Pinpoint ?;?;? NO!

is not correct solution because while Amazon Pinpoint allows you to send SMS and Email campaigns, as well as handle push notifications to a user base, it doesn't provide SMS sending feature by itself. Furthermore, it's a service mainly focused on sending and tracking marketing campaigns, not for managing two-way SMS communication and the reception of reply.

upvoted 3 times

 **Omok** 9 months, 4 weeks ago

What do think about <https://docs.aws.amazon.com/pinpoint/latest/userguide/channels-sms-two-way.html>?
upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Selected Answer: B
To send SMS messages and store the responses for a year for analysis, the company can use Amazon Pinpoint. Amazon Pinpoint is a fully-managed service that allows you to send targeted and personalized SMS messages to your users and track the results.

To meet the requirements of the company, a solutions architect can build an Amazon Pinpoint journey and configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving. The Kinesis data stream can be configured to store the data for a year, allowing the company to analyze the responses over time.

So, Option B is the correct answer.

Option B. Build an Amazon Pinpoint journey. Configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving.

upvoted 3 times

 **techhb** 11 months, 1 week ago

Selected Answer: B

We need to analyze and archiving A doesnt help with it.

upvoted 1 times

 **BENICE** 11 months, 2 weeks ago

B is correct answer

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: B

Answer B, This is Pinpoint usecase

upvoted 1 times

A company is planning to move its data to an Amazon S3 bucket. The data must be encrypted when it is stored in the S3 bucket. Additionally, the encryption key must be automatically rotated every year.

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

- A. Move the data to the S3 bucket. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.
- B. Create an AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket.
- C. Create an AWS Key Management Service (AWS KMS) customer managed key. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket. Manually rotate the KMS key every year.
- D. Encrypt the data with customer key material before moving the data to the S3 bucket. Create an AWS Key Management Service (AWS KMS) key without key material. Import the customer key material into the KMS key. Enable automatic key rotation.

Correct Answer: B

Community vote distribution

B (58%) A (41%)

 **Buruguduystunstugudunstuy**  11 months, 1 week ago

Selected Answer: A

KEYWORD: LEAST operational overhead

To encrypt the data when it is stored in the S3 bucket and automatically rotate the encryption key every year with the least operational overhead, the company can use server-side encryption with Amazon S3-managed encryption keys (SSE-S3). SSE-S3 uses keys that are managed by Amazon S3, and the built-in key rotation behavior of SSE-S3 encryption keys automatically rotates the keys every year.

To meet the requirements of the company, the solutions architect can move the data to the S3 bucket and enable server-side encryption with SSE-S3. This solution requires no additional configuration or maintenance and has the least operational overhead.

Hence, the correct answer is;

Option A. Move the data to the S3 bucket. Use server-side encryption with Amazon S3-managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.

upvoted 27 times

 **bicrasse** 1 week, 6 days ago

The good answer was B before May 2022, because the rotation schedule for AWS managed keys was 3 years (SSE-S3 is based on it)...

From May 2022 the schedule rotation is 1 year, then A is now the best answer because there is NO operational task to do: S3 is by default encrypted at rest with SSE-S3 (rotation every year)... So it depends if the question has been updated since 2022

upvoted 2 times

 **LuckyAro** 10 months ago

The order of these events is being ignored here in my opinion. The encryption checkbox needs to be checked before data is moved into the S3 bucket or it will not be encrypted otherwise, you'll have to encrypt manually and reload into S3 bucket. If the box was checked before moving data into S3 then you are good to go!

upvoted 5 times

 **Smart** 3 months, 4 weeks ago

Ignoring the new changes that the default encryption is already enabled. I agree that the encryption should be configured before moving the data into the bucket. Otherwise, the existing objects will remain unencrypted.

Correct Answer is B.

Additionally, where is the reference that SSE-S3 will rotate keys every year (which is the question's requirement).

upvoted 1 times

 **LuckyAro** 10 months ago

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Option B involves using a customer-managed AWS KMS key and enabling automatic key rotation, but this requires the company to manage the KMS key and monitor the key rotation process.

Option C involves using a customer-managed AWS KMS key, but this requires the company to manually rotate the key every year, which introduces additional operational overhead.

Option D involves encrypting the data with customer key material and creating a KMS key without key material, but this requires the company to manage the customer key material and import it into the KMS key, which introduces additional operational overhead.

upvoted 2 times

✉ **JayBee65** 10 months, 3 weeks ago

But...

For A there is no reference to how often these keys are rotated, and to rotate to a new key, you need to upload it, which is operational overhead. So not only does it not necessarily meet the 'rotate keys every year' requirement, but every year it requires operational overhead.

More importantly, the question states move the objects first, and then configure encryption, but ... "There is no change to the encryption of the objects that existed in the bucket before default encryption was enabled." from <https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>

So A is clearly wrong.

For B, whilst you have to set up KMS once, you then don't have to anything else, which i would say is LEAST operational overhead.

upvoted 13 times

✉ **ocbn3wby** 10 months, 4 weeks ago

God bless you, man! The most articulated answers, easy to understand. Good job!

upvoted 3 times

✉ **JayBee65** 10 months, 3 weeks ago

But wrong :)

upvoted 4 times

✉ **ocbn3wby** 9 months, 3 weeks ago

Reviewed it the second time. Some of them are wrong, indeed.

upvoted 1 times

✉ **techhb** Highly Voted 11 months, 1 week ago

Selected Answer: B

SSE-S3 - is free and uses AWS owned CMKs (CMK = Customer Master Key). The encryption key is owned and managed by AWS, and is shared among many accounts. Its rotation is automatic with time that varies as shown in the table here. The time is not explicitly defined.

SSE-KMS - has two flavors:

AWS managed CMK. This is free CMK generated only for your account. You can only view its policies and audit usage, but not manage it. Rotation is automatic - once per 1095 days (3 years),

Customer managed CMK. This uses your own key that you create and can manage. Rotation is not enabled by default. But if you enable it, it will be automatically rotated every 1 year. This variant can also use an imported key material by you. If you create such key with an imported material, there is no automated rotation. Only manual rotation.

SSE-C - customer provided key. The encryption key is fully managed by you outside of AWS. AWS will not rotate it.

upvoted 26 times

✉ **ruqui** 6 months, 1 week ago

AWS managed CMK rotates every 365 days (not 1095 days). Reference:

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#key-mgmt>

upvoted 1 times

✉ **xdkonorek2** Most Recent 2 weeks, 3 days ago

Selected Answer: B

I'm voting B

Each object in s3 using SSE-S3 uses separate key, this key is encrypted using another master key that is regularly rotated but AWS doesn't share how often it happens.

With SSE-KMS you have option to tick: "Automatically rotate this KMS key every year".

upvoted 1 times

✉ **bogobob** 2 weeks, 5 days ago

In 2023 the answer would be A. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingServerSideEncryption.html> states that S3 automatically uses SSE, and rotates the keys "regularly" which as far as I've understood is yearly

upvoted 1 times

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

but based on this reference:

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

it mentions varies, so I would stick with B

upvoted 1 times

✉ **rlamberti** 1 month, 1 week ago

Selected Answer: A

SSE-S3 are rotated automatically every year. Default behaviour.

upvoted 1 times

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

Selected Answer: A

LEAST operational overhead = Amazon S3 managed encryption keys

upvoted 3 times

✉ **XCheng** 2 months, 1 week ago

Selected Answer: —

https://docs.aws.amazon.com/zh_cn/AmazonS3/latest/userguide/default-bucket-encryption.html

upvoted 1 times

✉ **roggerrubens** 2 months, 2 weeks ago

Resposta A , todo objeto que é colocado no S3 , e automaticamente criptografado por padrão SSE-S3 , não ???

upvoted 1 times

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

Selected Answer: B

B. Create an AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket.

upvoted 2 times

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

Answer is B.

SSE-S3 encryption will not apply to existing objects in S3 bucket.

Question is when it is stored in S3, data must be encrypted.

If you already stored and later enable SSE-S3, will not be a solution.

So A is not the correct answer.

upvoted 1 times

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

Selected Answer: A

Once you enable SSE-S3 encryption for your S3 bucket, Amazon automatically rotates the data encryption keys for your objects every 365 days. This means that your data encryption keys are automatically replaced with new ones every year. You can also manually rotate the encryption keys for your objects at any time.

<https://saturncloud.io/blog/how-does-amazon-sses3-key-rotation-work/#:~:text=Once%20you%20enable%20SSE%2DS3,your%20objects%20at%20any%20time.>

upvoted 1 times

✉ **Sutariya** 2 months, 3 weeks ago

B is right Answer : If you need more control over your keys, such as managing key rotation and access policy grants, you can choose to use server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS), or dual-layer server-side encryption with AWS KMS keys (DSSE-KMS). For more information about editing KMS keys

upvoted 1 times

✉ **Aelodus** 3 months, 2 weeks ago

Selected Answer: B

Went to AWS office for a cloud developer course, I asked the trainer what is SSE-S3's key rotation frequency, the trainer mentioned that the information for the rotation frequency is not publicly available. This was done intentionally. He also said that if we truly wanted to know, we had to hold a private consultation with them, as a representative of our company.

Going back to the question, since we cannot confirm the frequency of SSE-S3's key rotation the best answer for this question is B. It might have higher operational overhead compared to A, but it is the only one that fulfills the requirements.

upvoted 2 times

✉ **npraveen** 3 months, 3 weeks ago

Selected Answer: A

Once you enable SSE-S3 encryption for your S3 bucket, Amazon automatically rotates the data encryption keys for your objects every 365 days. This means that your data encryption keys are automatically replaced with new ones every year.

upvoted 2 times

✉ **oguzbeliren** 3 months, 3 weeks ago

Answer is A

With server side encryption S3 will automatically manages the necryption keys and their rotation. The questions is specifically asking least operational overhead.

Option B also provides a valid solution, but it involves more manual configuration and management of a customer-managed AWS Key Management Service (AWS KMS) key, including enabling and configuring automatic key rotation.

upvoted 1 times

✉ **cookieMr** 5 months ago

Selected Answer: B

- A. While using SSE-S3 the key rotation is handled automatically by AWS. AWS rotates the encryption keys at least once every 1095 days (3 years) on your behalf.
- B. By using a customer managed key in AWS KMS with automatic key rotation enabled, and setting the S3 bucket's default encryption behavior to use this key, the data stored in the S3 bucket will be encrypted and the encryption key will be automatically rotated every year.
- C. This answer is not the most optimal solution as it suggests manually rotating the KMS key every year, which introduces manual intervention and increases operational overhead.
- D. This answer is not the most suitable option as it involves encrypting the data with customer key material and managing the key rotation manually. It adds complexity and management overhead compared to using AWS KMS for key management and encryption.

upvoted 4 times

 **pisica134** 5 months, 1 week ago

chat gpt says it's B

upvoted 1 times

The customers of a finance company request appointments with financial advisors by sending text messages. A web application that runs on Amazon EC2 instances accepts the appointment requests. The text messages are published to an Amazon Simple Queue Service (Amazon SQS) queue through the web application. Another application that runs on EC2 instances then sends meeting invitations and meeting confirmation email messages to the customers. After successful scheduling, this application stores the meeting information in an Amazon DynamoDB database.

As the company expands, customers report that their meeting invitations are taking longer to arrive.

What should a solutions architect recommend to resolve this issue?

- A. Add a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database.
- B. Add an Amazon API Gateway API in front of the web application that accepts the appointment requests.
- C. Add an Amazon CloudFront distribution. Set the origin as the web application that accepts the appointment requests.
- D. Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

Correct Answer: D

Community vote distribution

D (100%)

 **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week ago

Selected Answer: D

Option D. Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

To resolve the issue of longer delivery times for meeting invitations, the solutions architect can recommend adding an Auto Scaling group for the application that sends meeting invitations and configuring the Auto Scaling group to scale based on the depth of the SQS queue. This will allow the application to scale up as the number of appointment requests increases, improving the performance and delivery times of the meeting invitations.

upvoted 8 times

 **cookieMr** Highly Voted 5 months ago

Selected Answer: D

By adding an ASG for the application that sends meeting invitations and configuring it to scale based on the depth of the SQS, the system can automatically adjust its capacity based on the number of pending messages in the queue. This ensures that the application can handle increased message load and process the meeting invitations more efficiently, reducing the delay experienced by customers.

- A. Adding a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database would improve read performance for DynamoDB, but it does not directly address the issue of delayed meeting invitations.
- B. Adding an API Gateway API in front of the web application that accepts the appointment requests may help with request handling and management, but it does not directly address the issue of delayed meeting invitations.
- C. Adding an CloudFront distribution with the web application as the origin would improve content delivery and caching, but it does not directly address the issue of delayed meeting invitations.

upvoted 5 times

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

Selected Answer: D

Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

upvoted 1 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: D

Option D is the right Answer,

upvoted 2 times

✉  **k1kavi1** 11 months, 2 weeks ago

Selected Answer: D

Agreed

upvoted 1 times

✉  **jambajuice** 1 year ago

Selected Answer: D

ANswer d

upvoted 1 times

✉  **leonnnn** 1 year ago

Selected Answer: D

D meets the requirements

upvoted 1 times

✉  **Nigma** 1 year ago

Selected Answer: D

Answer : D

upvoted 1 times

An online retail company has more than 50 million active customers and receives more than 25,000 orders each day. The company collects purchase data for customers and stores this data in Amazon S3. Additional customer data is stored in Amazon RDS.

The company wants to make all the data available to various teams so that the teams can perform analytics. The solution must provide the ability to manage fine-grained permissions for the data and must minimize operational overhead.

Which solution will meet these requirements?

- A. Migrate the purchase data to write directly to Amazon RDS. Use RDS access controls to limit access.
- B. Schedule an AWS Lambda function to periodically copy data from Amazon RDS to Amazon S3. Create an AWS Glue crawler. Use Amazon Athena to query the data. Use S3 policies to limit access.
- C. Create a data lake by using AWS Lake Formation. Create an AWS Glue JDBC connection to Amazon RDS. Register the S3 bucket in Lake Formation. Use Lake Formation access controls to limit access.
- D. Create an Amazon Redshift cluster. Schedule an AWS Lambda function to periodically copy data from Amazon S3 and Amazon RDS to Amazon Redshift. Use Amazon Redshift access controls to limit access.

Correct Answer: D

Community vote distribution

C (100%)

 **anhike** Highly Voted 11 months, 3 weeks ago

Answer : C keyword "manage-fine-grained"
<https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/>
upvoted 14 times

 **markw92** 5 months, 2 weeks ago

You can manage fine grained using redshift as well - <https://aws.amazon.com/blogs/big-data/achieve-fine-grained-data-security-with-row-level-access-control-in-amazon-redshift/>
But, I believe the keyword to look for is "minimize operational overhead", which lakeformation does without duplicating much of the data. Redshift is operational overhead and duplication of data. not sure why the answer is D. i vote C as well.
upvoted 3 times

 **Olaunfazed** 5 months ago

yeah, most of examtopics answers are wrong
upvoted 3 times

 **karloscetina007** Most Recent 2 months ago

Selected Answer: C

a fine grained permissons is one of the conditions to accomplish with the requirement.
With the use of AWS Glue you can get accomplish with this requirement.
My answer is: C
upvoted 1 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: C

With Lake formation you can scale permissions more easily with fine-grained security capabilities, including row- and cell-level permissions and tag-based access control.
upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: C

Lake Formation enables the creation of a secure and scalable data lake on AWS, allowing centralized access controls for both S3 and RDS data. By using Lake Formation, the company can manage permissions effectively and integrate RDS data through the AWS Glue JDBC connection. Registering the S3 in Lake Formation ensures unified access control. This solution reduces operational overhead while providing fine-grained permissions management.
upvoted 2 times

 **cookieMr** 5 months ago

Selected Answer: C

Lake Formation enables the creation of a secure and scalable data lake on AWS, allowing centralized access controls for both S3 and RDS data. By using Lake Formation, the company can manage permissions effectively and integrate RDS data through the AWS Glue JDBC connection. Registering the S3 in Lake Formation ensures unified access control. This solution reduces operational overhead while providing fine-grained

permissions management.

A. Directly writing purchase data to Amazon RDS with RDS access controls lacks comprehensive permissions management for both S3 and RDS data.

B. Periodically copying data from RDS to S3 using Lambda and using AWS Glue and Athena for querying does not offer fine-grained permissions management and introduces data synchronization complexities.

D. Creating an Redshift cluster and copying data from S3 and RDS to Redshift adds complexity and operational overhead without the flexibility of Lake Formation's permissions management capabilities.

upvoted 3 times

 **pisica134** 5 months, 1 week ago

Answer is C AWS Lake Formation provides a comprehensive solution for building and managing a data lake. It simplifies data ingestion, organization, and access control. By creating a data lake using AWS Lake Formation, you can centralize and govern access to your data across multiple sources.

upvoted 1 times

 **Bmarodi** 5 months, 2 weeks ago

Selected Answer: C

Option C is right answer: <https://docs.aws.amazon.com/lake-formation/latest/dg/what-is-lake-formation.html>

upvoted 1 times

 **Abrar2022** 6 months ago

Lake Formation helps you manage fine-grained access for internal and external customers from a centralized location and in a scalable way.

upvoted 1 times

 **doorahmie** 10 months ago

<https://docs.aws.amazon.com/lake-formation/latest/dg/access-control-overview.html>

upvoted 2 times

 **LuckyAro** 10 months, 2 weeks ago

Selected Answer: C

To me, the give-away was: "The company wants to make all the data available to various teams" - Data-Lake - All data in one place.

upvoted 4 times

 **master1004** 10 months, 3 weeks ago

The correct answer is D.

The company uses all the data from various teams so that the teams can do their analysis.

Therefore, it is the best way to separately configure redshift for data warehousing and for all employees to connect to the redshift DB and perform analysis tasks without burdening the operating DB (must minimize operational overhead).

upvoted 3 times

 **ruqui** 5 months, 3 weeks ago

I don't think that "periodically copy data from Amazon S3 and RDS to Redshift" minimize the operational overhead. The correct answer for me is C

upvoted 1 times

 **aba2s** 10 months, 4 weeks ago

Selected Answer: C

Manage fine-grained access control using AWS Lake Formation

<https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/>

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Selected Answer: C

Option C. Create a data lake by using AWS Lake Formation. Create an AWS Glue JDBC connection to Amazon RDS. Register the S3 bucket in Lake Formation. Use Lake Formation access controls to limit access.

To make all the data available to various teams and minimize operational overhead, the company can create a data lake by using AWS Lake Formation. This will allow the company to centralize all the data in one place and use fine-grained access controls to manage access to the data.

To meet the requirements of the company, the solutions architect can create a data lake by using AWS Lake Formation, create an AWS Glue JDBC connection to Amazon RDS, and register the S3 bucket in Lake Formation. The solutions architect can then use Lake Formation access controls to limit access to the data. This solution will provide the ability to manage fine-grained permissions for the data and minimize operational overhead.

upvoted 3 times

 **majdango** 6 months, 1 week ago

.....

upvoted 1 times

 **kvenikoduru** 11 months, 1 week ago

Selected Answer: C

a combination of the following 2 URLs I believe it is C

<https://aws.amazon.com/lake-formation/>

<https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/>

upvoted 1 times

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

Option C is the right answer. Fine-grained access-control from different types of data sources is a Lakeformation usecase.

upvoted 2 times

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

Selected Answer: C

CCCCCCCCCC

upvoted 2 times

✉ **9014** 12 months ago

Selected Answer: C

ANSWER IS OF COURSE C

upvoted 1 times

A company hosts a marketing website in an on-premises data center. The website consists of static documents and runs on a single server. An administrator updates the website content infrequently and uses an SFTP client to upload new documents.

The company decides to host its website on AWS and to use Amazon CloudFront. The company's solutions architect creates a CloudFront distribution. The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin.

Which solution will meet these requirements?

- A. Create a virtual server by using Amazon Lightsail. Configure the web server in the Lightsail instance. Upload website content by using an SFTP client.
- B. Create an AWS Auto Scaling group for Amazon EC2 instances. Use an Application Load Balancer. Upload website content by using an SFTP client.
- C. Create a private Amazon S3 bucket. Use an S3 bucket policy to allow access from a CloudFront origin access identity (OAI). Upload website content by using the AWS CLI.
- D. Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP. Configure the S3 bucket for website hosting. Upload website content by using the SFTP client.

Correct Answer: C

Community vote distribution

C (76%)

D (24%)

✉  **bjexamprep**  3 months, 3 weeks ago

Selected Answer: C

The question here is whether the solution architect can change the requirement. The requirement says very clear about SFTP which cannot be addressed by option C. But the question also gives very clear hint about OAI which cannot be addressed by option D. Option D also doesn't mention anything about CloudFront which is part of the requirement of the question.

So, if the requirement cannot be changed, D is the answer; if the requirement can be changed, C is the answer. But if the requirement can be changed, what's the limitation? That will be a Chaos.

I'm voting C, and curse the question designer.

upvoted 9 times

✉  **Iconique** 2 months ago

"The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin." The solution architect is looking for a solution that can fit with CloudFront as origin! So it doesn't matter that option D does not mention CF, CF is part of the solution!

Having a marketing website on-premise clearly indicates having S3 as static content.

AWS Transfer Family is the way to upload files via FTP to S3!

So the answer is D.

Why not C?

User is already uploading content via FTP, option C is eliminating this option for him and forces using the CLI. The solution from C does not meet the requirements of having FTP.

upvoted 3 times

✉  **rlamberti**  1 month, 1 week ago

Selected Answer: C

Transferring via AWS CLI is cheaper than via Transfer Family.

It is not the best option, but will do the job of uploading the data to S3.

upvoted 1 times

✉  **juanrasus2** 1 month, 1 week ago

I'd go with D. In C there is no mention to S3 bucket being configured for web hosting. Simply adding the Cloudfront distribution and pointing that to the S3 won't work out of the box.

upvoted 1 times

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

Selected Answer: D

D - SFTP client to upload new documents.

upvoted 1 times

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

I changed C. is better then D
upvoted 1 times

(cookieMr) 5 months ago

Selected Answer: C

Hosting the website in a private S3 provides cost-effective and highly available storage for the static website content. By configuring a bucket policy to allow access from a CloudFront OAI, the S3 can be securely accessed only through CloudFront. This ensures that the website content is served through CloudFront while keeping the S3 private. Uploading website content using the AWS CLI allows for easy and efficient content management.

A. Hosting the website on an Lightsail virtual server would introduce additional management overhead and costs compared to using S3 directly for static content hosting.

B. Using an AWS ASG with EC2 instances and an ALB is not necessary for serving static website content. It would add unnecessary complexity and cost.

D. While using AWS Transfer for SFTP allows for SFTP uploads, it introduces additional costs and complexity compared to directly uploading content to an S3 using the AWS CLI. Additionally, hosting the website content in a public S3 may not be desirable from a security standpoint.
upvoted 3 times

(eugene_stalker) 6 months ago

Selected Answer: D

D - SFTP client to upload new documents.

upvoted 1 times

(bdp123) 9 months, 2 weeks ago

Selected Answer: C

AWS transfer is a cost and doesn't mention using CloudFront

<https://aws.amazon.com/aws-transfer-family/pricing/>

upvoted 4 times

(Yelizaveta) 9 months, 2 weeks ago

Selected Answer: C

If you don't want to disable block public access settings for your bucket but you still want your website to be public, you can create a Amazon CloudFront distribution to serve your static website. For more information, see Use an Amazon CloudFront distribution to serve a static website in the Amazon Route 53 Developer Guide.

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

upvoted 1 times

(PDR) 10 months ago

Selected Answer: C

I at first thought D but it is in fact C because

"D: Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP. Configure the S3 bucket for website hosting. Upload website content by using the SFTP client." questions says that the company has decided to use Amazon Cloudfront and this answer does not reference using CF and setting S3 as the Origin

"C. Create a private Amazon S3 bucket. Use an S3 bucket policy to allow access from a CloudFront origin access identity (OAI). Upload website content by using the AWS CLI." - mentions CF and the origin and the AWS CLI does infact support transfer by SFTP (which was the part I originally doubted but this link evidences that it does:

<https://docs.aws.amazon.com/cli/latest/reference/transfer/describe-server.html>

upvoted 3 times

(bullrem) 10 months, 1 week ago

Selected Answer: D

Option C, creating a private Amazon S3 bucket and using an S3 bucket policy to allow access from a CloudFront origin access identity (OAI), would not be the most cost-effective solution. While it would allow the company to use Amazon S3 for storage, it would also require additional setup and maintenance of the OAI, which would add additional cost. Additionally, this solution would not allow the use of SFTP client for uploading content which is the current method used by the company.

upvoted 1 times

(verguy) 10 months, 3 weeks ago

The Answer is C

<https://medium.com/aws-poc-and-learning/how-to-access-s3-hosted-website-via-cloudfront-using-oai-origin-access-identity-720ad7c57f15>

upvoted 2 times

(Mahadeva) 10 months, 3 weeks ago

Selected Answer: C

Option C is a better choice than D for following reasons:

(1) Cost effective: data transfer is cheaper for Cloudfront than directly from S3 bucket

(2) Resilient: recovery from failures. Having a Cloudfront distribution and making S3 bucket policy only for Cloudfront. ie. private bucket (with OAI for access) hardens and betters resiliency.

upvoted 3 times

 **gustavtd** 10 months, 4 weeks ago

Selected Answer: C

If you don't do extra setup in AWS, you can not use SFTP connecting to it, so D is not the case
upvoted 1 times

 **vtbk** 10 months, 4 weeks ago

Selected Answer: C

s3 + Cloudfront. In this case, S3 does not need to be public.
upvoted 1 times

 **Zerotn3** 11 months ago

Selected Answer: D

The most cost-effective and resilient solution for hosting a website on AWS with CloudFront is to create a public Amazon S3 bucket, configure AWS Transfer for SFTP, configure the S3 bucket for website hosting, and then upload website content using the SFTP client.

Option A involves using Amazon Lightsail to create a virtual server, which may not be the most cost-effective solution compared to using S3. Option B involves using an Auto Scaling group with EC2 instances and an Application Load Balancer, which may be more expensive and complex than using S3. Option C involves creating a private S3 bucket, which may not allow CloudFront to access the website content.

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Selected Answer: D

KEYWORD: most cost-effective and resilient architecture

Option D: Creating a public Amazon S3 bucket, configuring AWS Transfer for SFTP, configuring the S3 bucket for website hosting, and uploading website content by using the SFTP client will meet these requirements with the most cost-effective and resilient architecture.

Configuring AWS Transfer for SFTP allows the company to securely upload content to the S3 bucket using the SFTP client, which the administrator is already familiar with. This eliminates the need to change the administrator's workflow or learn new tools.

upvoted 1 times

 **Joxtat** 10 months, 2 weeks ago

<https://medium.com/aws-poc-and-learning/how-to-access-s3-hosted-website-via-cloudfront-using-oai-origin-access-identity-720ad7c57f15>
upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Option C: Creating a private Amazon S3 bucket and using an S3 bucket policy to allow access from a CloudFront origin access identity (OAI) is not a suitable solution because it does not allow the administrator to use an SFTP client to upload website content. The administrator would need to use the AWS CLI or a different tool to upload content to the S3 bucket, which would require a change in the administrator's workflow.

upvoted 1 times

 **JayBee65** 10 months, 3 weeks ago

The requirements are "cost-effective and resilient architecture", and nothing about least operational overhead so your concerns are not valid. Cloudfront makes it resilient and cuts costs, so far more relevant.

upvoted 1 times

 **PassNow1234** 11 months, 1 week ago

. The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin.

Are you sure about D?

upvoted 1 times

 **17Master** 10 months, 2 weeks ago

An administrator updates the website content infrequently and uses an SFTP client to upload new documents.

upvoted 1 times

 **techhb** 11 months, 1 week ago

Selected Answer: C

Answer is C only,Bucket doesn't need to be public when using cloudfront.

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>

upvoted 1 times

 **JayBee65** 10 months, 3 weeks ago

Yes " If your use case requires the block public access settings to be turned on, use the REST API endpoint as the origin. Then, restrict access by an origin access control (OAC) or origin access identity (OAI)."

upvoted 1 times

A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.

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

- A. Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a CreateImage API call is detected.
- B. Configure AWS CloudTrail with an Amazon Simple Notification Service (Amazon SNS) notification that occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on CreateImage when an API call is detected.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected.
- D. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a CreateImage API call is detected.

Correct Answer: D

Community vote distribution

C (66%)	A (23%)	9%
---------	---------	----

✉️ [User] [Removed] Highly Voted 12 months ago

Selected Answer: C

I'm team C.

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html#:~:text=For%20example%2C%20you%20can%20create%20an%20EventBridge%20rule%20that%20detects%20when%20the%20AMI%20creation%20process%20has%20completed%20and%20then%20invokes%20an%20Amazon%20SNS%20topic%20to%20send%20an%20email%20notification%20to%20you.>

upvoted 14 times

✉️ [User] **JayBee65** 10 months, 3 weeks ago

That link contains the exact use case and explains how C can be used.

Option B requires you to send logs to S3 and use Athena, 2 additional services that are not required, so this does not meet the "LEAST operational overhead?" requirement, since these are extra services requiring management.

upvoted 3 times

✉️ [User] **MutiverseAgent** 4 months, 1 week ago

C is correct > <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitor-ami-events.html>

upvoted 1 times

✉️ [User] **Wajif** Highly Voted 11 months, 1 week ago

Selected Answer: A

Why not A? API calls are already logged in Cloudtrail.

upvoted 14 times

✉️ [User] **rlamberti** Most Recent 1 month, 1 week ago

Selected Answer: C

"LEAST operational overhead"

Option A involves coding a Lambda. Not good!

Option C seems to be the correct.

upvoted 1 times

✉️ [User] **TariqKipkemei** 2 months, 1 week ago

Selected Answer: C

Event bridge was built specifically to handle this kind of scenario:

CreateImage API call (Event Source) -> Event bus -> Rules -> Amazon SNS (Event target)

upvoted 2 times

✉️ [User] **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: C

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected

upvoted 2 times

 **Nava702** 2 months, 3 weeks ago

Selected Answer: A

A look like the least overhead option to capture an API call.

upvoted 1 times

 **Mia2009687** 4 months, 3 weeks ago

Selected Answer: B

The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.

With option C, it won't "The company needs to design an application that captures AWS API calls". it only sends the "CreateImage API " event. We need to store the AWS API calls as well.

upvoted 1 times

 **cookieMr** 5 months ago

EventBridge (formerly CloudWatch Events) is a fully managed event bus service that allows you to monitor and respond to events within your AWS environment. By creating an EventBridge rule specifically for the CreateImage API call, you can easily detect and capture this event. Configuring the target as an SNS topic allows you to send an alert whenever a CreateImage API call occurs. This solution requires minimal operational overhead as EventBridge and SNS are fully managed services.

A. While using an Lambda to query CloudTrail logs and send an alert can achieve the desired outcome, it introduces additional operational overhead compared to using EventBridge and SNS directly.

B. Configuring CloudTrail with an SNS notification and using Athena to query on CreateImage API calls would require more setup and maintenance compared to using EventBridge and SNS.

D. Configuring an SQS FIFO queue as a target for CloudTrail logs and using a function to send an alert to an SNS topic adds unnecessary complexity to the solution and increases operational overhead. Using EventBridge and SNS directly is a simpler and more efficient approach.

upvoted 4 times

 **pisica134** 5 months, 1 week ago

D makes no sense, FIFO is not required, SQS is not used for sending notifications...C all the way

upvoted 1 times

 **edric1998** 5 months, 1 week ago

Selected Answer: D

As the link shared by who chose C, it said EventBridge can catch event (available/failed/deregistered). In this doc, CreateImage not distinct with CopyImage/RegisterImage/CreateRestoreImageTask.

So It not C.

It not B because it very overhead.

And the question say "whenever", means quick as possible, so It not A.

The right answer is D

upvoted 1 times

 **TheAbsoluteTruth** 7 months, 4 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html#:~:text=For%20example%2C%20you%20can%20create%20an%20EventBridge%20regla%20que%20detecta%20cuando%20el%20creación%20AMI%20proceso%20ha%20completado%20y%20entonces%20invoca%20un%20Amazon%20SNS%20tema%20para%20enviar%20un%20correoelectrónico%20notificación%20para%20usted>

upvoted 1 times

 **test_devops_aws** 8 months, 1 week ago

Selected Answer: C

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html>

upvoted 2 times

 **kraken21** 8 months ago

Option C makes sense here.

upvoted 1 times

 **Zerotn3** 11 months ago

Selected Answer: C

LEAST operational overhead

upvoted 1 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Selected Answer: C

The correct solution is Option C. Creating an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call and configuring the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected will meet the requirements with the least operational overhead.

Amazon EventBridge is a serverless event bus that makes it easy to connect applications together using data from your own applications, integrated Software as a Service (SaaS) applications, and AWS services. By creating an EventBridge rule for the CreateImage API call, the company can set up alerts whenever this operation is called within their account. The alert can be sent to an SNS topic, which can then be configured to send

notifications to the company's email or other desired destination.

This solution does not require the company to create a Lambda function or query CloudTrail logs, which makes it the most cost-effective and efficient option.

upvoted 7 times

 **career360guru** 11 months, 2 weeks ago

Selected Answer: C

Option C is right answer.

Eventbridge has integration with CloudTrail as source of events (using pipes).

Option D is incorrect as Cloudtrail can not automatically send its API event logs to SQS.

upvoted 1 times

 **Shasha1** 11 months, 3 weeks ago

C

Option B is not correct because it involves using Amazon Athena to query AWS CloudTrail logs, which can be a time-consuming and error-prone process. Additionally, it requires the company to manage the underlying infrastructure for Amazon Athena, which adds operational overhead.

upvoted 1 times

 **Sahilbhai** 11 months, 3 weeks ago

Selected Answer: C

answer is c

upvoted 1 times

A company owns an asynchronous API that is used to ingest user requests and, based on the request type, dispatch requests to the appropriate microservice for processing. The company is using Amazon API Gateway to deploy the API front end, and an AWS Lambda function that invokes Amazon DynamoDB to store user requests before dispatching them to the processing microservices.

The company provisioned as much DynamoDB throughput as its budget allows, but the company is still experiencing availability issues and is losing user requests.

What should a solutions architect do to address this issue without impacting existing users?

- A. Add throttling on the API Gateway with server-side throttling limits.
- B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.
- C. Create a secondary index in DynamoDB for the table with the user requests.
- D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Correct Answer: D

Community vote distribution

D (96%) 4%

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

Selected Answer: D

This solution can handle bursts of incoming requests more effectively and reduce the chances of losing requests due to DynamoDB capacity limitations. The Lambda can be configured to retrieve messages from the SQS and write them to DynamoDB at a controlled rate, allowing DynamoDB to handle the requests within its provisioned capacity. This approach provides resilience to spikes in traffic and ensures that requests are not lost during periods of high demand.

upvoted 1 times

✉️  **cookieMr** 5 months ago

Selected Answer: D

This solution can handle bursts of incoming requests more effectively and reduce the chances of losing requests due to DynamoDB capacity limitations. The Lambda can be configured to retrieve messages from the SQS and write them to DynamoDB at a controlled rate, allowing DynamoDB to handle the requests within its provisioned capacity. This approach provides resilience to spikes in traffic and ensures that requests are not lost during periods of high demand.

A. It limits can help control the request rate, but it may lead to an increase in errors and affect the user experience. Throttling alone may not be sufficient to address the availability issues and prevent the loss of requests.

B. It can improve read performance but does not directly address the availability issues and loss of requests. It focuses on optimizing read operations rather than buffering writes.

C. It may help with querying the user requests efficiently, but it does not directly solve the availability issues or prevent the loss of requests. It is more focused on data retrieval rather than buffering writes.

upvoted 2 times

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

Selected Answer: D

DAX is for reads

upvoted 2 times

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

DAX is not ideal for the following types of applications:

Applications that require strongly consistent reads (or that cannot tolerate eventually consistent reads).

Applications that do not require microsecond response times for reads, or that do not need to offload repeated read activity from underlying tables.

Applications that are write-intensive, or that do not perform much read activity.

Applications that are already using a different caching solution with DynamoDB, and are using their own client-side logic for working with that caching solution.

upvoted 2 times

✉️  **nder** 9 months ago

Selected Answer: D

The key here is "Losing user requests" sqs messages will stay in the queue until it has been processed upvoted 3 times

✉ **dark_firzen** 10 months ago

Selected Answer: D

D because SQS is the cheapest way. First 1,000,000 requests are free each month.

Question states: "The company provisioned as much DynamoDB throughput as its budget allows"

upvoted 3 times

✉ **Wajif** 11 months, 1 week ago

Selected Answer: D

D is more likely to fix this problem as SQS queue has the ability to wait (buffer) for consumer to notify that the request or message has been processed.

upvoted 1 times

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

Selected Answer: D

To address the issue of lost user requests and improve the availability of the API, the solutions architect should use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB. Option D (correct answer)

By using an SQS queue and Lambda, the solutions architect can decouple the API front end from the processing microservices and improve the overall scalability and availability of the system. The SQS queue acts as a buffer, allowing the API front end to continue accepting user requests even if the processing microservices are experiencing high workloads or are temporarily unavailable. The Lambda function can then retrieve requests from the SQS queue and write them to DynamoDB, ensuring that all user requests are stored and processed. This approach allows the company to scale the processing microservices independently from the API front end, ensuring that the API remains available to users even during periods of high demand.

upvoted 4 times

✉ **alect096** 11 months, 1 week ago

Selected Answer: B

I would go to B : <https://aws.amazon.com/es/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>

upvoted 1 times

✉ **ruqui** 4 months, 3 weeks ago

That's wrong. The document you mentioned explained it very clearly:

"Whereas both read-through and write-through caches address read-heavy workloads, a write-back (or write-behind) cache is designed to address write-heavy workloads. Note that DAX is not a write-back cache currently"

upvoted 1 times

✉ **BENICE** 11 months, 2 weeks ago

D is correct answer

upvoted 1 times

✉ **NikaCZ** 11 months, 2 weeks ago

Selected Answer: D

D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

upvoted 1 times

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

Selected Answer: D

Option D is right answer

upvoted 1 times

✉ **alexfk** 11 months, 2 weeks ago

Why not B? DAX.

"When you're developing against DAX, instead of pointing your application at the DynamoDB endpoint, you point it at the DAX endpoint, and DAX handles the rest. As a read-through/write-through cache, DAX seamlessly intercepts the API calls that an application normally makes to DynamoDB so that both read and write activity are reflected in the DAX cache."

<https://aws.amazon.com/es/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>

upvoted 1 times

✉ **ruqui** 4 months, 3 weeks ago

B is wrong because of this:

"Whereas both read-through and write-through caches address read-heavy workloads, a write-back (or write-behind) cache is designed to address write-heavy workloads. Note that DAX is not a write-back cache currently"

upvoted 1 times

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

It is not DAX because of the company's budget restriction associated with the DynamoDB. This is a requirement in the question. DynamoDB charges for DAX capacity by the hour and your DAX instances run with no long-term commitments. Please refer to:

https://aws.amazon.com/dynamodb/pricing/provisioned/#.E2.80.A2_DynamoDB_Accelerator_.28DAX.29

upvoted 2 times

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

yeah I though the answer is also DAX.

upvoted 1 times

✉  **leonnnn** 1 year ago

Selected Answer: D

Using SQS should be the answer.

upvoted 3 times

✉  **nVizzz** 11 months, 4 weeks ago

Why not DAX? Could somebody explain?

upvoted 1 times

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

Using DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB, may improve the write performance of the system, but it does not provide the same level of scalability and availability as using an SQS queue and Lambda.

Hence, Option B is incorrect.

upvoted 1 times

✉  **bmofo** 11 months, 3 weeks ago

key noted issue is "losing user requests" which is resolved with SQS

upvoted 5 times

✉  **Rameez1** 11 months, 4 weeks ago

DAX helps in reducing the read loads from DynamoDB, here we need a solution to handle write requests, which is well handled by SQS and Lamda to buffer writes on DynamoDB.

upvoted 4 times

✉  **jambajuice** 1 year ago

Selected Answer: D

Answer d

upvoted 2 times

✉  **Nigma** 1 year ago

Answer : D

upvoted 1 times

A company needs to move data from an Amazon EC2 instance to an Amazon S3 bucket. The company must ensure that no API calls and no data are routed through public internet routes. Only the EC2 instance can have access to upload data to the S3 bucket.

Which solution will meet these requirements?

- A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
- B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2 instance is located. Attach appropriate security groups to the endpoint. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
- C. Run the nslookup tool from inside the EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
- D. Use the AWS provided, publicly available ip-ranges.json file to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

Correct Answer: B

Community vote distribution

A (51%)

B (49%)

 **SSASSWS** Highly Voted 1 year ago

Selected Answer: A

I think answer should be A and not B.
as we cannot "Attach a security groups to a gateway endpoint."
upvoted 20 times

 **A_New_Guy** 11 months, 2 weeks ago

It's possible:

<https://aws.amazon.com/premiumsupport/knowledge-center/connect-s3-vpc-endpoint/>
upvoted 3 times

 **Iconique** 2 months ago

Go to console and test it yourself! With Interface Endpoint you can add security groups.
upvoted 2 times

 **kruasan** 7 months ago

No, it's not
upvoted 3 times

 **Guru4Cloud** 2 months, 1 week ago

it is possible - you should do more reading
upvoted 2 times

 **markw92** 5 months, 2 weeks ago

Gateway endpoint must be used as a target in a route table does not use security groups.
upvoted 4 times

 **Buruguduystunstugudunstuy** Highly Voted 11 months, 1 week ago

Selected Answer: B

The correct solution to meet the requirements is Option B. A gateway VPC endpoint for Amazon S3 should be created in the Availability Zone where the EC2 instance is located. This will allow the EC2 instance to access the S3 bucket directly, without routing through the public internet. The endpoint should also be configured with appropriate security groups to allow access to the S3 bucket. Additionally, a resource policy should be attached to the S3 bucket to only allow the EC2 instance's IAM role for access.

upvoted 19 times

 **Buruguduystunstugudunstuy** 11 months, 1 week ago

Option A is incorrect because an interface VPC endpoint for Amazon S3 would not provide a direct connection between the EC2 instance and the S3 bucket.

Option C is incorrect because using the nslookup tool to obtain the private IP address of the S3 bucket's service API endpoint would not provide a secure connection between the EC2 instance and the S3 bucket.

Option D is incorrect because using the ip-ranges.json file to obtain the private IP address of the S3 bucket's service API endpoint is not a secure method to connect the EC2 instance to the S3 bucket.

upvoted 3 times

 **ChrisG1454** 9 months, 2 weeks ago

There are two types VPC Endpoint:

Gateway endpoint
Interface endpoint

A Gateway endpoint:

- 1) Helps you to securely connect to Amazon S3 and DynamoDB
- 2) Endpoint serves as a target in your route table for traffic
- 3) Provide access to endpoint (endpoint, identity and resource policies)

An Interface endpoint:

- 1) Help you to securely connect to AWS services EXCEPT FOR Amazon S3 and DynamoDB
- 2) Powered by PrivateLink (keeps network traffic within AWS network)
- 3) Needs a elastic network interface (ENI) (entry point for traffic)

upvoted 19 times

 **slackbot** 3 months ago

interface endpoint exists for S3 as well

upvoted 1 times

 **mhmt4438** 10 months, 4 weeks ago

An interface VPC endpoint does provide a direct connection between the EC2 instance and the S3 bucket. It enables private communication between instances in your VPC and resources in other services without requiring an internet gateway, a NAT device, or a VPN connection.

Option A , which recommends creating an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located and attaching a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access, is the correct solution for the given scenario. It meets the requirement to ensure that no API calls and no data are routed through public internet routes and that only the EC2 instance can have access to upload data to the S3 bucket.

upvoted 3 times

 **Omok** 9 months, 4 weeks ago

In support, see <https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>

upvoted 4 times

 **lucasbg** Most Recent 14 hours, 56 minutes ago

Definitely A since you cant attach a security group to a gateway endpoint, only to an ENI.

upvoted 1 times

 **Marco_St** 2 days, 4 hours ago

Selected Answer: A

I voted A since the question did not mention LEAST cost operation. interface VPC endpoint can be used for most services while it is not free. Gateway VPC endpoint is free and only for S3 and AWS DynamoDB. But Gateway Endpoint is not using security group to control the access, it is using route table. Security group is required for interface VPC endpoint which provides an ENI and needs security group. So A

upvoted 1 times

 **Marco_St** 2 days, 4 hours ago

I voted A since the question did not mention LEAST cost operation. interface VPC endpoint can be used for most services while it is not free. Gateway VPC endpoint is free and only for S3 and AWS DynamoDB. But Gateway Endpoint is not using security group to control the access, it is using route table. Security group is required for interface VPC endpoint which provides an ENI and needs security group. So A

upvoted 1 times

 **ivan_riqueros12** 1 month, 1 week ago

Selected Answer: B

B. The endpoint should also be configured with appropriate security groups to allow access to the S3 bucket

upvoted 1 times

 **Phoese** 1 month, 1 week ago

Option B

B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2 instance is located. Attach appropriate security groups to the endpoint. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

This solution ensures that the traffic between the EC2 instance and S3 bucket does not leave the Amazon network, meeting the company's requirement for no data to be routed through the public internet. The use of security groups and resource policies ensures that only the specified EC2 instance has access to the S3 bucket.

upvoted 1 times

 **Wayne23Fang** 1 month, 2 weeks ago

Selected Answer: B

But first phrase in (A) is wrong: Interface Endpoint doesn't work for the case.

upvoted 1 times

✉ **Ramdi1** 1 month, 3 weeks ago

Selected Answer: B

Gateway VPC endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC

upvoted 1 times

✉ **vijaykamal** 2 months ago

Selected Answer: A

Option B mentions creating a gateway VPC endpoint for Amazon S3, but gateway endpoints are primarily used for routing traffic to Amazon S3 over Direct Connect or VPN connections, and they don't support attaching security groups. It's also essential to restrict access with a resource policy on the S3 bucket, which is not mentioned in option B.

Options C and D suggest alternative approaches using DNS resolution and VPC route tables, but these options may not provide the same level of security and isolation as the interface VPC endpoint in option A. Additionally, these options are more complex to set up and maintain.

upvoted 1 times

✉ **Mandar15** 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>

upvoted 1 times

✉ **Mandar15** 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>

upvoted 1 times

✉ **JKevin778** 2 months ago

Selected Answer: B

Gateway Endpoint for S3 and DynamoDB, So B

upvoted 2 times

✉ **Guru4Cloud** 2 months, 1 week ago

Selected Answer: B

B is the correct answer.

To meet the requirements of no public internet access and only allowing the EC2 instance access, the solution is to:

Create a gateway VPC endpoint for S3 in the subnet where the EC2 instance is located. This keeps S3 access within the VPC and does not route via the internet.

Attach appropriate security groups to the endpoint to control access.

Use a S3 bucket resource policy to only allow access from the EC2 instance IAM role.

upvoted 2 times

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

Selected Answer: A

You can provision interface endpoints for s3.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#:~:text=With-,AWS%20PrivateLink,-for%20Amazon%20S3>

upvoted 1 times

✉ **5ab5e39** 2 months, 3 weeks ago

B is correct, The outbound rules for the security group for instances that access Amazon S3 through the gateway endpoint must allow traffic to Amazon S3. You can use the prefix list ID for Amazon S3 as the destination in the outbound rule.

upvoted 1 times

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

Selected Answer: B

nothing call interface VPC endpoint for s3, only gateway interface VPC for s3

upvoted 2 times

✉ **skh015** 3 months ago

Interface endpoint exists

<https://youtu.be/TqApkvJx5hw>

upvoted 1 times

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.

What should the solutions architect do to ensure that the architecture supports distributed session data management?

- A. Use Amazon ElastiCache to manage and store session data.
- B. Use session affinity (sticky sessions) of the ALB to manage session data.
- C. Use Session Manager from AWS Systems Manager to manage the session.
- D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session.

Correct Answer: A

Community vote distribution

A (100%)

 **Buruguduystunstugudunstuy**  11 months, 1 week ago

Selected Answer: A

The correct answer is A. Use Amazon ElastiCache to manage and store session data.

In order to support distributed session data management in this scenario, it is necessary to use a distributed data store such as Amazon ElastiCache. This will allow the session data to be stored and accessed by multiple EC2 instances across multiple Availability Zones, which is necessary for a scalable and highly available architecture.

Option B, using session affinity (sticky sessions) of the ALB, would not be sufficient because this would only allow the session data to be stored on a single EC2 instance, which would not be able to scale across multiple Availability Zones.

Options C and D, using Session Manager and the GetSessionToken API operation in AWS STS, are not related to session data management and would not be appropriate solutions for this scenario.

upvoted 16 times

 **TariqKipkemei**  2 months, 1 week ago

Selected Answer: A

Yap agree with go you guys, this is one of the use cases for Amazon ElastiCache.

It was designed to store ephemeral session data to quickly personalize gaming, e-commerce, social media, and online applications with microsecond response times.

<https://aws.amazon.com/elasticsearch/#:~:text=Store,-,ephemeral,-session%20data%20to>

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

The correct answer is A. Use Amazon ElastiCache to manage and store session data.

upvoted 1 times

 **cookieMr** 4 months, 3 weeks ago

Selected Answer: A

ElastiCache is a managed in-memory data store service that is well-suited for managing session data in a distributed architecture. It provides high-performance, scalable, and durable storage for session data, allowing multiple EC2 instances to access and share session data seamlessly. By using ElastiCache, the application can offload the session management workload from the EC2 instances and leverage the distributed caching capabilities of ElastiCache for improved scalability and performance.

Option B, using session affinity (sticky sessions) of the ALB, is not the best choice for distributed session data management because it ties each session to a specific EC2 instance. As the instances scale up and down frequently, it can lead to uneven load distribution and may not provide optimal scalability.

Options C and D are not applicable for managing session data. AWS Systems Manager's Session Manager is primarily used for secure remote shell access to EC2 instances, and the AWS STS GetSessionToken API operation is used for temporary security credentials and not session data management.

upvoted 1 times

 **cookieMr** 5 months ago

ElastiCache is a managed in-memory data store service that is well-suited for managing session data in a distributed architecture. It provides high-performance, scalable, and durable storage for session data, allowing multiple EC2 instances to access and share session data seamlessly. By using ElastiCache, the application can offload the session management workload from the EC2 instances and leverage the distributed caching capabilities of ElastiCache for improved scalability and performance.

Option B, using session affinity (sticky sessions) of the ALB, is not the best choice for distributed session data management because it ties each session to a specific EC2 instance. As the instances scale up and down frequently, it can lead to uneven load distribution and may not provide optimal scalability.

Options C and D are not applicable for managing session data. AWS Systems Manager's Session Manager is primarily used for secure remote shell access to EC2 instances, and the AWS STS GetSessionToken API operation is used for temporary security credentials and not session data management.

upvoted 2 times

✉ **Abrar2022** 5 months, 1 week ago

Selected Answer: A

A. Use Amazon ElastiCache to manage and store session data.

- Correct. - Session data is managed at the application-layer, and a distributed cache should be used

B. Use session affinity (sticky sessions) of the ALB to manage session data.

- Wrong. This tightly couples the individual EC2 instances to the session data, and requires additional logic in the ALB. When scale-in happens, the session data stored on individual EC2 instances is destroyed

upvoted 1 times

✉ **techhb** 10 months, 2 weeks ago

Selected Answer: A

correct answer is A as instance are getting up and down.

upvoted 1 times

✉ **inseong** 11 months, 2 weeks ago

야 근데 210문제는 어딨나 ..?

upvoted 1 times

✉ **noche** 9 months ago

<https://www.examtopics.com/discussions/amazon/view/94992-exam-aws-certified-solutions-architect-associate-saa-c03/>

여기 임마

upvoted 1 times

✉ **NikaCZ** 11 months, 2 weeks ago

Selected Answer: A

Amazon ElastiCache to manage and store session data.

upvoted 1 times

✉ **k1kavi1** 11 months, 2 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/46412-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

✉ **Shasha1** 11 months, 3 weeks ago

A

Amazon ElastiCache to manage and store session data. This solution will allow the application to automatically scale across multiple Availability Zones without losing session data, as the session data will be stored in a cache that is accessible from any EC2 instance. Additionally, using Amazon ElastiCache will enable the company to easily manage and scale the cache as needed, without requiring any changes to the application code. Option C is not correct because Session Manager from AWS Systems Manager will not provide the necessary support for distributed session data management. Session Manager is a tool for managing and tracking sessions on EC2 instances, but it does not provide a mechanism for storing and managing session data in a distributed environment.

upvoted 3 times

✉ **Tela0** 12 months ago

better justification found here...

<https://www.examtopics.com/discussions/amazon/view/46412-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

✉ **kmaneith** 12 months ago

why not C?

upvoted 1 times

✉ **leonnnn** 1 year ago

Selected Answer: A

ALB sticky session can keep request accessing to the same backend application. But it says "distributed session management" and company "will to change code", so I think A is better

upvoted 3 times

✉ **Nigma** 1 year ago

Selected Answer: A

Answer : A

upvoted 1 times

A company offers a food delivery service that is growing rapidly. Because of the growth, the company's order processing system is experiencing scaling problems during peak traffic hours. The current architecture includes the following:

- A group of Amazon EC2 instances that run in an Amazon EC2 Auto Scaling group to collect orders from the application
- Another group of EC2 instances that run in an Amazon EC2 Auto Scaling group to fulfill orders

The order collection process occurs quickly, but the order fulfillment process can take longer. Data must not be lost because of a scaling event.

A solutions architect must ensure that the order collection process and the order fulfillment process can both scale properly during peak traffic hours. The solution must optimize utilization of the company's AWS resources.

Which solution meets these requirements?

- Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure each Auto Scaling group's minimum capacity according to peak workload values.
- Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure a CloudWatch alarm to invoke an Amazon Simple Notification Service (Amazon SNS) topic that creates additional Auto Scaling groups on demand.
- Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Scale the Auto Scaling groups based on notifications that the queues send.
- Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Create a metric based on a backlog per instance calculation. Scale the Auto Scaling groups based on this metric.

Correct Answer: C

Community vote distribution

D (83%)

C (17%)

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

Selected Answer: D

When the backlog per instance reaches the target value, a scale-out event will happen. Because the backlog per instance is already 150 messages (1500 messages / 10 instances), your group scales out, and it scales out by five instances to maintain proportion to the target value.

Backlog per instance: To calculate your backlog per instance, start with the ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling group is the number of instances in the InService state, to get the backlog per instance.

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

upvoted 6 times

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

Selected Answer: D

D. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Create a metric based on a backlog per instance calculation. Scale the Auto Scaling groups based on this metric.

upvoted 2 times

✉  **n43u435b543ht2b** 3 months, 3 weeks ago

Selected Answer: D

C is incorrect as scaling based on the number of "notifications" doesn't make logical sense. This means that both the order collection and fulfillment instances would scale in parallel, but they have clearly said that the collection is processing quickly while the fulfillment is struggling. Therefore, we should scale the pool when there is a backlog building in a respective queue - not just based on the number of incoming requests.

upvoted 3 times

✉  **argl1995** 5 months ago

SQS auto-scales by default so I don't think we need to mention it explicitly. Option D should be correct.

upvoted 1 times

✉  **cookieMr** 5 months ago

Selected Answer: D

A. This approach focuses solely on CPU utilization, which may not accurately reflect the scaling needs of the order collection and fulfillment processes. It does not address the need for decoupling and reliable message processing.

B. While this approach incorporates alarms to trigger additional Auto Scaling groups, it lacks the decoupling and reliable message processing provided by using SQS queues. It may lead to inefficient scaling and potential data loss.

C. Although using SQS queues is a step in the right direction, scaling solely based on queue notifications may not provide optimal resource utilization. It does not consider the backlog per instance and does not allow for fine-grained control over scaling.

Overall, option D, which involves using SQS queues for order collection and fulfillment, creating a metric based on backlog per instance calculation, and scaling the Auto Scaling groups accordingly, is the most suitable solution to address the scaling problems while optimizing resource utilization and ensuring reliable message processing.

upvoted 3 times

studynoplay 6 months, 2 weeks ago

Selected Answer: D

C is incorrect. "based on notifications that the queues send" SQS does not send notification

upvoted 2 times

mandragon 6 months, 3 weeks ago

Selected Answer: C

D is not correct because it requires more operational overhead and complexity than option C which is simpler and more cost-effective. It uses the existing queue metrics that are provided by Amazon SQS and does not require creating or publishing any custom metrics. You can use target tracking scaling policies to automatically maintain a desired backlog per instance ratio without having to calculate or monitor it yourself.

upvoted 2 times

JayBee65 10 months, 1 week ago

Selected Answer: D

Scale based on queue length

upvoted 2 times

Rudraman 10 months, 2 weeks ago

answer is D.

read question again

upvoted 2 times

LuckyAro 10 months, 2 weeks ago

Selected Answer: D

The number of instances in your Auto Scaling group can be driven by how long it takes to process a message and the acceptable amount of latency (queue delay).

The solution is to use a backlog per instance metric with the target value being the acceptable backlog per instance to maintain.

upvoted 1 times

Aseem8888 10 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

Rudraman 10 months, 2 weeks ago

C

Need to Auto-Scale Queue of SQS

upvoted 1 times

JayBee65 10 months, 1 week ago

Why would you scale based on " Scale the Auto Scaling groups based on notifications that the queues send."? Would it not make 1000 times more sense to scale base don queue length "Create a metric based on a backlog per instance calculation"?

upvoted 3 times

techhb 10 months, 2 weeks ago

Selected Answer: D

I think its D as here we are creating new metric to calculate load on each EC2 instance.

upvoted 2 times

techhb 10 months, 2 weeks ago

I think its D as here we are creating new metric to calculate load on each EC2 instance.

upvoted 2 times

wmp7039 10 months, 2 weeks ago

Selected Answer: D

C is incorrect as SQS doesn't send notifications and needs to be polled by the consumers

upvoted 2 times

KM01 10 months, 2 weeks ago

I think, D

upvoted 1 times

swolfgang 10 months, 2 weeks ago

Selected Answer: C

i think c ,but i m not sure i think both of solve problem
upvoted 1 times

 **JayBee65** 10 months, 1 week ago

No they don't. How exactly would you scale based on a queue sending a message? Scale up when it sends a message? Scale up every time it sends a message? This takes no account of how quickly messages are processed.

upvoted 2 times

A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of “application” and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.

Which solution meets these requirements?

- A. Use AWS CloudTrail to generate a list of resources with the application tag.
- B. Use the AWS CLI to query each service across all Regions to report the tagged components.
- C. Run a query in Amazon CloudWatch Logs Insights to report on the components with the application tag.
- D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag.

Correct Answer: D

Community vote distribution

D (100%)

 **cookieMr** Highly Voted 5 months ago

Selected Answer: D

A is not the quickest solution because CloudTrail primarily focuses on capturing and logging API activity. While it can provide information about resource changes, it may not provide a comprehensive and quick way to identify all the tagged components across multiple services and Regions.

B involves manually querying each service using the AWS CLI, which can be time-consuming and cumbersome, especially when dealing with multiple services and Regions. It is not the most efficient solution for quickly identifying tagged components.

C is focused on analyzing logs rather than directly identifying the tagged components. While CloudWatch Logs Insights can help extract information from logs, it may not provide a straightforward and quick way to gather a consolidated list of all tagged components across different services and Regions.

D is the quickest solution as it leverages the Resource Groups Tag Editor, which is specifically designed for managing and organizing resources based on tags. It offers a centralized and efficient approach to generate a report of tagged components across multiple services and Regions.
upvoted 6 times

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

Selected Answer: D

Tags are key and value pairs that act as metadata for organizing your AWS resources

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag

upvoted 2 times

 **Bmarodi** 6 months, 1 week ago

Selected Answer: D

A solutions architect can provide the quickest solution for identifying all of the tagged components by running a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag, hence the option D is right answer.

upvoted 2 times

 **Dondozzy** 8 months, 2 weeks ago

Selected Answer: D

The answer is D

upvoted 2 times

 **sh0811** 10 months ago

Selected Answer: D

D가 맞습니다.

upvoted 2 times

 **Training4aBetterLife** 10 months ago

Selected Answer: D

<https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html>

upvoted 2 times

 **Rudraman** 10 months, 2 weeks ago

Answer is D.

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: D

validated

<https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html>

upvoted 1 times

 **kbaruu** 10 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **waiyiu9981** 10 months, 2 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/51352-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company needs to export its database once a day to Amazon S3 for other teams to access. The exported object size varies between 2 GB and 5 GB. The S3 access pattern for the data is variable and changes rapidly. The data must be immediately available and must remain accessible for up to 3 months. The company needs the most cost-effective solution that will not increase retrieval time.

Which S3 storage class should the company use to meet these requirements?

- A. S3 Intelligent-Tiering
- B. S3 Glacier Instant Retrieval
- C. S3 Standard
- D. S3 Standard-Infrequent Access (S3 Standard-IA)

Correct Answer: A

Community vote distribution

A (71%)	D (17%)	11%
---------	---------	-----

✉  **techhb**  10 months, 2 weeks ago

Selected Answer: A

S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the Infrequent Access tier and after 90 days of no access to the Archive Instant Access tier.

upvoted 11 times

✉  **Devsin2000** 6 months, 3 weeks ago

<https://aws.amazon.com/getting-started/hands-on/getting-started-using-amazon-s3-intelligent-tiering/>

upvoted 2 times

✉  **VladanO**  3 weeks, 1 day ago

Selected Answer: B

<https://aws.amazon.com/s3/storage-classes/glacier/instant-retrieval/>

"Amazon S3 Glacier Instant Retrieval is an archive storage class that delivers the lowest-cost storage for long-lived data that is rarely accessed and requires retrieval in milliseconds"

upvoted 1 times

✉  **ivan_riqueros12** 1 month, 1 week ago

Selected Answer: A

A. El patrón de acceso a los datos es variable y cambia rápidamente = S3 Intelligent-Tiering

upvoted 1 times

✉  **Abdou1604** 1 month, 2 weeks ago

very important note , S3 Intelligent-Tiering got no retrieval charges

upvoted 2 times

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

Selected Answer: A

access pattern for the data is variable and changes rapidly = S3 Intelligent-Tiering

upvoted 2 times

✉  **Sultanoid** 3 months ago

Selected Answer: C

There are 2 viable options A and C.

The Intelligent tearing(A) might put your data in the archive or Infrequent Acces if it is not used for 80 days and then used as crazy for the last 10 days of the period which will cause delays in retrieval or the costs associated with traffic.

Option C can be optimised with the Time To Live policy of 90 days and will be the most efficient and reliable solution to satisfy the needs.

upvoted 4 times

✉  **mtmayer** 3 months, 4 weeks ago

Has to be C. S3 Intelligent-Tiering is for data with varying or unknown access needs. Not the case here. We know data must be highly available for 30 days.

upvoted 2 times

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

Selected Answer: A

key - "Changing access patterns"

upvoted 1 times

 **maheshudara** 4 months, 3 weeks ago

"The S3 access pattern for the data is variable and changes rapidly"
upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: A

Option A is designed for objects with changing access patterns, but it may not be the most cost-effective solution for long-term storage of the data, especially if the access pattern is variable and changes rapidly.

Option B is optimized for long-term archival storage and may not provide the immediate accessibility required by the company. Retrieving data from Glacier storage typically incurs a longer retrieval time compared to other storage classes.

Option C is the appropriate choice for immediate availability and quick access to the data. It offers high durability, availability, and low latency access, making it suitable for the company's needs. However, it is not the most cost-effective option for long-term storage.

Option D is a more cost-effective storage class compared to S3 Standard, especially for data that is accessed less frequently. However, since the access pattern for the data is variable and changes rapidly, S3 Standard-IA may not be the most cost-effective solution, as it incurs additional retrieval fees for frequent access.

upvoted 2 times

 **markw92** 5 months, 2 weeks ago

Answer A: S3 Intelligent-Tiering is the recommended storage class for data with unknown, changing, or unpredictable access patterns, independent of object size or retention period, such as data lakes, data analytics, and new applications.

upvoted 1 times

 **AlankarJ** 5 months, 3 weeks ago

The questions specifically says, data should me immediately available. So D can't be true as S3 Infrequent access is for data which is not accessed frequently. Don't forget upto 3 months.

upvoted 2 times

 **ruqui** 6 months, 1 week ago

Selected Answer: A

Amazon S3 Intelligent-Tiering is the only cloud storage class that delivers automatic storage cost savings when data access patterns change, without performance impact or operational overhead

upvoted 1 times

 **ErfanKh** 7 months, 3 weeks ago

Selected Answer: D

I think D and ChatGPT says D as well

upvoted 1 times

 **ALLVCAP01** 5 months ago

chatgpt isn't perfect yet. Most of them are wrong when it comes to problems.

upvoted 1 times

 **mahejosh** 5 months, 3 weeks ago

ChatGpt is cheeks, eff that

upvoted 1 times

 **studynoplay** 6 months, 2 weeks ago

ChatGPT is not always correct. Use your intelligence to answer questions

upvoted 3 times

 **Grace83** 8 months, 2 weeks ago

Definitely A

upvoted 1 times

 **Russ99** 8 months, 2 weeks ago

Selected Answer: D

D is the correct answer for this use case

upvoted 1 times

 **neosis91** 9 months, 3 weeks ago

Selected Answer: D

Response D, not A

S3 Intelligent-Tiering is a cost-optimized storage class that automatically moves data to the most cost-effective access tier based on changing access patterns. Although it offers cost savings, it also introduces additional latency and retrieval time into the data retrieval process, which may not meet the requirement of "immediately available" data.

On the other hand, S3 Standard-Infrequent Access (S3 Standard-IA) provides low cost storage with low latency and high throughput performance. It is designed for infrequently accessed data that can be recreated if lost, and can be retrieved in a timely manner if required. It is a cost-effective solution that meets the requirement of immediately available data and remains accessible for up to 3 months.

upvoted 2 times

 **Rudraman** 10 months, 2 weeks ago

Changes rapidly and immidiately available so Answe is AAAAA.
upvoted 4 times

A company is developing a new mobile app. The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection. The company has minimal infrastructure and operational staff. The company needs to reduce its share of the responsibility in managing, updating, and securing servers for its AWS environment.

What should a solutions architect recommend to meet these requirements?

- A. Configure AWS WAF rules and associate them with the ALB.
- B. Deploy the application using Amazon S3 with public hosting enabled.
- C. Deploy AWS Shield Advanced and add the ALB as a protected resource.
- D. Create a new ALB that directs traffic to an Amazon EC2 instance running a third-party firewall, which then passes the traffic to the current ALB.

Correct Answer: A

Community vote distribution

A (69%)

C (31%)

✉  **ShinobiGrappler** Highly Voted 10 months, 2 weeks ago

Selected Answer: C

C --- Read and understand the question. *The company needs to reduce its share of responsibility in managing, updating, and securing servers for its AWS environment* Go with AWS Shield advanced --This is a managed service that includes AWS WAF, custom mitigations, and DDoS insight.
upvoted 14 times

✉  **rokeus** 1 month ago

I agree, both A and C answer the first demand ,where A is answer to the technical request., but for reducing responsibility you will need shield advance - meaning C.
upvoted 1 times

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

I dont know how this comment gets 11x upvotes.
A.To filter traffic and protect against application attacks like cross-site scripting and SQL injection, the company can use AWS Web Application Firewall with managed rules on the Application Load Balancer. This provides security with minimal infrastructure and operations overhead.
upvoted 6 times

✉  **Steve_4542636** 9 months ago

You stated, "This is a managed service that includes AWS WAF, custom mitigations, and DDoS insight." and you are correct. However, the service you would actually have to setup to prevent SQL injection attacks is WAF.
upvoted 8 times

✉  **darn** 7 months, 1 week ago

exactly, thats like saying lets implemented NEtwork firewall Manager to manage WAF, absurd!
upvoted 3 times

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

Brother answer is A, Read the question once again or ask CHATGPT for more in-depth analysis
upvoted 2 times

✉  **TariqKipkemei** Most Recent 2 months, 1 week ago

Selected Answer: A

AWS WAF helps you protect against common web exploits and bots that can affect availability, compromise security, or consume excessive resources. Protect against vulnerabilities and exploits such as SQL injection or Cross site scripting attacks.
upvoted 4 times

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

Selected Answer: A

To filter traffic and protect against application attacks like cross-site scripting and SQL injection, the company can use AWS Web Application Firewall with managed rules on the Application Load Balancer. This provides security with minimal infrastructure and operations overhead.
upvoted 2 times

✉  **Undisputed** 4 months ago

Selected Answer: A

To achieve proper traffic filtering and protect the Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting (XSS) or SQL injection, while minimizing infrastructure and operational overhead, the company can consider using AWS Web Application Firewall (WAF) with AWS Managed Rules.

upvoted 2 times

✉️ **vini15** 4 months, 2 weeks ago

A-- Keywords(cross-site scripting or SQL injection)

upvoted 3 times

✉️ **animefan1** 4 months, 4 weeks ago

Selected Answer: A

WAF benefits are rules, SQL injection & XSS protection

upvoted 1 times

✉️ **sbnpj** 5 months ago

Selected Answer: A

Not C because- WS Shield Advanced provides DDoS protection, it does not specifically address application-level attacks such as XSS or SQL injection

upvoted 3 times

✉️ **cookieMr** 5 months ago

Selected Answer: A

By configuring AWS WAF rules and associating them with the ALB, the company can filter and block malicious traffic before it reaches the application. AWS WAF offers pre-configured rule sets and allows custom rule creation to protect against common vulnerabilities like XSS and SQL injection.

Option B does not provide the necessary security and traffic filtering capabilities to protect against application-level attacks. It is more suitable for hosting static content rather than implementing security measures.

Option C is focused on DDoS protection rather than application-level attacks like XSS or SQL injection. While AWS Shield Advanced does not address the specific requirements mentioned in the scenario.

Option D involves maintaining and securing additional infrastructure, which goes against the requirement of reducing responsibility and relying on minimal operational staff.

upvoted 4 times

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

Selected Answer: C

With Shield advanced you get centralized protection management; this allows you to use AWS firewall manager (included in AWS Shield) with policies automatically apply WAF to appliances. Massive sales pitch, see the link: <https://aws.amazon.com/shield/features/>

upvoted 1 times

✉️ **Terry_123** 6 months, 2 weeks ago

Selected Answer: A

Shield is not aimed to handle SQL injection.

upvoted 1 times

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

Selected Answer: A

WAF = cross-site scripting or SQL injection

Shield/Shield Advanced = DDoS

upvoted 3 times

✉️ **Abhineet9148232** 6 months, 4 weeks ago

Selected Answer: A

Even with AWS Shield Advanced, you would still need to configure AWS WAF (only its costing is included with Shield Adv.) rules to protect against common application-level attacks such as cross-site scripting or SQL injection.

Since, there is no mention of protection against DDoS attacks, C is a more costly and not useful.

upvoted 2 times

✉️ **SkyZeroZx** 7 months, 1 week ago

Selected Answer: A

WAF == application-level attacks, such as cross-site scripting or SQL injection

A

upvoted 2 times

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

Selected Answer: A

Answer is A, WAF will protect the infra from CSS typing of injections while Shield will be used to protect Infra from DDOS attacks

Dont get Confused.

only trick to get the right answer for the question is

read the question multiple times even when you are very confident about the answer you chose on first attempt

upvoted 4 times

 **Kenzo** 8 months ago

Answer is A

upvoted 1 times

 **[Removed]** 8 months ago

Selected Answer: A

AWS WAF projects against SQL injection.

upvoted 1 times

 **supppp** 8 months ago

CCCCCCCCCCCCCCCCCCCCCC

upvoted 1 times

A company's reporting system delivers hundreds of .csv files to an Amazon S3 bucket each day. The company must convert these files to Apache Parquet format and must store the files in a transformed data bucket.

Which solution will meet these requirements with the LEAST development effort?

- A. Create an Amazon EMR cluster with Apache Spark installed. Write a Spark application to transform the data. Use EMR File System (EMRFS) to write files to the transformed data bucket.
- B. Create an AWS Glue crawler to discover the data. Create an AWS Glue extract, transform, and load (ETL) job to transform the data. Specify the transformed data bucket in the output step.
- C. Use AWS Batch to create a job definition with Bash syntax to transform the data and output the data to the transformed data bucket. Use the job definition to submit a job. Specify an array job as the job type.
- D. Create an AWS Lambda function to transform the data and output the data to the transformed data bucket. Configure an event notification for the S3 bucket. Specify the Lambda function as the destination for the event notification.

Correct Answer: D

Community vote distribution

B (100%)

 **Babba**  10 months, 2 weeks ago

Selected Answer: B

It looks like AWS Glue allows fully managed CSV to Parquet conversion jobs: <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>

upvoted 10 times

 **nileeka97**  2 months ago

Selected Answer: B

Parquet format =====> Amazon Glue

upvoted 2 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: B

B. Create an AWS Glue crawler to discover the data. Create an AWS Glue extract, transform, and load (ETL) job to transform the data. Specify the transformed data bucket in the output step.

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: B

AWS Glue is a fully managed ETL service that simplifies the process of preparing and transforming data for analytics. Using AWS Glue requires minimal development effort compared to the other options.

Option A requires more development effort as it involves writing a Spark application to transform the data. It also introduces additional infrastructure management with the EMR cluster.

Option C requires writing and managing custom Bash scripts for data transformation. It requires more manual effort and does not provide the built-in capabilities of AWS Glue for data transformation.

Option D requires developing and managing a custom Lambda for data transformation. While Lambda can handle the transformation, it requires more effort compared to AWS Glue, which is specifically designed for ETL operations.

Therefore, option B provides the easiest and least development effort by leveraging AWS Glue's capabilities for data discovery, transformation, and output to the transformed data bucket.

upvoted 3 times

 **markw92** 5 months, 2 weeks ago

Least development effort means lambda. Glue also works but more overhead and cost. A simple lambda like this <https://github.com/ayshaysha/aws-csv-to-parquet-converter/blob/main/csv-parquet-converter.py> can be used to convert as soon as you see files in s3 bucket.

upvoted 3 times

 **achevez85** 8 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>

upvoted 1 times

 **Training4aBetterLife** 10 months, 1 week ago

Selected Answer: B

S3 provides a single control to automatically encrypt all new objects in a bucket with SSE-S3 or SSE-KMS. Unfortunately, these controls only affect new objects. If your bucket already contains millions of unencrypted objects, then turning on automatic encryption does not make your bucket secure as the unencrypted objects remain.

For S3 buckets with a large number of objects (millions to billions), use Amazon S3 Inventory to get a list of the unencrypted objects, and Amazon S3 Batch Operations to encrypt the large number of old, unencrypted files.

upvoted 2 times

 **Training4aBetterLife** 10 months, 1 week ago

Versioning:

When you overwrite an S3 object, it results in a new object version in the bucket. However, this will not remove the old unencrypted versions of the object. If you do not delete the old version of your newly encrypted objects, you will be charged for the storage of both versions of the objects.

S3 Lifecycle

If you want to remove these unencrypted versions, use S3 Lifecycle to expire previous versions of objects. When you add a Lifecycle configuration to a bucket, the configuration rules apply to both existing objects and objects added later. C is missing this step, which I believe is what makes B the better choice. B includes the functionality of encrypting the old unencrypted objects via Batch Operations, whereas, Versioning does not address the old unencrypted objects.

upvoted 1 times

 **Training4aBetterLife** 10 months, 1 week ago

Please delete this. I was meaning to place this response on a different question.

upvoted 1 times

 **Training4aBetterLife** 10 months, 1 week ago

Please delete this. I was meaning to place this response on a different question.

upvoted 1 times

 **Rudraman** 10 months, 2 weeks ago

ETL = Glue

upvoted 3 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: B

AWS Glue Crawler is for ETL

upvoted 1 times

 **kbaruu** 10 months, 2 weeks ago

Selected Answer: B

The correct answer is B

upvoted 1 times

 **Mamiololo** 10 months, 2 weeks ago

B is the answer

upvoted 2 times

 **swolfgang** 10 months, 2 weeks ago

Selected Answer: B

it should be b

upvoted 1 times

 **marcioicebr** 10 months, 2 weeks ago

Selected Answer: B

De acordo com a documentação, a resposta certa é B.

https://docs.aws.amazon.com/pt_br/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html

upvoted 1 times

 **AHUI** 10 months, 2 weeks ago

B is the ans

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: B

Answer is B

upvoted 1 times

 **Kayamables** 10 months, 2 weeks ago

Option B sounds more plausible to me.

upvoted 1 times

A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data need to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migration must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.

What should a solutions architect do to migrate and store the data at the LOWEST cost?

- A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
- B. Deploy a VPN connection between the data center and Amazon VPC. Use the AWS CLI to copy the data from on premises to Amazon S3 Glacier.
- C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
- D. Use AWS DataSync to transfer the data and deploy a DataSync agent on premises. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

Correct Answer: A

Community vote distribution

A (100%)

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: A

Terabytes, low costs, limited time = AWS snowball devices
upvoted 2 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
upvoted 1 times

 **voccer** 4 months, 3 weeks ago

Selected Answer: A

hundreds of Terabytes => always use Snowball
upvoted 4 times

 **gosai90786** 5 months ago

one DataSync agent can use 10GBps and can setup a bandwidth.
So total time = $(700 \times 1000) \text{GB} / 10 \text{GBps} = 70000 \text{ sec} = 19.4 \text{ days}$.
Using Multiple Snowball devices will involve ordering them from AWS, setting them up on your data-center for copy and then incurring the shipping cost for too and fro movement to your AWS cloud.
if time constraint was critical , say 1 week then snowball would have been a viable option. But here we have 30 days, so DataSync will be less costly(takes ~19days)
upvoted 1 times

 **slackbot** 3 months ago

your math is wrong mate, and they have 0.5Gbps connection, not 10GBps
500Mbps = roughly 60MBps
 $30 \times 24 \times 3600 \times 0.06 \text{TB} = \text{roughly } 155 \text{TB}$
this is way short of 700TB
upvoted 2 times

 **cookieMr** 5 months ago

Selected Answer: A

By ordering Snowball devices, the company can transfer the 700 TB of backup data from its data center to AWS. Once the data is transferred to S3, a lifecycle policy can be applied to automatically transition the files from the S3 Standard storage class to the cost-effective Amazon S3 Glacier Deep Archive storage class.

Option B would require continuous data transfer over the public internet, which could be time-consuming and costly given the large amount of data. It may also require significant bandwidth allocation.

Option C would involve additional costs for provisioning and maintaining the dedicated connection, which may not be necessary for a one-time data migration.

Option D could be a viable option, but it may incur additional costs for deploying and managing the DataSync agent.

Therefore, option A is the recommended choice as it provides a secure and efficient data transfer method using Snowball devices and allows for cost optimization through lifecycle policies by transitioning the data to S3 Glacier Deep Archive for long-term storage.

upvoted 2 times

 **arjundevops** 7 months, 1 week ago

A is the correct answer.

even though they have 500mbps internetspeed, it will take around 130days to transfer the data from on premises to AWS

so they have only 1 option which is Snowball devices

upvoted 2 times

 **Paras043** 7 months, 3 weeks ago

Selected Answer: A

A is the correct one

upvoted 1 times

 **CapJackSparrow** 8 months, 2 weeks ago

Q: What is AWS Snowball Edge?

AWS Snowball Edge is an edge computing and data transfer device provided by the AWS Snowball service. It has on-board storage and compute power that provides select AWS services for use in edge locations. Snowball Edge comes in two options, Storage Optimized and Compute Optimized, to support local data processing and collection in disconnected environments such as ships, windmills, and remote factories. Learn more about its features here.

Q: What happened with the original 50 TB and 80 TB AWS Snowball devices?

The original Snowball devices were transitioned out of service and Snowball Edge Storage Optimized are now the primary devices used for data transfer.

Q: Can I still order the original Snowball 50 TB and 80 TB devices?

No. For data transfer needs now, please select the Snowball Edge Storage Optimized devices.

upvoted 1 times

 **vherman** 9 months ago

Selected Answer: A

Snowball

upvoted 1 times

 **KZM** 9 months, 2 weeks ago

9 Snowball devices are needed to migrate the 700TB of data.

upvoted 1 times

 **KZM** 9 months, 2 weeks ago

700TB of Data can not be transferred through a 500Mbps link within one month.

Total data that can be transferred in one month = bandwidth x time

= (500 Mbps / 8 bits per byte) x (30 days x 24 hours x 3600 seconds per hour)

= 648,000 GB or 648 TB

This is calculated theoretically with the maximum available situation. Due to a number of factors, the actual total transferred Data may be less than 645 TB.

upvoted 3 times

 **mandragon** 6 months, 3 weeks ago

Good thinking. Agree with the solution. Only the calculation is wrong. It should give 162tb as a result

upvoted 3 times

 **Rudraman** 10 months, 2 weeks ago

Snow ball Devices the answe is AAAAAA.

upvoted 2 times

 **wmp7039** 10 months, 2 weeks ago

A is incorrect as DC is an expensive option. Correct answer should be C as the company already has 500Mbps that can be used for data transfer. By consuming all the available internet bandwidth, data transfer will complete in 3 hours 6 mins - <https://www.omnicalculator.com/other/data-transfer>

upvoted 1 times

 **wmp7039** 10 months, 2 weeks ago

Ignore please, miscalculated time to transfer, it will take 129 days and will breach the 1 month requirement. A is correct.

upvoted 5 times

 **kbaruu** 10 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **swolfgang** 10 months, 2 weeks ago

a is correct but not less expensive.I think,should be D.

upvoted 1 times

✉  **Parsons** 10 months, 2 weeks ago

Selected Answer: A

A is correct.

Cannot copy files directly from on-prem to S3 Glacier with DataSync. It should be S3 standard first, then configuration S3 Lifecycle to transit to Glacier => Exclude D.

upvoted 1 times

✉  **PDR** 10 months ago

yes you can - <https://docs.aws.amazon.com/datasync/latest/userguide/create-s3-location.html#using-storage-classes>

upvoted 1 times

✉  **mhmt4438** 10 months, 2 weeks ago

Selected Answer: A

The correct answer is A

upvoted 1 times

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

Less expensive = Data Sync i guess (D)

upvoted 2 times

✉  **Pindol** 10 months, 1 week ago

"The migration must be complete within 1 month" you can't complete this with transfer 500Mb/s. With that speed we need 129days to transfer. Snowball is only way to do it in desired time.

upvoted 2 times

A company has a serverless website with millions of objects in an Amazon S3 bucket. The company uses the S3 bucket as the origin for an Amazon CloudFront distribution. The company did not set encryption on the S3 bucket before the objects were loaded. A solutions architect needs to enable encryption for all existing objects and for all objects that are added to the S3 bucket in the future.

Which solution will meet these requirements with the LEAST amount of effort?

- A. Create a new S3 bucket. Turn on the default encryption settings for the new S3 bucket. Download all existing objects to temporary local storage. Upload the objects to the new S3 bucket.
- B. Turn on the default encryption settings for the S3 bucket. Use the S3 Inventory feature to create a .csv file that lists the unencrypted objects. Run an S3 Batch Operations job that uses the copy command to encrypt those objects.
- C. Create a new encryption key by using AWS Key Management Service (AWS KMS). Change the settings on the S3 bucket to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Turn on versioning for the S3 bucket.
- D. Navigate to Amazon S3 in the AWS Management Console. Browse the S3 bucket's objects. Sort by the encryption field. Select each unencrypted object. Use the Modify button to apply default encryption settings to every unencrypted object in the S3 bucket.

Correct Answer: B

Community vote distribution

B (86%) 11%

 **Parsons**  10 months, 2 weeks ago

Selected Answer: B

Step 1: S3 inventory to get object list
 Step 2 (If needed): Use S3 Select to filter
 Step 3: S3 object operations to encrypt the unencrypted objects.

On the going object use default encryption.

upvoted 11 times

 **Parsons** 10 months, 2 weeks ago

Useful ref link: <https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>
 upvoted 8 times

 **cookieMr**  5 months ago

Selected Answer: B

By enabling default encryption settings on the S3, all newly added objects will be automatically encrypted. To encrypt the existing objects, the S3 Inventory feature can be used to generate a list of unencrypted objects. Then, an S3 Batch Operations job can be executed to copy those objects while applying encryption.

A. This solution involves creating a new S3 and manually downloading and uploading all existing objects. It requires significant effort and time to transfer millions of objects, making it a less efficient solution.

C. While enabling SSE with AWS KMS is a valid approach to encrypt objects in an S3, it does not address the requirement of encrypting existing objects. It only applies encryption to new objects added to the bucket.

D. Manually modifying each object in the S3 to apply default encryption settings is a labor-intensive and error-prone process. It would require individually selecting and modifying each unencrypted object, which is impractical for a large number of objects.

upvoted 5 times

 **CapJackSparrow**  8 months, 2 weeks ago

Selected Answer: B

B...

<https://catalog.us-east-1.prod.workshops.aws/workshops/05f16f1a-0bbf-45a7-a304-4fcf7fca3d1f/en-US/s3-track/module-2>

You're welcome

upvoted 3 times

 **bdp123** 9 months, 2 weeks ago

Selected Answer: B

Amazon S3 now configures default encryption on all existing unencrypted buckets to apply server-side encryption with S3 managed keys (SSE-S3) as the base level of encryption for new objects uploaded to these buckets. Objects that are already in an existing unencrypted bucket won't be

automatically encrypted.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-encryption-faq.html>

upvoted 3 times

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

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-copy-example-bucket-key.html>

upvoted 1 times

✉ **aakashkumar1999** 9 months, 4 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

✉ **Val182** 9 months, 4 weeks ago

Selected Answer: B

B 100%

<https://spin.atomicobject.com/2020/09/15/aws-s3-encrypt-existing-objects/>

upvoted 1 times

✉ **LuckyAro** 10 months ago

Selected Answer: A

Why is no one discussing A ? I think A can also achieve the required results. B is the most appropriate answer though.

upvoted 1 times

✉ **Training4aBetterLife** 10 months, 1 week ago

Selected Answer: B

S3 provides a single control to automatically encrypt all new objects in a bucket with SSE-S3 or SSE-KMS. Unfortunately, these controls only affect new objects. If your bucket already contains millions of unencrypted objects, then turning on automatic encryption does not make your bucket secure as the unencrypted objects remain.

For S3 buckets with a large number of objects (millions to billions), use Amazon S3 Inventory to get a list of the unencrypted objects, and Amazon S3 Batch Operations to encrypt the large number of old, unencrypted files.

upvoted 3 times

✉ **Training4aBetterLife** 10 months, 1 week ago

Versioning:

When you overwrite an S3 object, it results in a new object version in the bucket. However, this will not remove the old unencrypted versions of the object. If you do not delete the old version of your newly encrypted objects, you will be charged for the storage of both versions of the objects.

S3 Lifecycle

If you want to remove these unencrypted versions, use S3 Lifecycle to expire previous versions of objects. When you add a Lifecycle configuration to a bucket, the configuration rules apply to both existing objects and objects added later. C is missing this step, which I believe is what makes B the better choice. B includes the functionality of encrypting the old unencrypted objects via Batch Operations, whereas, Versioning does not address the old unencrypted objects.

upvoted 1 times

✉ **Training4aBetterLife** 10 months, 1 week ago

S3 provides a single control to automatically encrypt all new objects in a bucket with SSE-S3 or SSE-KMS. Unfortunately, these controls only affect new objects. If your bucket already contains millions of unencrypted objects, then turning on automatic encryption does not make your bucket secure as the unencrypted objects remain.

For S3 buckets with a large number of objects (millions to billions), use Amazon S3 Inventory to get a list of the unencrypted objects, and Amazon S3 Batch Operations to encrypt the large number of old, unencrypted files.

upvoted 1 times

✉ **Training4aBetterLife** 10 months, 1 week ago

Versioning:

When you overwrite an S3 object, it results in a new object version in the bucket. However, this will not remove the old unencrypted versions of the object. If you do not delete the old version of your newly encrypted objects, you will be charged for the storage of both versions of the objects.

S3 Lifecycle

If you want to remove these unencrypted versions, use S3 Lifecycle to expire previous versions of objects. When you add a Lifecycle configuration to a bucket, the configuration rules apply to both existing objects and objects added later. C is missing this step, which I believe is what makes B the better choice. B includes the functionality of encrypting the old unencrypted objects via Batch Operations, whereas, Versioning does not address the old unencrypted objects.

upvoted 1 times

✉ **Training4aBetterLife** 10 months, 1 week ago

Please remove duplicate response as I was meaning to submit a voting comment.

upvoted 1 times

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

Selected Answer: B

C is wrong. Even though you turn on the SSE-KMS with a new key, the existing objects are still yet to be encrypted. They still need to be manually encrypted by AWS batch

upvoted 1 times

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

Selected Answer: B

<https://spin.atomicobject.com/2020/09/15/aws-s3-encrypt-existing-objects/>

upvoted 1 times

✉  **Aninina** 10 months, 2 weeks ago

Selected Answer: C

C is the answer

upvoted 1 times

✉  **techhb** 10 months, 2 weeks ago

Selected Answer: B

Agree with Parsons

upvoted 1 times

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

the answer is C

also, the questions require future encryption of the objects is the S3 bucket = VERSIONING

upvoted 1 times

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

Selected Answer: C

could not open default encrypton for exist bucket,so need to use KMS

upvoted 1 times

✉  **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C

The correct answer is C

upvoted 1 times

A company runs a global web application on Amazon EC2 instances behind an Application Load Balancer. The application stores data in Amazon Aurora. The company needs to create a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss. The solution does not need to handle the load when the primary infrastructure is healthy.

What should a solutions architect do to meet these requirements?

- A. Deploy the application with the required infrastructure elements in place. Use Amazon Route 53 to configure active-passive failover. Create an Aurora Replica in a second AWS Region.
- B. Host a scaled-down deployment of the application in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora Replica in the second Region.
- C. Replicate the primary infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora database that is restored from the latest snapshot.
- D. Back up data with AWS Backup. Use the backup to create the required infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-passive failover. Create an Aurora second primary instance in the second Region.

Correct Answer: D

Community vote distribution

A (73%)

D (27%)

 **Parsons** Highly Voted 10 months, 2 weeks ago

Selected Answer: A

A is correct.

- "The solution does not need to handle the load when the primary infrastructure is healthy." => Should use Route 53 Active-Passive ==> Exclude B, C

- D is incorrect because "Create an Aurora second primary instance in the second Region.", we need to create an Aurora Replica enough.
upvoted 20 times

 **Parsons** 10 months, 2 weeks ago

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

upvoted 4 times

 **diabloexodia** Highly Voted 4 months, 1 week ago

Selected Answer: A

Anything that is not instant recovery is active - passive.

In active -passive we have :

1. Aws Backup(least op overhead) - RTO/RPO = hours
2. Pilot Light (Basic Infra is already deployed, but needs to be fully implemented) -RTO/RPO = 10's of minutes.
3. Warm Standby- (Basic infra + runs small loads (might need to add auto scaling) -RTO/RPO= minutes
4. (ACTIVE -ACTIVE) : Multi AZ option : instant

here we can tolerate 30 mins

hence B,D are incorrect. AWS backup is in hours, hence D is incorrect .

therefore A

upvoted 10 times

 **Jeffab** Most Recent 1 month ago

If this is the quality of the questions in exam, then we are all screwed! I don't think any options are correct. A probably the most correct, but a big flaw. "Deploy the application with the required infrastructure elements in place." Deploy to where? Fair enough if you assume another region/AZ, but it's not stated and only Aurora replica is mentioned, not the Web/app servers etc.

upvoted 5 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: A

'Can tolerate up to 30 minutes of downtime and potential data loss' rules out any option with 'active-active'. Leaves D and A. D is convoluted. Leaving A.

upvoted 2 times

 **cookieMr** 5 months ago

Selected Answer: A

A. involves deploying the application and infrastructure elements in the primary Region. An Aurora Replica is created in a second Region to serve as the standby database. Route 53 is configured with active-passive failover, directing traffic to the primary Region by default. In the event of a disaster, Route 53 can automatically redirect traffic to the standby Region, minimizing downtime. Data loss may occur up to the point of the last replication to the standby Region, which can be within the defined tolerance of 30 minutes.

Option B, is not necessary in this case as the solution does not need to handle the load when the primary infrastructure is healthy, and it may involve higher complexity and costs.

Option C, may introduce additional complexity and potential data loss, as the standby database might not be up-to-date with the primary database.

Option D, may be suitable for backup and recovery scenarios but may not provide the required failover and downtime tolerance specified in the requirements.

upvoted 2 times

✉ **antropaws** 5 months, 3 weeks ago

Selected Answer: D

I vote D, because option A is not highly available. In option A, you can't configure active-passive failover because you haven't created a backup infrastructure.

upvoted 1 times

✉ **kraken21** 8 months ago

Selected Answer: A

It is a cross region DR strategy. You need a read replica and Application in another region to have a realistic DR option. The read replica will take few minutes to promote/Active and the application is available. Option D lacks clarity on application and Backups can take time to restore.

upvoted 2 times

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

Selected Answer: A

Depending on the Regions involved and the amount of data to be copied, a cross-Region snapshot copy can take hours to complete and will be a factor to consider for the RPO requirements. You need to take this into account when you estimate the RPO of this DR strategy.

If you have strict RTO and RPO requirements, you should consider a different DR strategy, such as Amazon Aurora Global Database .
<https://aws.amazon.com/blogs/database/cost-effective-disaster-recovery-for-amazon-aurora-databases-using-aws-backup/>

upvoted 1 times

✉ **JiyuKim** 9 months, 3 weeks ago

Selected Answer: D

The solution does not need to handle the load when the primary infrastructure is healthy. -> Amazon Route 53 active-passive failover -> A,D
The company can tolerate up to 30 minutes of downtime and potential data loss -> backup -> D
you don't have to use read replicas if you can tolerate downtime and data loss.

upvoted 3 times

✉ **ChrisG1454** 9 months, 2 weeks ago

Consider Answer B.

It is suggesting a Pilot Light DR strategy.

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

upvoted 2 times

✉ **Bofi** 9 months ago

I will Vote B and i initially thought it Pilot Light however after 2nd read, it seem it more like warm standby. Option D looks more like back up and Restore strategy and it will take more than 30 minutes to get it done. C is wrong, snapshot takes longer time to restore

upvoted 1 times

✉ **ChrisG1454** 9 months ago

The key sentence is

"a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss"

Take a look at the visualization in the URL provided. Pilot light = 30 minutes.

upvoted 2 times

✉ **aakashkumar1999** 9 months, 4 weeks ago

Selected Answer: D

I am confused within A and D but I think D is the answer because this seems to be a cost related problem, a replica is kind of a standby and you can promote to be the main db anytime without any much downtime, but here it says it can withstand 30 mins of downtime so we can just keep a backup of the instance and then create a DB whenever required from the backup, hence less cost

upvoted 10 times

✉ **Aninina** 10 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

✉ **gunmin** 10 months, 2 weeks ago

Selected Answer: A

aaaaaaaaa

upvoted 1 times

✉ **mhmt4438** 10 months, 2 weeks ago

Selected Answer: A

answer is d
upvoted 1 times

 **alanp** 10 months, 2 weeks ago

Ans is A
upvoted 1 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: A

A is correct answer.

<https://www.examtopics.com/discussions/amazon/view/81439-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/81439-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address. The default security group is assigned to the EC2 instance. The default network ACL has been modified to block all traffic. A solutions architect needs to make the web server accessible from everywhere on port 443.

Which combination of steps will accomplish this task? (Choose two.)

- A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
- B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.
- C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.
- D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
- E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

Correct Answer: AE

Community vote distribution

AE (83%) AC (17%)

 **Parsons** Highly Voted 10 months, 2 weeks ago

Selected Answer: AE

A, E is perfect the combination. To be more precise, We should add outbound with "outbound TCP port 32768-65535 to destination 0.0.0.0/0." as an ephemeral port due to the stateless of NACL.

upvoted 9 times

 **MohammadTofic8787** 2 months, 1 week ago

i Think AD because acl is stateless we must open the port outbound and inbound , in option E we only open 443 on inbound
upvoted 1 times

 **MohammadTofic8787** 2 months, 1 week ago

i Think AD because acl is stateless we must open the port outbound and inbound , in option c we only open 443 on inbound
upvoted 1 times

 **oguzbeliren** 3 months, 3 weeks ago

What is the main reason that you are using the TCP port 32768-65535> In the question, it doesn't ask you any requirement about it.
upvoted 3 times

 **Kaoru** Most Recent 1 week, 3 days ago

Selected Answer: AC

For typical web server scenarios, such as serving content over HTTPS (port 443), you generally do not need to explicitly open outbound ports in the network ACL (NACL) for the return traffic.

upvoted 1 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: AE

ACL is stateless. you have to define both inbound and outbound rules.

upvoted 2 times

 **MohammadTofic8787** 2 months, 1 week ago

i Think AD because acl is stateless we must open the port outbound and inbound , in option c we only open 443 on inbound
upvoted 2 times

 **MohammadTofic8787** 2 months, 1 week ago

please admin delete this , sorry
upvoted 1 times

 **MohammadTofic8787** 2 months, 1 week ago

i Think AD because acl is stateless we must open the port outbound and inbound , in option D we only open 443 on inbound
upvoted 1 times

please admin delete this , sorry

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: AE

A, E is perfect the combination. To be more precise, We should add outbound with "outbound TCP port 32768-65535 to destination 0.0.0.0/0." as an ephemeral port due to the stateless of NACL.

upvoted 2 times

 **beginnercloud** 3 months ago

Selected Answer: AE

AE is the best answer here, but in reality, E is not good enough. Here, it says that the client chooses the ephemeral port, and it can start from 1024. Only Linux clients have the range starting at 32768 <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports> Unless the destination advertises the ephemeral ports, which I don't think is the case

upvoted 1 times

 **Thornessen** 4 months, 1 week ago

Selected Answer: AE

AE is the best answer here, but in reality, E is not good enough.

Here, it says that the client chooses the ephemeral port, and it can start from 1024. Only Linux clients have the range starting at 32768 <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports>

Unless the destination advertises the ephemeral ports, which I don't think is the case

upvoted 2 times

 **Abrar2022** 6 months ago

32768-65535 ports Allows outbound IPv4 responses to clients on the internet (for example, serving webpages to people visiting the web servers in the subnet).

upvoted 1 times

 **Whericanstart** 8 months, 3 weeks ago

Selected Answer: AE

NACL blocks outgoing traffic since it is infact stateless..Option E allows outbound traffic from ephemeral ports going outside of the VPC back to the web.

upvoted 2 times

 **Brak** 8 months, 3 weeks ago

It can't be C, since the current NACL blocks all traffic, including outbound. Need to allow outbound traffic through the NACL.
But E is a bad answer, since ephemeral ports start at 1024, not 32768.

upvoted 1 times

 **neosis91** 9 months, 3 weeks ago

Selected Answer: AC

A and C not E

Option E states to allow incoming TCP ports on 443 and outgoing on 32768-65535 to all IP addresses (0.0.0.0/0). This option only allows outgoing ports and does not guarantee that incoming connections on 443 will be allowed. It does not meet the requirement of making the web server accessible on port 443 from anywhere. Therefore, option C which states to allow incoming TCP ports on 443 from all IP addresses is the best answer to meet the requirements.

upvoted 4 times

 **slackbot** 3 months ago

seems like either you did not read what you wrote "Option E states to allow incoming TCP ports on 443 and outgoing on 32768-65535 to all IP addresses (0.0.0.0/0)." (because first part of the sentence allows incoming 443) or you do not understand how ACLs work - they are STATELESS, which means, you need to allow both IN and OUT, not just IN like SGs which are stateful. if they were the same - what would be the purpose of the ACLs?

upvoted 1 times

 **JoeGuan** 3 months, 1 week ago

It seems there are lots of questions that ask for minimum requirements, and often times adding 'things' to the solution are not correct. I am not sure about this question and I would pick C. E adds ambiguity. What if you only needed to open ports for Lambda? That would be a different set of ports. I think E adds some assumptions into the question. I think opening some ports for some assumptions and keeping ports closed for other assumptions is not correct. The best assumption is to assume they are asking how to open ports for 443

upvoted 1 times

 **slackbot** 3 months ago

E still guarantees something will work. C definitely means - nothing will work, because you are not allowing egress traffic at all
upvoted 1 times

 **Deepak_k** 9 months, 1 week ago

Answer : AE - Incoming traffic on port 443 but sever can use any port to reply back.

upvoted 2 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: AE

AE correct

upvoted 3 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: AE

A & E , E as NACL is stateless.

upvoted 2 times

 **AHUI** 10 months, 2 weeks ago

AE:

<https://www.examtopics.com/discussions/amazon/view/29767-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: AE

<https://www.examtopics.com/discussions/amazon/view/29767-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **kbaruu** 10 months, 2 weeks ago

Selected Answer: AE

A E is correct

upvoted 1 times

 **alanp** 10 months, 2 weeks ago

Ans AE

upvoted 1 times

A company's application is having performance issues. The application is stateful and needs to complete in-memory tasks on Amazon EC2 instances. The company used AWS CloudFormation to deploy infrastructure and used the M5 EC2 instance family. As traffic increased, the application performance degraded. Users are reporting delays when the users attempt to access the application.

Which solution will resolve these issues in the MOST operationally efficient way?

- A. Replace the EC2 instances with T3 EC2 instances that run in an Auto Scaling group. Make the changes by using the AWS Management Console.
- B. Modify the CloudFormation templates to run the EC2 instances in an Auto Scaling group. Increase the desired capacity and the maximum capacity of the Auto Scaling group manually when an increase is necessary.
- C. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Use Amazon CloudWatch built-in EC2 memory metrics to track the application performance for future capacity planning.
- D. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Deploy the Amazon CloudWatch agent on the EC2 instances to generate custom application latency metrics for future capacity planning.

Correct Answer: D

Community vote distribution

D (100%)

 **Parsons**  10 months, 2 weeks ago

Selected Answer: D

D is the correct answer.

"in-memory tasks" => need the "R" EC2 instance type to archive memory optimization. So we are concerned about C & D. Because EC2 instances don't have built-in memory metrics to CW by default. As a result, we have to install the CW agent to archive the purpose.
upvoted 21 times

 **Babba**  10 months, 2 weeks ago

Selected Answer: D

It's D, EC2 do not provide by default memory metrics to CloudWatch and require the CloudWatch Agent to be installed on the monitored instances : <https://aws.amazon.com/premiumsupport/knowledge-center/cloudwatch-memory-metrics-ec2/>
upvoted 6 times

 **Guru4Cloud**  2 months, 2 weeks ago

Selected Answer: D

R5 instances are better optimized for the in-memory workload than M5.
Auto Scaling alone doesn't handle stateful applications well, manual capacity adjustments would still be needed.
Custom latency metrics give better visibility than built-in metrics for capacity planning.

upvoted 2 times

 **cookieMr** 5 months ago

Selected Answer: D

By replacing the M5 instances with R5 instances, which are optimized for memory-intensive workloads, the application can benefit from increased memory capacity and performance.

In addition, deploying the CloudWatch agent on the EC2 instances allows for the generation of custom application latency metrics, which can provide valuable insights into the application's performance.

This solution addresses the performance issues efficiently by leveraging the appropriate instance types and collecting custom application metrics for better monitoring and future capacity planning.

- A. Replacing with T3 instances may not provide enough memory capacity for in-memory tasks.
- B. Manually increasing the capacity of the ASG does not directly address the performance issues.
- C. Relying solely on built-in EC2 memory metrics may not provide enough granularity for optimizing in-memory tasks.

The most efficient solution is to modify the CloudFormation templates, replace with R5 instances, and deploy the CloudWatch agent for custom metrics.

upvoted 3 times

 **Bmarodi** 6 months, 1 week ago

Selected Answer: D

Option D is the correct answer.

upvoted 1 times

 **BABU97** 8 months ago

will go for C

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: D

Would go with D

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: D

I think D

upvoted 1 times

A solutions architect is designing a new API using Amazon API Gateway that will receive requests from users. The volume of requests is highly variable; several hours can pass without receiving a single request. The data processing will take place asynchronously, but should be completed within a few seconds after a request is made.

Which compute service should the solutions architect have the API invoke to deliver the requirements at the lowest cost?

- A. An AWS Glue job
- B. An AWS Lambda function
- C. A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)
- D. A containerized service hosted in Amazon ECS with Amazon EC2

Correct Answer: B*Community vote distribution*

B (94%)	6%
---------	----

✉️  **Parsons** Highly Voted 10 months, 2 weeks ago

Selected Answer: B

B is the correct answer.
API Gateway + Lambda is the perfect solution for modern applications with serverless architecture.

upvoted 6 times

✉️  **TariqKipkemei** Most Recent 2 months, 1 week ago

Selected Answer: B

data processing should be completed within a few seconds = An AWS Lambda function
upvoted 1 times

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

Selected Answer: B

B. An AWS Lambda function
upvoted 1 times

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

Selected Answer: D

lambda is expensive than running ECS on EC2
upvoted 1 times

✉️  **Undisputed** 4 months ago

Selected Answer: B

Lambda all the way.
upvoted 1 times

✉️  **cookieMr** 5 months ago

Selected Answer: B

Lambda is a serverless compute service that can be triggered by API Gateway to process requests asynchronously. It automatically scales based on the incoming request volume and allows for cost optimization by charging only for the actual compute time used to process the requests.

- A. Glue is a fully managed ETL service. It is designed for data processing and transformation tasks rather than serving API requests. It may not be suitable for handling variable request volumes and delivering responses within a few seconds.
- C. While EKS provides scalability and flexibility, it may introduce additional complexity and overhead for managing and scaling the infrastructure for handling variable API request volumes.
- D. Similar to the previous option, using ECS with EC2 would require additional effort for infrastructure management and scaling, which may not be necessary for handling intermittent and variable API request volumes.
upvoted 2 times

✉️  **Bmarodi** 6 months, 1 week ago

Selected Answer: B

Option B meets the requirements.
upvoted 1 times

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

Selected Answer: B

Lambda !

upvoted 3 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/43780-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company runs an application on a group of Amazon Linux EC2 instances. For compliance reasons, the company must retain all application log files for 7 years. The log files will be analyzed by a reporting tool that must be able to access all the files concurrently.

Which storage solution meets these requirements MOST cost-effectively?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon EC2 instance store
- D. Amazon S3

Correct Answer: D

Community vote distribution

D (100%)

 **Ruffyit** 1 week, 2 days ago

A. EBS provides block-level storage volumes for use with EC2 instances. While it offers durability and persistence, it is not the most cost-effective solution for long-term retention of log files. Additionally, it does not provide concurrent access to the files, which is a requirement in this scenario.

B. EFS is a scalable file storage service that can be mounted on multiple EC2 instances concurrently. While it provides concurrent access to files, it may not be the most cost-effective option for long-term retention due to its higher pricing compared to S3.

C. The instance store is a temporary storage option that is physically attached to the EC2 instance. It does not provide the durability and long-term retention required for compliance purposes. Additionally, the instance store is not accessible outside of the specific EC2 instance it is attached to, so concurrent access by the reporting tool would not be possible.

upvoted 1 times

 **Chiquitabandita** 1 month, 4 weeks ago

this sounds like an expensive solution but if necessary then S3 would be the best

upvoted 1 times

 **TariqKipkemei** 2 months, 1 week ago

most cost effective = Amazon S3

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

D. Amazon S3

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: D

A. EBS provides block-level storage volumes for use with EC2 instances. While it offers durability and persistence, it is not the most cost-effective solution for long-term retention of log files. Additionally, it does not provide concurrent access to the files, which is a requirement in this scenario.

B. EFS is a scalable file storage service that can be mounted on multiple EC2 instances concurrently. While it provides concurrent access to files, it may not be the most cost-effective option for long-term retention due to its higher pricing compared to S3.

C. The instance store is a temporary storage option that is physically attached to the EC2 instance. It does not provide the durability and long-term retention required for compliance purposes. Additionally, the instance store is not accessible outside of the specific EC2 instance it is attached to, so concurrent access by the reporting tool would not be possible.

Therefore, considering the requirements for long-term retention, concurrent access, and cost-effectiveness, S3 is the most suitable and cost-effective storage solution.

upvoted 4 times

 **kapit** 5 months, 1 week ago

s3<efs<ebs

upvoted 1 times

 **Iconique** 2 months ago

actually S3 < EBS < EFS, but for EBS you need to pay for the underlying provisioned GB.

If you compare 1 GB then S3 < EBS < EFS but if you have 100GB storage for EBS than EBS is more expensive.

upvoted 1 times

 **mattcl** 5 months, 2 weeks ago

"The log files will be analyzed by a reporting tool that must be able to access all the files concurrently" , so you need to access concurrently to get the logs. So is EFS. Letter B

upvoted 1 times

 **northyork** 5 months, 3 weeks ago

<https://aws.amazon.com/efs/faq/>

EFS is a file storage service for use with Amazon compute (EC2, containers, serverless) and on-premises servers. EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently accessible storage for up to thousands of EC2 instances.

upvoted 1 times

 **alexandercamachop** 6 months, 2 weeks ago

Selected Answer: D

Whenever we see long time storage and no special requirements that needs EFS or FSx, then S3 is the way.

upvoted 2 times

 **elearningtakai** 8 months ago

Selected Answer: D

To meet the requirements of retaining application log files for 7 years and allowing concurrent access by a reporting tool, while also being cost-effective, the recommended storage solution would be D: Amazon S3.

upvoted 2 times

 **osmk** 8 months ago

ddddddddddddd

upvoted 2 times

 **udo2020** 8 months, 1 week ago

What about the keyword "concurrently"? Doesn't this mean EFS?

upvoted 3 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: D

Cost Effective: S3

upvoted 2 times

 **Parsons** 10 months, 2 weeks ago

Selected Answer: D

S3 is enough with the lowest cost perspective.

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/22182-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

A company has hired an external vendor to perform work in the company's AWS account. The vendor uses an automated tool that is hosted in an AWS account that the vendor owns. The vendor does not have IAM access to the company's AWS account.

How should a solutions architect grant this access to the vendor?

- A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.
- B. Create an IAM user in the company's account with a password that meets the password complexity requirements. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.
- C. Create an IAM group in the company's account. Add the tool's IAM user from the vendor account to the group. Attach the appropriate IAM policies to the group for the permissions that the vendor requires.
- D. Create a new identity provider by choosing "AWS account" as the provider type in the IAM console. Supply the vendor's AWS account ID and user name. Attach the appropriate IAM policies to the new provider for the permissions that the vendor requires.

Correct Answer: A

Community vote distribution

A (86%) 9%

 **mp165**  10 months, 2 weeks ago

Selected Answer: A

A is proper

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html
upvoted 7 times

 **Ruffyt**  1 week, 2 days ago

Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires
upvoted 1 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: A

Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires
upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.
upvoted 1 times

 **cookieMr** 5 months ago

By creating an IAM role and delegating access to the vendor's IAM role, you establish a trust relationship between accounts. This allows the vendor's automated tool to assume the role in the company's account and access the necessary resources.

By attaching the appropriate IAM policies to the role, you can define the precise permissions that the vendor requires for their tool to perform its tasks. This ensures that the vendor has the necessary access without granting them direct IAM access to the company's account.

B is incorrect because creating an IAM user with a password would require sharing the credentials with the vendor, which is not recommended for security reasons.

C is incorrect because adding the vendor's IAM user to an IAM group in the company's account would not provide a direct and controlled way to delegate access to the vendor's tool.

D is incorrect because creating a new identity provider for the vendor's AWS account would not provide a straightforward way to delegate access to the vendor's tool. Identity providers are typically used for federated access using external identity systems.
upvoted 3 times

 **teja54** 6 months ago

Selected Answer: C

.....

upvoted 1 times

 **Bmarodi** 6 months ago

Selected Answer: A

Option A fulfill the requirements.

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: A

IAM role is the answer

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: A

A is correct answer.

upvoted 1 times

 **kbaruu** 10 months, 2 weeks ago

Selected Answer: A

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

upvoted 2 times

 **venice1234** 10 months, 2 weeks ago

Selected Answer: A

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

upvoted 2 times

 **Parsons** 10 months, 2 weeks ago

Selected Answer: A

A is the correct answer.

upvoted 3 times

 **Babba** 10 months, 2 weeks ago

Selected Answer: D

My guess is D: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

upvoted 2 times

A company has deployed a Java Spring Boot application as a pod that runs on Amazon Elastic Kubernetes Service (Amazon EKS) in private subnets. The application needs to write data to an Amazon DynamoDB table. A solutions architect must ensure that the application can interact with the DynamoDB table without exposing traffic to the internet.

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

- A. Attach an IAM role that has sufficient privileges to the EKS pod.
- B. Attach an IAM user that has sufficient privileges to the EKS pod.
- C. Allow outbound connectivity to the DynamoDB table through the private subnets' network ACLs.
- D. Create a VPC endpoint for DynamoDB.
- E. Embed the access keys in the Java Spring Boot code.

Correct Answer: AD

Community vote distribution

AD (100%)

 **Ruffyit** 1 week, 1 day ago

The application needs to write data to an Amazon DynamoDB table = Attach an IAM role that has write privileges to the EKS pod
Without exposing traffic to the internet = VPC endpoint for DynamoDB
upvoted 1 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: AD

The application needs to write data to an Amazon DynamoDB table = Attach an IAM role that has write privileges to the EKS pod
Without exposing traffic to the internet = VPC endpoint for DynamoDB
upvoted 2 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: AD

A. By attaching an IAM role to the EKS pod, you can grant the necessary permissions for the pod to access DynamoDB. The IAM role should have appropriate policies allowing access to the DynamoDB table.

D. Creating a VPC endpoint for DynamoDB allows the EKS pod to access DynamoDB privately within the VPC, without the need for internet connectivity. The VPC endpoint provides a direct and secure connection to DynamoDB, eliminating the need for traffic to flow over the internet.
upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: AD

A. By attaching an IAM role to the EKS pod, you can grant the necessary permissions for the pod to access DynamoDB. The IAM role should have appropriate policies allowing access to the DynamoDB table.

D. Creating a VPC endpoint for DynamoDB allows the EKS pod to access DynamoDB privately within the VPC, without the need for internet connectivity. The VPC endpoint provides a direct and secure connection to DynamoDB, eliminating the need for traffic to flow over the internet.

B is incorrect because attaching an IAM user to the pod is not a recommended approach. IAM users are meant for accessing AWS services through the AWS Management Console or API.

C is incorrect because configuring outbound connectivity through network ACLs would not provide a secure and direct connection to DynamoDB.

E is incorrect because embedding access keys in the code is not a recommended security practice. It can lead to potential security vulnerabilities. It is better to use IAM roles or other secure mechanisms for providing access to AWS services.

upvoted 2 times

 **Bmarodi** 6 months ago

Selected Answer: AD

A & D options fulfill the requirements.
upvoted 1 times

 **LuckyAro** 10 months, 2 weeks ago

Selected Answer: AD

Definitely
upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: AD

A D are the correct options

upvoted 1 times

 **venice1234** 10 months, 2 weeks ago

Selected Answer: AD

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

<https://aws.amazon.com/about-aws/whats-new/2019/09/amazon-eks-adds-support-to-assign-iam-permissions-to-kubernetes-service-accounts/>

upvoted 2 times

 **Parsons** 10 months, 2 weeks ago

Selected Answer: AD

A, D is the correct answer.

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: AD

The correct answer is A,D

upvoted 1 times

A company recently migrated its web application to AWS by rehosting the application on Amazon EC2 instances in a single AWS Region. The company wants to redesign its application architecture to be highly available and fault tolerant. Traffic must reach all running EC2 instances randomly.

Which combination of steps should the company take to meet these requirements? (Choose two.)

- A. Create an Amazon Route 53 failover routing policy.
- B. Create an Amazon Route 53 weighted routing policy.
- C. Create an Amazon Route 53 multivalue answer routing policy.
- D. Launch three EC2 instances: two instances in one Availability Zone and one instance in another Availability Zone.
- E. Launch four EC2 instances: two instances in one Availability Zone and two instances in another Availability Zone.

Correct Answer: CE

Community vote distribution

CE (61%)

BE (39%)

 **cookieMr**  5 months ago

Selected Answer: CE

C. A multivalue answer routing policy in Route 53 allows you to configure multiple values for a DNS record, and Route 53 responds to DNS queries with multiple random values. This enables the distribution of traffic randomly among the available EC2 instances.

E. By launching EC2 instances in different AZs, you achieve high availability and fault tolerance. Launching four instances (two in each AZ) ensures that there are enough resources to handle the traffic load and maintain the desired level of availability.

A. Failover routing is designed to direct traffic to a backup resource or secondary location only when the primary resource or location is unavailable.

B. Although a weighted routing policy allows you to distribute traffic across multiple EC2 instances, it does not ensure random distribution.

D. While launching instances in multiple AZs is important for fault tolerance, having only three instances does not provide an even distribution of traffic. With only three instances, the traffic may not be evenly distributed, potentially leading to imbalanced resource utilization.

upvoted 8 times

 **Steve_4542636**  9 months ago

Selected Answer: BE

I went back and rewatched the lectures from Udemy on Weighted and Multi-Value. The lecturer said that Multi-value is *not* as substitute for ELB and he stated that DNS load balancing is a good use case for Weighted routing policies

upvoted 8 times

 **smartegnine** 5 months, 3 weeks ago

Weighted routing based on weight assigned, it can not do randomly choose, please see last sentence of the question choose randomly.

upvoted 7 times

 **Ruffyit**  1 week, 1 day ago

C. A multivalue answer routing policy in Route 53 allows you to configure multiple values for a DNS record, and Route 53 responds to DNS queries with multiple random values. This enables the distribution of traffic randomly among the available EC2 instances.

E. By launching EC2 instances in different AZs, you achieve high availability and fault tolerance. Launching four instances (two in each AZ) ensures that there are enough resources to handle the traffic load and maintain the desired level of availability.

A. Failover routing is designed to direct traffic to a backup resource or secondary location only when the primary resource or location is unavailable.

B. Although a weighted routing policy allows you to distribute traffic across multiple EC2 instances, it does not ensure random distribution.

upvoted 1 times

 **mohamoha** 3 weeks ago

First I thought it was weighted but after research C is the correct answer :

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

upvoted 1 times

 **daniel33** 1 month, 3 weeks ago

Selected Answer: CE

Multivalue routing can do random load balancing according to the AWS website:

To route traffic approximately randomly to multiple resources, such as web servers, you create one multivalue answer record for each resource and, optionally, associate a Route 53 health check with each record.

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

upvoted 3 times

✉ **Tom123456ac** 1 month, 3 weeks ago

This questions is so wired , 3 instances nothing wrong with it

upvoted 1 times

✉ **Techi47** 2 months ago

Option CE Correct:

To route traffic roughly and randomly to multiple resources, such as web servers, you create a multi-value response record for each resource and optionally associate a Route 53 health check with each record.

<https://disaster-recovery.workshop.aws/en/services/networking/route53/routing-policies/routing-multiple-answer.html>

upvoted 1 times

✉ **kwang312** 2 months, 1 week ago

Selected Answer: CE

CE is correct

upvoted 1 times

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

Selected Answer: CE

Highly available and fault tolerant = two instances in two AZs

Route traffic randomly = Amazon Route 53 multivalue answer routing policy

upvoted 1 times

✉ **LazyTs** 2 months, 3 weeks ago

Selected Answer: CE

Multivalue answer routing policy – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random. You can use multivalue answer routing to create records in a private hosted zone.

Weighted routing policy – Use to route traffic to multiple resources in proportions that you specify. You can use weighted routing to create records in a private hosted zone.

upvoted 1 times

✉ **Zeezie** 4 months ago

I chose CE, but couldn't it also be BE? If you set all of the weights to the same, equal value? Wouldn't then the traffic be distributed randomly and evenly among all healthy instances?

upvoted 1 times

✉ **jacob_ho** 2 months, 3 weeks ago

This is "equal distribution", not "random distribution"; think about the differences

upvoted 1 times

✉ **samsoft556** 5 months, 1 week ago

Selected Answer: CE

Randomly is the key word

upvoted 2 times

✉ **secdgs** 5 months, 3 weeks ago

Selected Answer: CE

C: Multi-value To route traffic approximately randomly to multiple resources and have healt check

B: Weighted default use for when you need load to one server more than ohter server. if you need for random to all server should be letter in this C options "and weight to all server with same value".

upvoted 1 times

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

Selected Answer: CE

Must C and E, B is not correct because it based on the assigned weight it can not do randomly

upvoted 1 times

✉ **ChrisAn** 5 months, 3 weeks ago

Selected Answer: CE

Option C, creating an Amazon Route 53 multivalue answer routing policy, is the correct choice. With this routing policy, Route 53 returns multiple IP addresses for the same domain name, allowing the traffic to be distributed randomly among the available EC2 instances. This ensures that the traffic is evenly distributed across the instances launched in different Availability Zones, achieving the desired randomness and load balancing.

Option E is the correct choice. By launching instances in different Availability Zones, the company ensures that there are redundant copies of the application running in separate physical locations, providing fault tolerance. With two instances in one Availability Zone and two instances in another, traffic can be distributed randomly among them, improving availability and load balancing.

upvoted 1 times

 **Axeashes** 5 months, 3 weeks ago

Selected Answer: CE

<https://aws.amazon.com/route53/faqs/>

upvoted 2 times

 **Bmarodi** 6 months ago

Selected Answer: BE

I vote for B & E options.

upvoted 1 times

A media company collects and analyzes user activity data on premises. The company wants to migrate this capability to AWS. The user activity data store will continue to grow and will be petabytes in size. The company needs to build a highly available data ingestion solution that facilitates on-demand analytics of existing data and new data with SQL.

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

- A. Send activity data to an Amazon Kinesis data stream. Configure the stream to deliver the data to an Amazon S3 bucket.
- B. Send activity data to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliver the data to an Amazon Redshift cluster.
- C. Place activity data in an Amazon S3 bucket. Configure Amazon S3 to run an AWS Lambda function on the data as the data arrives in the S3 bucket.
- D. Create an ingestion service on Amazon EC2 instances that are spread across multiple Availability Zones. Configure the service to forward data to an Amazon RDS Multi-AZ database.

Correct Answer: A

Community vote distribution

B (93%) 7%

 **Ruffyit** 1 week, 1 day ago

1- Kinesis Data Stream provides a fully managed platform for custom data processing and analysis. Or we can say that used for custom data processing and analysis which required more manual intervention.
2- Kinesis Data Firehose simplifies the delivery of streaming data to various destinations without the need for complex transformations. Option B is more suitable for the given scenario.

upvoted 1 times

 **David_Ang** 1 month ago

Selected Answer: B

always if you have a service that is meant for a specific job, it the correct answer, is logic. "A" is not good enough for this situation
upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: B

B. Send activity data to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliver the data to an Amazon Redshift cluster.
upvoted 1 times

 **beginnercloud** 3 months ago

Selected Answer: B

Petabyte scale- Redshift
upvoted 4 times

 **NVenkatS** 3 months ago

Selected Answer: B

Petabyte scale- Redshift
upvoted 2 times

 **A1975** 3 months, 3 weeks ago

Selected Answer: B

1- Kinesis Data Stream provides a fully managed platform for custom data processing and analysis. Or we can say that used for custom data processing and analysis which required more manual intervention.
2- Kinesis Data Firehose simplifies the delivery of streaming data to various destinations without the need for complex transformations. Option B is more suitable for the given scenario.
upvoted 2 times

 **sickcow** 4 months, 4 weeks ago

Selected Answer: B

Petabyte Scale sounds like Redshift!
upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: B

B provides a fully managed and scalable solution for data ingestion and analytics. KDF simplifies the data ingestion process by automatically scaling to handle large volumes of streaming data. It can directly load the data into an Redshift cluster, which is a powerful and fully managed data warehousing solution.

A. While Kinesis can handle streaming data, it requires additional processing to load the data into an analytics solution.

C. Although S3 and Lambda can handle the storage and processing of data, it requires more manual configuration and management compared to the fully managed solution offered by KDF and Redshift.

D. This option involves more operational overhead, as it requires managing and scaling the EC2 instances and RDS database infrastructure manually.

Therefore, option B with KDF delivering the data to Redshift cluster offers the most streamlined and operationally efficient solution for ingesting and analyzing the user activity data in the given scenario.

upvoted 1 times

✉ **pisica134** 5 months, 1 week ago

petabytes in size => redshift

upvoted 2 times

✉ **mattcl** 5 months, 2 weeks ago

It's A. Data Stream is better in this case, and you can query data in S3 with Athena

upvoted 2 times

✉ **JoeGuan** 3 months, 1 week ago

<https://aws.amazon.com/streaming-data/> a good explanation of either option. firehose appears to be an option for Least operational overhead, as the streams product requires some building of apps etc.

upvoted 1 times

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

Data Stream Can't write to S3. That's why B is only left correct answer.

upvoted 1 times

✉ **baba365** 5 months ago

Answer A... key phrase' least operational overhead'

KDF can write to S3 ... <https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html>

upvoted 1 times

✉ **Bmarodi** 6 months ago

Selected Answer: B

Option B is correct answer.

upvoted 1 times

✉ **kruasan** 7 months ago

Selected Answer: B

This solution meets the requirements as follows:

- Kinesis Data Firehose can scale to ingest and process multiple terabytes per hour of streaming data. This can easily handle the petabyte-scale data volumes.
- Firehose can deliver the data to Redshift, a petabyte-scale data warehouse, enabling on-demand SQL analytics of the data.
- Redshift is a fully managed service, minimizing operational overhead. Firehose is also fully managed, handling scalability, availability, and durability of the streaming data ingestion.

upvoted 3 times

✉ **gold4otas** 8 months ago

Selected Answer: B

B: The answer is certainly option "B" because ingesting user activity data can easily be handled by Amazon Kinesis Data streams. The ingested data can then be sent into Redshift for Analytics.

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. Amazon Redshift Serverless lets you access and analyze data without all of the configurations of a provisioned data warehouse.

<https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html>

upvoted 2 times

✉ **GalileoEC2** 8 months, 2 weeks ago

the Key sentence here is: "that facilitates on-demand analytics", that's the reason because we need to choose Kinesis Data streams over Data Firehose

upvoted 1 times

✉ **alexleely** 10 months, 1 week ago

Selected Answer: B

B: Kinesis Data Firehose service automatically loads the data into Amazon Redshift and is a petabyte-scale data warehouse service. It allows you to perform on-demand analytics with minimal operational overhead. Since the requirement didn't state what kind of analytics you need to run, we can assume that we do not need to set up additional services to provide further analytics. Thus, it has the least operational overhead.

Why not A: It is a viable solution, but storing the data in S3 would require you to set up additional services like Amazon Redshift or Amazon Athena to perform the analytics.

upvoted 2 times

 **Berny** 10 months, 1 week ago

Selected Answer: B

Data ingestion through Kinesis data streams will require manual intervention to provide more shards as data size grows. Kinesis firehose will ingest data with the least operational overhead.

upvoted 4 times

 **mp165** 10 months, 2 weeks ago

Selected Answer: A

I think the key word in the question is "ingestion"...whish is data stream

Data Streams is a low latency streaming service in AWS Kinesis with the facility for ingesting at scale. On the other hand, Kinesis Firehose aims to serve as a data transfer service. The primary purpose of Kinesis Firehose focuses on loading streaming data to Amazon S3, Splunk, ElasticSearch, and RedShift

upvoted 3 times

A company collects data from thousands of remote devices by using a RESTful web services application that runs on an Amazon EC2 instance. The EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket. The number of remote devices will increase into the millions soon. The company needs a highly scalable solution that minimizes operational overhead.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Use AWS Glue to process the raw data in Amazon S3.
- B. Use Amazon Route 53 to route traffic to different EC2 instances.
- C. Add more EC2 instances to accommodate the increasing amount of incoming data.
- D. Send the raw data to Amazon Simple Queue Service (Amazon SQS). Use EC2 instances to process the data.
- E. Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3.

Correct Answer: AE

Community vote distribution

AE (100%)

 **Parsons** Highly Voted 10 months, 2 weeks ago

Selected Answer: AE

A, E is the correct answer

"RESTful web services" => API Gateway.

"EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket" => GLUE with (Extract - Transform - Load)

upvoted 8 times

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

A - Use AWS Glue to process the raw data in Amazon S3

E - Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3

upvoted 1 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: AE

E then A no doubt.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: AE

A. It automatically discovers the schema of the data and generates ETL code to transform it.

E. API Gateway can be used to receive the raw data from the remote devices via RESTful web services. It provides a scalable and managed infrastructure to handle the incoming requests. The data can then be sent to an Amazon Kinesis data stream, which is a highly scalable and durable real-time data streaming service. From there, Amazon Kinesis Data Firehose can be configured to use the data stream as a source and deliver the transformed data to Amazon S3. This combination of services allows for the seamless ingestion and processing of data while minimizing operational overhead.

upvoted 1 times

 **ibu007** 2 months, 3 weeks ago

Selected Answer: AE

A - Use AWS Glue to process the raw data in Amazon S3

E - Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3

upvoted 2 times

 **GCB1990** 3 months ago

Correct answer: D and E

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: AE

A. It automatically discovers the schema of the data and generates ETL code to transform it.

E. API Gateway can be used to receive the raw data from the remote devices via RESTful web services. It provides a scalable and managed infrastructure to handle the incoming requests. The data can then be sent to an Amazon Kinesis data stream, which is a highly scalable and durable real-time data streaming service. From there, Amazon Kinesis Data Firehose can be configured to use the data stream as a source and deliver the transformed data to Amazon S3. This combination of services allows for the seamless ingestion and processing of data while minimizing operational overhead.

B. It does not directly address the need for scalable data processing and storage. It focuses on managing DNS and routing traffic to different endpoints.

C. Adding more EC2 can lead to increased operational overhead in terms of managing and scaling the instances.

D. Using SQS and EC2 for processing data introduces more complexity and operational overhead.

upvoted 2 times

✉  **wRhIH** 5 months, 1 week ago

Why not BC?

upvoted 1 times

✉  **AnnieTran_91** 5 months, 2 weeks ago

Why it not CE?

Add more EC2 instances to accommodate the increasing amount of incoming data?

upvoted 1 times

✉  **TTaws** 5 months, 1 week ago

EC2 is not server-less. they want to minimize overhead

upvoted 1 times

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

Selected Answer: AE

minimizes operational overhead = Serverless

Glue, Kinesis Datastream, S3 are serverless

upvoted 1 times

✉  **KZM** 9 months, 2 weeks ago

How about "C" to increase EC2 instances for the increased devices soon?

upvoted 1 times

✉  **Aninina** 10 months, 2 weeks ago

Selected Answer: AE

Glue and API

upvoted 2 times

✉  **mhmt4438** 10 months, 2 weeks ago

Selected Answer: AE

<https://www.examtopics.com/discussions/amazon/view/83387-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company needs to retain its AWS CloudTrail logs for 3 years. The company is enforcing CloudTrail across a set of AWS accounts by using AWS Organizations from the parent account. The CloudTrail target S3 bucket is configured with S3 Versioning enabled. An S3 Lifecycle policy is in place to delete current objects after 3 years.

After the fourth year of use of the S3 bucket, the S3 bucket metrics show that the number of objects has continued to rise. However, the number of new CloudTrail logs that are delivered to the S3 bucket has remained consistent.

Which solution will delete objects that are older than 3 years in the MOST cost-effective manner?

- A. Configure the organization's centralized CloudTrail trail to expire objects after 3 years.
- B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.
- C. Create an AWS Lambda function to enumerate and delete objects from Amazon S3 that are older than 3 years.
- D. Configure the parent account as the owner of all objects that are delivered to the S3 bucket.

Correct Answer: B

Community vote distribution

B (87%) 13%

 **Ruffyit** 1 week, 1 day ago

This is the most cost-effective option because:

- Versioning has caused the number of objects to increase over time, even as current objects are deleted after 3 years. By deleting previous versions as well, this will clean up old object versions and reduce storage costs.
- An S3 Lifecycle policy incurs no additional charges and requires no additional resources to configure and run. It is a native S3 tool for managing object lifecycles cost-effectively.

upvoted 1 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: B

Ensure to delete previous versions as well.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: B

This is the most cost-effective option because:

- Versioning has caused the number of objects to increase over time, even as current objects are deleted after 3 years. By deleting previous versions as well, this will clean up old object versions and reduce storage costs.
- An S3 Lifecycle policy incurs no additional charges and requires no additional resources to configure and run. It is a native S3 tool for managing object lifecycles cost-effectively.

upvoted 2 times

 **cookieMr** 5 months ago

Selected Answer: B

By configuring the S3 Lifecycle policy to delete previous versions as well as current versions, the older versions of the CloudTrail logs will be deleted. This ensures that objects older than 3 years are removed from the S3 bucket, reducing the object count and controlling storage costs.

- A. This option is not directly related to managing objects in the S3. It focuses on configuring the expiration of CloudTrail trails, which may not address the need to delete objects from the S3 bucket.
- C. While it is technically possible to create a Lambda to delete objects older than 3 years, this approach would introduce additional complexity and operational overhead.
- D. Changing the ownership of the objects in the S3 bucket does not directly address the need to delete objects older than 3 years. Ownership does not affect the deletion behavior of the objects.

upvoted 2 times

 **Bmarodi** 6 months ago

Selected Answer: B

I go for option B.

upvoted 1 times

 **ruqui** 6 months, 1 week ago

I don't think it's possible to configure an S3 lifecycle policy to delete all versions of an object, so B is wrong ... I think the question is improperly worded

upvoted 1 times

✉ **Rahulbit34** 6 months, 4 weeks ago

- Versioning has caused the number of objects to increase over time, even as current objects are deleted after 3 years. By deleting previous versions as well, this will clean up old object versions and reduce storage costs.
- An S3 Lifecycle policy incurs no additional charges and requires no additional resources to configure and run. It is a native S3 tool for managing object lifecycles cost-effectively.

upvoted 1 times

✉ **kruasan** 7 months ago

Selected Answer: B

This is the most cost-effective option because:

- Versioning has caused the number of objects to increase over time, even as current objects are deleted after 3 years. By deleting previous versions as well, this will clean up old object versions and reduce storage costs.
- An S3 Lifecycle policy incurs no additional charges and requires no additional resources to configure and run. It is a native S3 tool for managing object lifecycles cost-effectively.

upvoted 3 times

✉ **kruasan** 7 months ago

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

upvoted 2 times

✉ **bullrem** 10 months, 1 week ago

Selected Answer: C

A more cost-effective solution would be to configure the organization's centralized CloudTrail trail to expire objects after 3 years. This would ensure that all objects, including previous versions, are deleted after the specified retention period.

Another option would be to create an AWS Lambda function to enumerate and delete objects from Amazon S3 that are older than 3 years, this would allow you to have more control over the deletion process and to write a custom logic that best fits your use case.

upvoted 3 times

✉ **JayBee65** 10 months, 1 week ago

Selected Answer: B

The question clearly says "An S3 Lifecycle policy is in place to delete current objects after 3 years". This implies that previous versions are not deleted, since this is a separate setting, and since logs are constantly changed, it would seem to make sense to delete previous versions so, so B. D is wrong, since the parent account (the management account) will already be the owner of all objects delivered to the S3 bucket, "All accounts in the organization can see MyOrganizationTrail in their list of trails, but member accounts cannot remove or modify the organization trail. Only the management account or delegated administrator account can change or delete the trail for the organization.", see <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

upvoted 2 times

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

Selected Answer: B

B is the right answer. Ref: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html#:~:text=The%20CloudTrail%20trail,time%20has%20passed.>

Option A is wrong. No way to expire the cloudtrail logs

upvoted 3 times

✉ **techhb** 10 months, 2 weeks ago

Selected Answer: B

Configure the S3 Lifecycle policy to delete previous versions

upvoted 2 times

✉ **Aninina** 10 months, 2 weeks ago

Selected Answer: B

B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.

upvoted 1 times

✉ **Aninina** 10 months, 2 weeks ago

B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.

upvoted 1 times

✉ **Parsons** 10 months, 2 weeks ago

Selected Answer: B

B is correct answer

upvoted 2 times

✉ **AHUI** 10 months, 2 weeks ago

Ans: A

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

When you create an organization trail, a trail with the name that you give it is created in every AWS account that belongs to your organization. Users with CloudTrail permissions in member accounts can see this trail when they log into the AWS CloudTrail console from their AWS accounts, or when they run AWS CLI commands such as describe-trail. However, users in member accounts do not have sufficient permissions to delete the organization trail, turn logging on or off, change what types of events are logged, or otherwise change the organization trail in any way.

upvoted 1 times

 **AHUI** 10 months, 2 weeks ago

correction: Ans D is the answer.
<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: B

B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.

To delete objects that are older than 3 years in the most cost-effective manner, the company should configure the S3 Lifecycle policy to delete previous versions as well as current versions. This will ensure that all versions of the objects, including the previous versions, are deleted after 3 years.

upvoted 1 times

A company has an API that receives real-time data from a fleet of monitoring devices. The API stores this data in an Amazon RDS DB instance for later analysis. The amount of data that the monitoring devices send to the API fluctuates. During periods of heavy traffic, the API often returns timeout errors.

After an inspection of the logs, the company determines that the database is not capable of processing the volume of write traffic that comes from the API. A solutions architect must minimize the number of connections to the database and must ensure that data is not lost during periods of heavy traffic.

Which solution will meet these requirements?

- A. Increase the size of the DB instance to an instance type that has more available memory.
- B. Modify the DB instance to be a Multi-AZ DB instance. Configure the application to write to all active RDS DB instances.
- C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.
- D. Modify the API to write incoming data to an Amazon Simple Notification Service (Amazon SNS) topic. Use an AWS Lambda function that Amazon SNS invokes to write data from the topic to the database.

Correct Answer: C

Community vote distribution

C (100%)

✉️  **Ruffyit** 1 week, 1 day ago

Decouple the API and the DB with Amazon Simple Queue Service (Amazon SQS) queue.

upvoted 1 times

✉️  **oluolope** 1 month, 1 week ago

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-lambda-function-trigger.html>
SQS can invoke lambda indeed. Initially I picked D because I wasn't sure it was possible but , this article shows it is. It makes this question even more confusing for me as it is also possible to trigger lambda from SNS:

<https://docs.aws.amazon.com/sns/latest/dg/sns-lambda-as-subscriber.html>

I don't know which option between C and D makes more sense. I still have a preference for D as it seems less hacky than C.

upvoted 1 times

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

Selected Answer: C

Decouple the API and the DB with Amazon Simple Queue Service (Amazon SQS) queue.

upvoted 1 times

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

Selected Answer: C

C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.

upvoted 1 times

✉️  **cookieMr** 5 months ago

Selected Answer: C

By leveraging SQS as a buffer and using an Lambda to process and write data from the queue to the database, the solution provides scalability, decoupling, and reliability while minimizing the number of connections to the database. This approach handles fluctuations in traffic and ensures data integrity during high-traffic periods.

A. Increasing the size of the DB instance may provide more memory, but it does not address the issue of handling high write traffic efficiently and minimizing connections to the database.

B. Modifying the DB instance to be a Multi-AZ instance and writing to all active instances can improve availability but does not address the issue of efficiently handling high write traffic and minimizing connections to the database.

D. Using SNS and an Lambda can provide decoupling and scalability, but it is not suitable for handling heavy write traffic efficiently and minimizing connections to the database.

upvoted 2 times

✉️  **Moccorso** 5 months, 1 week ago

I think D, "Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database" SQS can't invokes Lambda because SQS is pull.

upvoted 3 times

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

Why not B

upvoted 2 times

✉ **Russ99** 8 months, 2 weeks ago

C is indeed the correct answer for the use case

upvoted 1 times

✉ **kaushald** 8 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

✉ **Steve_4542636** 9 months ago

Selected Answer: C

C is correct

upvoted 1 times

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

Selected Answer: C

C looks ok

upvoted 1 times

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

why not D?

upvoted 1 times

✉ **Parsons** 10 months, 2 weeks ago

Selected Answer: C

C is correct.

upvoted 2 times

✉ **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C

C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.

To minimize the number of connections to the database and ensure that data is not lost during periods of heavy traffic, the company should modify the API to write incoming data to an Amazon SQS queue. The use of a queue will act as a buffer between the API and the database, reducing the number of connections to the database. And the use of an AWS Lambda function invoked by SQS will provide a more flexible way of handling the data and processing it. This way, the function will process the data from the queue and insert it into the database in a more controlled way.

upvoted 2 times

✉ **Aninina** 10 months, 2 weeks ago

Did you use ChatGPT?

upvoted 6 times

✉ **Nguyen25183** 9 months ago

same question as you :D

upvoted 1 times

A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.

Which solution meets these requirements?

- A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.
- B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.
- C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
- D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Correct Answer: A

Community vote distribution

A (100%)

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: A

Migrate the databases to Amazon Aurora Serverless for Aurora MySQL

upvoted 1 times

 **Undisputed** 4 months ago

Selected Answer: A

Aurora MySQL

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: A

Migrating the databases to Aurora Serverless provides automated scaling and replication capabilities. Aurora Serverless automatically scales the capacity based on the workload, allowing for seamless addition or removal of compute capacity as needed. It also offers improved performance, durability, and high availability without requiring manual management of replication and scaling.

B. Incorrect because it suggests migrating to a different database engine, which may introduce compatibility issues and require significant code modifications.

C. Incorrect because consolidating into a larger MySQL database on larger EC2 instances does not provide the desired scalability and automation.

D. Incorrect because using EC2 Auto Scaling groups for the database tier still requires manual management of replication and scaling.
upvoted 4 times

 **Bmarodi** 6 months ago

Selected Answer: A

Option A is right answer.

upvoted 1 times

 **Bhrino** 9 months, 1 week ago

Selected Answer: A

A is correct because aurora might be more expensive but its serverless and is much faster

upvoted 1 times

 **mp165** 10 months, 2 weeks ago

Selected Answer: A

A is porper

<https://aws.amazon.com/rds/aurora/serverless/>

upvoted 3 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: A

Aurora MySQL

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/51509-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application. A solutions architect wants to implement a solution that is highly available, fault tolerant, and automatically scalable.

What should the solutions architect recommend?

- A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
- B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
- C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.
- D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

Correct Answer: C

Community vote distribution

C (100%)

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: C

Highly available, fault tolerant, and automatically scalable = two NAT gateways in different Availability Zones
upvoted 2 times

 **Undisputed** 4 months ago

Selected Answer: C

Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones
upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: C

This recommendation ensures high availability and fault tolerance by distributing the NAT gateways across multiple AZs. NAT gateways are managed AWS services that provide scalable and highly available outbound NAT functionality. By deploying NAT gateways in different AZs, the company can achieve redundancy and avoid a single point of failure. This solution also provides automatic scaling to handle increasing traffic without manual intervention.

Option A is incorrect because placing both NAT gateways in the same Availability Zone does not provide fault tolerance.

Option B is incorrect because using Auto Scaling groups with Network Load Balancers is not the recommended approach for NAT instances.

Option D is incorrect because Spot Instances are not suitable for critical infrastructure components like NAT instances.
upvoted 2 times

 **Axeashes** 5 months, 3 weeks ago

Selected Answer: C

HA: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>
Scalability: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>
upvoted 1 times

 **Bhrino** 9 months, 1 week ago

Selected Answer: C

fyi yall in most cases nat instances are a bad thing because their customer managed while nat gateways are AWS Managed. So in this case I already know to get rid of the nat instances the reason its c is because it wants high availability meaning different AZs
upvoted 4 times

 **Theodorz** 9 months, 2 weeks ago

Could anybody teach me why the B cannot be correct answer? This solution also seems providing Scalability(Auto Scaling Group), High Availability(different AZ), and Fault Tolerance(NLB & AZ).

I honestly think that C is not enough, because each NAT gateway can provide a few scalability, but the bandwidth limit is clearly explained in the document. The C exactly mentioned "two NAT gateways" so the number of NAT is fixed, which will reach its limit soon.

upvoted 2 times

 **KZM** 9 months, 2 weeks ago

Option B proposes to use an Auto Scaling group with Network Load Balancers to continue using the existing two NAT instances. However, NAT instances do not support automatic failover without a script, unlike NAT gateways which provide this functionality. Additionally, using Network Load Balancers to balance traffic between NAT instances adds more complexity to the solution.

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

upvoted 2 times

 **JayBee65** 10 months, 1 week ago

C. If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html#nat-gateway-basics>

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: C
Replace NAT Instances with Gateway
upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C
Correct answer is C
upvoted 2 times

An application runs on an Amazon EC2 instance that has an Elastic IP address in VPC A. The application requires access to a database in VPC B. Both VPCs are in the same AWS account.

Which solution will provide the required access MOST securely?

- A. Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.
- B. Configure a VPC peering connection between VPC A and VPC B.
- C. Make the DB instance publicly accessible. Assign a public IP address to the DB instance.
- D. Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.

Correct Answer: B

Community vote distribution

B (83%) A (17%)

✉  **JayBee65**  10 months, 1 week ago

A is correct. B will work but is not the most secure method, since it will allow everything in VPC A to talk to everything in VPC B and vice versa, not at all secure. A on the other hand will only allow the application (since you select its IP address) to talk to the application server in VPC A - you are allowing only the required connectivity. See the link for this exact use case:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.RDSSecurityGroups.html>

upvoted 13 times

✉  **mhmt4438** 10 months ago

" allows all traffic from the public IP address" Nice bro niceee This is absolutely the most secure method at all. :))

upvoted 11 times

✉  **graveend** 3 months, 2 weeks ago

Both VPCs are in the "SAME AWS ACCOUNT" and the requirement specifies allowing traffic from the *PUBLIC IP of the APPLICATION SERVER*. In this case the traffic remains inside the AWS infrastructure or will it go through the public internet?

upvoted 2 times

✉  **datz** 7 months, 3 weeks ago

he must be the security engineer lolol :D

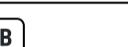
"Jaybee" - Please dont ever say that traffic over the public internet is secure :D

upvoted 3 times

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

:))))))))

upvoted 1 times

✉  **DUBURA**  6 days, 7 hours ago

Selected Answer: B

B. Configure a VPC peering connection between VPC A and VPC B.

The most secure solution is to configure a VPC peering connection between the two VPCs. This allows private communication between the application server and the database, without exposing resources to the public internet.

Option A exposes the database to the public internet by allowing inbound traffic from a public IP address.

Option C makes the database instance itself public, which is insecure.

Option D adds complexity with a proxy that is not needed when a VPC peering connection can enable private communication between VPCs.

So option B is the most secure while allowing the necessary connectivity between the application server and the database in the separate VPCs.
upvoted 1 times

✉  **Ruffyit** 1 week ago

When you establish peering relationships between VPCs across different AWS Regions, resources in the VPCs (for example, EC2 instances and Lambda functions) in different AWS Regions can communicate with each other using private IP addresses, without using a gateway, VPN connection, or network appliance. The traffic remains in the private IP space. All inter-Region traffic is encrypted with no single point of failure, or bandwidth bottleneck. Traffic always stays on the global AWS backbone, and never traverses the public internet, which reduces threats, such as common exploits, and DDoS attacks. Inter-Region VPC peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy.

upvoted 1 times

✉  **rlamberti** 1 month ago

Selected Answer: B

Most secure = not leaving AWS network.
VPC peering is the way.

upvoted 1 times

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

Selected Answer: B

VPC to VPC comms = VPC peering
upvoted 1 times

✉ **Sutariya** 2 months, 3 weeks ago

B is correct : Setup VPC peering and connect Application from VPC A to connect with VPC B in private subnet so DB instance always secure with internet.

upvoted 1 times

✉ **_d1rk_** 3 months, 1 week ago

Am I missing something or simply A is wrong because, without VPC peering (or other inter-connection sharing mechanisms such as Transit Gateway or VPN), VPC A and VPC B cannot communicate each other?

upvoted 1 times

✉ **jacob_ho** 2 months, 3 weeks ago

can use vpc endpoints but no option use that
upvoted 1 times

✉ **A1975** 3 months, 3 weeks ago

Selected Answer: B

When you establish peering relationships between VPCs across different AWS Regions, resources in the VPCs (for example, EC2 instances and Lambda functions) in different AWS Regions can communicate with each other using private IP addresses, without using a gateway, VPN connection, or network appliance. The traffic remains in the private IP space. All inter-Region traffic is encrypted with no single point of failure, or bandwidth bottleneck. Traffic always stays on the global AWS backbone, and never traverses the public internet, which reduces threats, such as common exploits, and DDoS attacks. Inter-Region VPC peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
upvoted 2 times

✉ **animefan1** 4 months, 4 weeks ago

Selected Answer: B

With peering, we EC2 can communicate with RDS. RDS SG can have inbound from EC2 IP rather than VPC CIDR for more security
upvoted 1 times

✉ **maggie135** 5 months ago

Selected Answer: B

VPC peering uses AWS network.
upvoted 1 times

✉ **cookieMr** 5 months ago

Selected Answer: B

By configuring a VPC peering connection between VPC A and VPC B, you can establish private and secure communication between the EC2 instance in VPC A and the database in VPC B. VPC peering allows traffic to flow between the two VPCs using private IP addresses, without the need for public IP addresses or exposing the database to the internet.

Option A is not the best solution as it requires allowing all traffic from the public IP address of the application server, which can be less secure.

Option C involves making the DB instance publicly accessible, which introduces security risks by exposing the database directly to the internet.

Option D adds unnecessary complexity by launching an additional EC2 instance in VPC B and proxying all requests through it, which is not the most efficient and secure approach in this scenario.

upvoted 3 times

✉ **joechen2023** 5 months, 2 weeks ago

Selected Answer: B

I don't like A because the security group setting is wrong as it set up to allow all public IP addresses. If the security group setting is correct, then I will go for A

I don't like B because it needs to set up security group as well on top of peering.
for exam purpose only, I will go with the least worst choice which is B

upvoted 1 times

✉ **Bmarodi** 5 months, 2 weeks ago

Selected Answer: A

The keywords are: "access MOST securely", hence the option A meets these requirements.
upvoted 1 times

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

Selected Answer: A

Each VPC security group rule makes it possible for a specific source to access a DB instance in a VPC that is associated with that VPC security group. The source can be a range of addresses (for example, 203.0.113.0/24), or another VPC security group.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide>

upvoted 1 times

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

Selected Answer: B

Most secure = VPC peering

upvoted 1 times

✉ **Bmarodi** 6 months ago

Selected Answer: B

I vote for option B.

upvoted 1 times

✉ **Piccalo** 6 months, 1 week ago

Selected Answer: B

BBBB. A is not secure

upvoted 1 times

A company runs demonstration environments for its customers on Amazon EC2 instances. Each environment is isolated in its own VPC. The company's operations team needs to be notified when RDP or SSH access to an environment has been established.

- A. Configure Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected.
- B. Configure the EC2 instances with an IAM instance profile that has an IAM role with the AmazonSSMManagedInstanceCore policy attached.
- C. Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state.
- D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

Correct Answer: C

Community vote distribution

C (76%)	13%	11%
---------	-----	-----

✉  **Vickysss** Highly Voted 10 months, 2 weeks ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>
upvoted 8 times

✉  **NitiATOS** 10 months ago

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#flow-log-example-accepted-rejected>

Adding this to support that VPC flow logs can be used to capture Accepted or Rejected SSH and RDP traffic.
upvoted 3 times

✉  **ruqui** 6 months ago

I don't think C would be an acceptable solution ... the request is to be notified WHEN a SSH and/or RDP connection is established so it requires real-time monitoring and that is something the C solution does not provide ... I would select A as a correct answer
upvoted 1 times

✉  **cookieMr** Highly Voted 5 months ago

Selected Answer: C

By publishing VPC flow logs to CloudWatch Logs and creating metric filters to detect RDP or SSH access, the operations team can configure an CloudWatch metric alarm to notify them when the alarm is triggered. This will provide the desired notification when RDP or SSH access to an environment is established.

Option A is incorrect because CloudWatch Application Insights is not designed for detecting RDP or SSH access.

Option B is also incorrect because configuring an IAM instance profile with the AmazonSSMManagedInstanceCore policy does not directly address the requirement of notifying the operations team when RDP or SSH access occurs.

Option D is wrong because configuring an EventBridge rule to listen for EC2 Instance State-change Notification events and using an SNS topic as a target will notify the operations team about changes in the instance state, such as starting or stopping instances. However, it does not specifically detect or notify when RDP or SSH access is established, which is the requirement stated in the question.

upvoted 7 times

✉  **Ruffyit** Most Recent 1 week ago

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#flow-log-example-accepted-rejected>

Adding this to support that VPC flow logs can be used to capture Accepted or Rejected SSH and RDP traffic.
upvoted 1 times

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

Selected Answer: C

Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state

upvoted 1 times

✉  **Bmarodi** 5 months, 2 weeks ago

Selected Answer: C

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to the following locations: Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose. After you create a flow log, you can retrieve and view the flow log records in the log group, bucket, or delivery stream that you configured.

Flow logs can help you with a number of tasks, such as:

Diagnosing overly restrictive security group rules

Monitoring the traffic that is reaching your instance

Determining the direction of the traffic to and from the network interfaces

Ref link: <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

upvoted 2 times

✉ **cokutan** 5 months, 3 weeks ago

Selected Answer: C

seems like c:

<https://aws.amazon.com/tr/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>

upvoted 1 times

✉ **ChrisAn** 5 months, 3 weeks ago

Selected Answer: D

D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic. This setup allows the EventBridge rule to capture instance state change events, such as when RDP or SSH access is established. The rule can then send notifications to the specified SNS topic, which is subscribed by the operations team.

upvoted 2 times

✉ **markw92** 5 months, 1 week ago

D is wrong. EC2 instance state change is only for pending, running etc. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-instance-state-changes.html> you can't have state change of ssh or rdp.

upvoted 1 times

✉ **datz** 7 months, 3 weeks ago

Selected Answer: C

C:

<https://www.youtube.com/watch?v=KAe3Eju59OU>

upvoted 1 times

✉ **Abhineet9148232** 9 months ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>

upvoted 1 times

✉ **bullrem** 10 months, 1 week ago

Selected Answer: A

A. Configuring Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected would be the most appropriate solution in this scenario. This would allow the operations team to be notified when RDP or SSH access has been established and provide them with the necessary information to take action if needed. Additionally, Amazon CloudWatch Application Insights would allow for monitoring and troubleshooting of the system in real-time.

upvoted 1 times

✉ **Training4aBetterLife** 10 months, 1 week ago

Selected Answer: C

EC2 Instance State-change Notifications are not the same as RDP or SSH established connection notifications. Use Amazon CloudWatch Logs to monitor SSH access to your Amazon EC2 Linux instances so that you can monitor rejected (or established) SSH connection requests and take action.

upvoted 4 times

✉ **alexleely** 10 months, 1 week ago

Selected Answer: A

The Answer can be A or C depending on the requirement if it requires real-time notification.

A: Allows the operations team to be notified in real-time when access is established, and also provides visibility into the access events through the OpsItems.

C: The logs will need to be analyzed and metric filters applied to detect access, and then the alarm will trigger based on that analysis. This method could have a delay in providing notifications. Thus, not the best solution if real-time notification is required.

Why not D: RDP or SSH access does not cause an EC2 instance to have a state change. The state change events that Amazon EventBridge can listen for include stopping, starting, and terminated instances, which do not apply to RDP or SSH access. But RDP or SSH connection to an EC2 instance does generate an event in the system, such as a log entry which can be used to notify the Operation team. Since its a log, you would require a service that monitors logs like CloudTrail, VPC Flow logs, or AWS Systems Manager Session Manager.

upvoted 3 times

✉ **JayBee65** 10 months, 1 week ago

I completely agree with the logic here, but I'm thinking C, since I believe you will need to "Create required metric filters" in order to detect RDP or SSH access, and this is not specified in the question, see <https://docs.aws.amazon.com/systems-manager/latest/userguide/OpsCenter-create-OpsItems-from-CloudWatch-Alarms.html>

upvoted 2 times

 **owlminus** 10 months, 1 week ago

Selected Answer: C

It's C fam. RDP or SSH connections won't change the state of the EC2 instance, so D doesn't make sense.

upvoted 4 times

 **forzadejan** 10 months, 2 weeks ago

D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

EC2 instances sends events to the EventBridge when state change occurs, such as when a new RDP or SSH connection is established, you can use EventBridge to configure a rule that listens for these events and trigger an action, like sending an email or SMS, when the connection is detected. The operations team can be notified by subscribing to the Amazon Simple Notification Service (Amazon SNS) topic, which can be configured as the target of the EventBridge rule.

upvoted 3 times

 **alanp** 10 months, 2 weeks ago

Are state changes pending:

- running
- stopping
- stopped
- shutting-down
- terminated

<https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: D

Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic. This approach allows you to set up a rule that listens for state change events on the EC2 instances, specifically for when RDP or SSH access is established, and trigger a notification via Amazon SNS to the operations team. This way they will be notified when RDP or SSH access to an environment has been established.

upvoted 3 times

 **CapJackSparrow** 8 months, 2 weeks ago

um, isn't "EC2 Instance State-change" like running, terminated, or stopped?

upvoted 1 times

A solutions architect has created a new AWS account and must secure AWS account root user access.

Which combination of actions will accomplish this? (Choose two.)

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Correct Answer: AB

Community vote distribution

AB (76%) BD (16%) 8%

 **Ruffyit** 1 week ago

Ensure the root user uses a strong password. Enable multi-factor authentication to the root user.

upvoted 1 times

 **TariqKipkemei** 2 months, 1 week ago

Selected Answer: AB

Ensure the root user uses a strong password. Enable multi-factor authentication to the root user.

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: AB

A. Setting a strong password for the root user is an essential security measure to prevent unauthorized access.

B. Enabling MFA adds an extra layer of security by requiring an additional authentication factor, such as a code from a mobile app or a hardware token, in addition to the password.

C. Root user access keys should be avoided whenever possible, and it is best to use IAM users with restricted permissions instead.

D. The root user already has unrestricted access to all resources and services in the account, so granting additional administrative permissions could increase the risk of unauthorized actions.

E. Instead, it is recommended to create IAM users with appropriate permissions and use those users for day-to-day operations, while keeping the root user secured and only using it for necessary administrative tasks.

upvoted 3 times

 **DiscussionMonke** 5 months, 1 week ago

Selected Answer: AB

Options A & B are the CORRECT answers.

upvoted 1 times

 **Bmarodi** 6 months ago

Selected Answer: AB

Options A & B are the right answers.

upvoted 1 times

 **luisgu** 6 months, 3 weeks ago

Selected Answer: AB

See <https://docs.aws.amazon.com/SetUp/latest/UserGuide/best-practices-root-user.html>

upvoted 1 times

 **Kunj7** 8 months ago

Selected Answer: AB

A and B are the correct answers:

Option A: A strong password is always required for any AWS account you create, and should not be shared or stored anywhere as there is always a risk.

Option B: This is following AWS best practice, by enabling MFA on your root user which provides another layer of security on the account and unauthorised access will be denied if the user does not have the correct password and MFA.

upvoted 1 times

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

Selected Answer: AB

AB are the right answers.

upvoted 1 times

✉  **fkie4** 8 months, 3 weeks ago

This is probably the hardest question in AWS history

upvoted 3 times

✉  **ProfXsamson** 10 months ago

Selected Answer: AB

AB is the only feasible answer here.

upvoted 3 times

✉  **bullrem** 10 months, 1 week ago

Selected Answer: BE

B. Enabling multi-factor authentication for the root user provides an additional layer of security to ensure that only authorized individuals are able to access the root user account.

E. Applying the required permissions to the root user with an inline policy document ensures that the root user only has the necessary permissions to perform the necessary tasks, and not any unnecessary permissions that could potentially be misused.

upvoted 2 times

✉  **bullrem** 10 months, 1 week ago

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

upvoted 1 times

✉  **bullrem** 10 months, 1 week ago

The other options are not sufficient to secure the root user access because:

A. A strong password alone is not enough to protect against potential security threats such as phishing or brute force attacks.

C. Storing the root user access keys in an encrypted S3 bucket does not address the root user's authentication process.

D. Adding the root user to a group with administrative permissions does not address the root user's authentication process and does not provide an additional layer of security.

upvoted 1 times

✉  **[Removed]** 7 months, 3 weeks ago

Strong passwords + multi factor is the counter to brute force...

upvoted 1 times

✉  **Pindol** 10 months, 1 week ago

Selected Answer: AB

AB obviously

upvoted 1 times

✉  **david76x** 10 months, 1 week ago

Selected Answer: AB

Root user already has admin, so D is not correct

upvoted 1 times

✉  **Aninina** 10 months, 2 weeks ago

Selected Answer: AB

AB are correct

upvoted 1 times

✉  **wmp7039** 10 months, 2 weeks ago

Selected Answer: AB

D is incorrect as root user already has full admin access.

upvoted 2 times

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

Selected Answer: AB

D. Add the root user to a group containing administrative permissions. >> its not about security, actually its unsecure so >> a&B

upvoted 1 times

✉  **raf123123** 10 months, 2 weeks ago

Selected Answer: BD

BD is correct

upvoted 2 times

A company is building a new web-based customer relationship management application. The application will use several Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS) volumes behind an Application Load Balancer (ALB). The application will also use an Amazon Aurora database. All data for the application must be encrypted at rest and in transit.

Which solution will meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) certificates on the ALB to encrypt data in transit. Use AWS Certificate Manager (ACM) to encrypt the EBS volumes and Aurora database storage at rest.
- B. Use the AWS root account to log in to the AWS Management Console. Upload the company's encryption certificates. While in the root account, select the option to turn on encryption for all data at rest and in transit for the account.
- C. Use AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and Aurora database storage at rest. Attach an AWS Certificate Manager (ACM) certificate to the ALB to encrypt data in transit.
- D. Use BitLocker to encrypt all data at rest. Import the company's TLS certificate keys to AWS Key Management Service (AWS KMS) Attach the KMS keys to the ALB to encrypt data in transit.

Correct Answer: C

Community vote distribution

C (100%)

 **cookieMr** Highly Voted 5 months ago

Selected Answer: C

AWS KMS can be used to encrypt the EBS and Aurora database storage at rest. ACM can be used to obtain an SSL/TLS certificate and attach it to the ALB. This encrypts the data in transit between the clients and the ALB.

A is incorrect because it suggests using ACM to encrypt the EBS, which is not the correct service for encrypting EBS.

B is incorrect because relying on the AWS root account and selecting an option in the AWS Management Console to enable encryption for all data at rest and in transit is not a valid approach.

D is incorrect because BitLocker is not a suitable solution for encrypting data in AWS services. It is primarily used for encrypting data on Windows-based operating systems. Additionally, importing TLS certificate keys to AWS KMS and attaching them to the ALB is not the recommended approach for encrypting data in transit.

upvoted 5 times

 **Ruffyit** Most Recent 1 week ago

To encrypt data at rest, AWS Key Management Service (AWS KMS) can be used to encrypt EBS volumes and Aurora database storage.

To encrypt data in transit, an AWS Certificate Manager (ACM) certificate can be attached to the Application Load Balancer (ALB) to enable HTTPS and TLS encryption.

upvoted 1 times

 **TariqKipkemei** 2 months ago

Selected Answer: C

Use AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and Aurora database storage at rest. Attach an AWS Certificate Manager (ACM) certificate to the ALB to encrypt data in transit

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: C

C is the best answer.

To encrypt data at rest, AWS Key Management Service (AWS KMS) can be used to encrypt EBS volumes and Aurora database storage.

To encrypt data in transit, an AWS Certificate Manager (ACM) certificate can be attached to the Application Load Balancer (ALB) to enable HTTPS and TLS encryption.

upvoted 1 times

 **MAMADOUG** 5 months, 2 weeks ago

Selected Answer: C

Option C it's correct

upvoted 1 times

 **Bmarodi** 6 months ago

Selected Answer: C

Option C fulfills the requirements.

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: C

C is correct ,A REVERSES the work of each service.

upvoted 3 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: C

C is correct!

upvoted 3 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C

c is correct answer

upvoted 2 times

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

- A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.
- B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Correct Answer: C

Community vote distribution

C (85%) A (15%)

✉  **aakashkumar1999** Highly Voted 9 months, 3 weeks ago

Selected Answer: C

C : because we need SCT to convert from Oracle to PostgreSQL, and we need memory optimized machine for databases not compute optimized.
upvoted 8 times

✉  **hissein** 2 months, 3 weeks ago

why it is memory optimized and not compute optimized machine ?
upvoted 3 times

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

A memory-optimized replication instance is recommended because the database has a high number of reads and writes. Memory-optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.
upvoted 5 times

✉  **hissein** 1 month, 4 weeks ago

thank you
upvoted 1 times

✉  **Ruffyit** Most Recent 1 week ago

because we need SCT to convert from Oracle to PostgreSQL, and we need memory optimized machine for databases not compute optimized.
A memory-optimized replication instance is recommended because the database has a high number of reads and writes. Memory-optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.
upvoted 1 times

✉  **Po_chih** 1 month, 3 weeks ago

Selected Answer: C

because we need SCT to convert from Oracle to PostgreSQL, and we need memory optimized machine for databases not compute optimized.
<https://repost.aws/zh-Hant/knowledge-center/dms-optimize-aws-sct-performance>
upvoted 1 times

✉  **TariqKipkemei** 2 months ago

Selected Answer: C

Oracle database to Amazon Aurora PostgreSQL = AWS Schema Conversion Tool
High number of reads and writes = memory optimized replication instance
upvoted 2 times

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

Selected Answer: C

A memory-optimized replication instance is recommended because the database has a high number of reads and writes. Memory-optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.
upvoted 1 times

✉  **_d1rk_** 3 months, 1 week ago

Selected Answer: C

DataSync is for file-level synch, so A and B can be excluded. C is better than D because memory-optimized instances are recommended to handle the high number of reads and writes

upvoted 2 times

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

Selected Answer: A

why not a? only capture the change is sufficient

upvoted 2 times

✉ **Mmmmmmkkkk** 4 months, 4 weeks ago

Bbbbbbb

upvoted 1 times

✉ **cookieMr** 5 months ago

Selected Answer: C

The AWS SCT is used to convert the schema and code of the Oracle database to be compatible with Aurora PostgreSQL. AWS DMS is utilized to migrate the data from the Oracle database to Aurora PostgreSQL. Using a memory-optimized replication instance is recommended to handle the high number of reads and writes during the migration process.

By creating a full load plus CDC replication task, the initial data migration is performed, and ongoing changes in the Oracle database are continuously captured and applied to the Aurora PostgreSQL database. Selecting all tables for table mapping ensures that all the applications writing to the same tables are migrated.

Option A & B are incorrect because using AWS DataSync alone is not sufficient for database migration and data synchronization.

Option D is incorrect because using a compute optimized replication instance is not the most suitable choice for handling the high number of reads and writes.

upvoted 2 times

✉ **omoakin** 6 months ago

BBBBBBBBBBBBBBB

upvoted 2 times

✉ **SimiTik** 7 months, 2 weeks ago

B chatgpt

upvoted 2 times

✉ **KZM** 9 months, 1 week ago

DMS+SCT for Oracle to Aurora PostgreSQL migration

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-oracle-database-to-aurora-postgresql-using-aws-dms-and-aws-sct.html>

upvoted 2 times

✉ **icurfer** 10 months ago

<https://aws.amazon.com/ko/premiumsupport/knowledge-center/dms-memory-optimization/>

upvoted 1 times

✉ **dark_firzen** 10 months ago

Selected Answer: C

It has to be either C or D because it requires Schema Conversion Tool to convert Oracle database to Amazon Aurora PostgreSQL. C would be the better choice here because it replicates a memory optimized instance, which is recommended for databases. Also, the database must be kept in sync, so they require mapping to select all tables.

upvoted 3 times

✉ **bullrem** 10 months, 1 week ago

A or C are both valid options. Both options involve using AWS DataSync for the initial migration, and then using AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task for ongoing data synchronization.

Option A: Uses a memory optimized replication instance.

Option C: Uses a compute optimized replication instance.

Option A is a better choice for migrations where the data is more complex and may require more memory.

Option C is a better choice for migrations that require more processing power.

It is also depend on the size of the data, the complexity of the data, and the resources available in the target Aurora cluster.

upvoted 1 times

✉ **JayBee65** 10 months, 1 week ago

Why would you not use the schema conversion tool, which is designed specifically to convert from one db engine to another. It can convert Oracle to Aurora PostgreSQL, see https://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/CHAP_Welcome.html. Then it is a choice of C or D. Since you want to move all tables C makes more sense than D.

A and B are wrong since DataSync deals with data not databases, see <https://aws.amazon.com/datasync/faqs/>.

upvoted 4 times

✉ **brownest** 10 months, 1 week ago

Selected Answer: A

Initial migration is full using DataSync and on-going replication is through CDC for the changes. The full load was already performed so no need to do it again as with Answer B.

upvoted 1 times

 **brownest** 10 months, 1 week ago

Changing my answer to C as you need schema conversion from Oracle the PostgreSQL

upvoted 2 times

A company has a three-tier application for image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance for the application layer, and a third EC2 instance for a MySQL database. A solutions architect must design a scalable and highly available solution that requires the least amount of change to the application.

Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer. Use AWS Lambda functions for the application layer. Move the database to an Amazon DynamoDB table. Use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS DB instance with multiple read replicas to serve users' images.
- C. Use Amazon S3 to host the front-end layer. Use a fleet of EC2 instances in an Auto Scaling group for the application layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images.

Correct Answer: A

Community vote distribution

D (63%) B (33%)

 **PDR** Highly Voted 10 months ago

Selected Answer: B

B and D very similar with D being the 'best' solution but it is not the one that requires the least amount of development changes as the application would need to be changed to store images in S3 instead of DB

upvoted 10 times

 **Ruffyit** Most Recent 1 week ago

Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images

upvoted 1 times

 **rlamberti** 1 month ago

Option B - DB is not a good option to store images. Read replicas won't improve HA for write, only scales reading IO. Therefore no true HA achieved.

D is the goal for me.

upvoted 1 times

 **TariqKipkemei** 2 months ago

Selected Answer: D

Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

Use Elastic Beanstalk load-balanced environments for the web and app tiers. This provides auto scaling and high availability with minimal effort. Move the database to RDS Multi-AZ. This handles scaling reads and storage, and provides HA with automated failover. Use S3 for serving user images. S3 is highly scalable and durable storage.

The application code remains unchanged using this approach.

upvoted 1 times

 **Mia2009687** 5 months ago

Selected Answer: A

AWS Elastic Beanstalk makes it even easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

I don't quite understand why people choose D.

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: D

By using load-balanced Multi-AZ AWS EBS, you achieve scalability and high availability for both layers without requiring significant changes to the application. Moving the DB to an RDS Multi-AZ DB ensures high availability and automatic failover. Storing and serving users' images through S3 provides a scalable and highly available solution.

A is incorrect because using S3 for the front-end layer and Lambda for the application layer would require significant changes to the application architecture. Moving the DB to DynamoDB would require rewriting the DB-related code.

B is incorrect because using load-balanced Multi-AZ AWS EBS environments and an RDS DB with read replicas for serving images would be a more suitable solution. RDS with read replicas can handle the image-serving workload more efficiently than using S3 for this purpose.

C is incorrect because using S3 for the front-end layer and an ASG of EC2 for the application layer would require modifying the application architecture. Storing and serving images from a memory-optimized EC2 type may not be the most efficient and scalable approach compared to using S3.

upvoted 2 times

 **markw92** 5 months, 1 week ago

"least amount of change to the application." - A has lots of changes, completely revamping the application and lots of new pieces. D is closest with only addition of s3 to store images which is right move. You do not want images to store in any database anyway.

upvoted 3 times

 **aaroncelestin** 3 months, 1 week ago

Thats what I was thinking, but the question doesn't mention anything about storing users' images anywhere. Are we supposed to just assume that they wanted to store the images in a DB even though that is a bad idea?

upvoted 1 times

 **Bmarodi** 6 months ago

Selected Answer: D

Option D meets the requirements.

upvoted 1 times

 **Grace83** 8 months, 2 weeks ago

D is correct

upvoted 2 times

 **focus_23** 10 months ago

Selected Answer: D

RDS multi AZ.

upvoted 2 times

 **wmp7039** 10 months, 2 weeks ago

Selected Answer: D

D is correct as application changes needs to me minimal

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: D

Correct answer is D

upvoted 2 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: D

for "Highly available": Multi-AZ &

for "least amount of changes to the application": Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring

upvoted 4 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/24840-exam-aws-certified-solutions-architect-associate-saa-c02/>

Please ExamTopics, review your own answers

upvoted 4 times

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both VPCs are in separate AWS accounts. The network administrator needs to design a solution to configure secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

- A. Set up a VPC peering connection between VPC-A and VPC-B.
- B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
- C. Attach a virtual private gateway to VPC-B and set up routing from VPC-A.
- D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A.

Correct Answer: A

Community vote distribution

A (93%)	7%
---------	----

 **LuckyAro** Highly Voted 10 months ago

Selected Answer: A

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
upvoted 8 times

 **Ruffyt** Most Recent 6 days, 23 hours ago

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

A. Set up a VPC peering connection between VPC-A and VPC-B
upvoted 1 times

 **MNotABot** 4 months, 2 weeks ago

<https://www.bing.com/search?q=can+we+do+VPC+peering+across+AWS+accounts&cvid=48a8ceec85a429c9ddd698b01055890&aqs=edge..69i57j0l8j69i11004.10897j0j1&FORM=ANNAB1&PC=LCTS>
upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: A

A VPC peering connection allows secure communication between instances in different VPCs using private IP addresses without the need for internet gateways, VPN connections, or NAT devices. By setting it up, the application running in VPC-A can directly access the EC2 in VPC-B without going through the public internet or any single point of failure.

B is incorrect because VPC gateway endpoints are used for accessing S3 or DynamoDB from a VPC without going over the internet. They are not designed for establishing connectivity between EC2 instances in different VPCs.

C is incorrect because it would require configuring a VPN connection between the VPCs. This would introduce additional complexity and potential single points of failure.

D is incorrect because creating a private VIF and adding routes would be applicable for establishing a direct connection between on-premises infrastructure and VPC-B using Direct Connect, but it is not suitable for the scenario of communication between EC2 instances in separate VPCs within different AWS accounts.

upvoted 4 times

 **Anmol_1010** 5 months, 2 weeks ago

D, VPC PEERINGVIS IN SAME ACCOUNT
upvoted 1 times

 **im6h** 5 months, 2 weeks ago

No, VPC Peering can use across account.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
upvoted 2 times

✉ **omoakin** 6 months ago

DDDDDDDDDDDDDD
upvoted 2 times

✉ **omoakin** 6 months ago

This is the only viable solution
Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A
upvoted 1 times

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

Selected Answer: A

"You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account."

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
upvoted 4 times

✉ **PDR** 10 months ago

Selected Answer: A

correct answer is A and as mentioned by JayBee65 below, key reason being that solution should not have a single point of failure and bandwidth restrictions

the following paragraph is taken from the AWS docs page linked below that backs this up

"AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck."

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
upvoted 2 times

✉ **LuckyAro** 10 months, 1 week ago

Selected Answer: B

A VPC endpoint gateway to the EC2 Instance is more specific and more secure than forming a VPC peering that exposes the whole of the VPC infrastructure just for one connection.

upvoted 2 times

✉ **JayBee65** 10 months, 1 week ago

Your logic is correct but security is not a requirement here - the requirements are "The connectivity should not have a single point of failure or bandwidth concerns." A VPC gateway endpoint would form a single point of failure, so B is incorrect, (and C and D are incorrect for the same reason, they create single points of failure).

upvoted 4 times

✉ **mhmt4438** 10 months, 2 weeks ago

Selected Answer: A

Correct answer is A

upvoted 2 times

✉ **Aninina** 10 months, 2 weeks ago

Selected Answer: A

VPC peering allows resources in different VPCs to communicate with each other as if they were within the same network. This solution would establish a direct network route between VPC-A and VPC-B, eliminating the need for a single point of failure or bandwidth concerns.

upvoted 1 times

✉ **waiyiu9981** 10 months, 2 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/27763-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 4 times

A company wants to experiment with individual AWS accounts for its engineer team. The company wants to be notified as soon as the Amazon EC2 instance usage for a given month exceeds a specific threshold for each account.

What should a solutions architect do to meet this requirement MOST cost-effectively?

- A. Use Cost Explorer to create a daily report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
- B. Use Cost Explorer to create a monthly report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
- C. Use AWS Budgets to create a cost budget for each account. Set the period to monthly. Set the scope to EC2 instances. Set an alert threshold for the budget. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.
- D. Use AWS Cost and Usage Reports to create a report with hourly granularity. Integrate the report data with Amazon Athena. Use Amazon EventBridge to schedule an Athena query. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.

Correct Answer: B

Community vote distribution

C (95%) 5%

 **Aninina**  10 months, 2 weeks ago

Selected Answer: C

AWS Budgets allows you to create budgets for your AWS accounts and set alerts when usage exceeds a certain threshold. By creating a budget for each account, specifying the period as monthly and the scope as EC2 instances, you can effectively track the EC2 usage for each account and be notified when a threshold is exceeded. This solution is the most cost-effective option as it does not require additional resources such as Amazon Athena or Amazon EventBridge.

upvoted 8 times

 **Ruffyit**  6 days ago

AWS Budgets allows you to create budgets for your AWS accounts and set alerts when usage exceeds a certain threshold. By creating a budget for each account, specifying the period as monthly and the scope as EC2 instances, you can effectively track the EC2 usage for each account and be notified when a threshold is exceeded. This solution is the most cost-effective option as it does not require additional resources such as Amazon Athena or Amazon EventBridge.

upvoted 1 times

 **vijaykamal** 2 months ago

Selected Answer: C

Option A and Option B suggest using Cost Explorer to create reports and send notifications. While Cost Explorer is useful for analyzing costs, it does not provide the real-time alerting capability that AWS Budgets offers.

Option D suggests using AWS Cost and Usage Reports integrated with Amazon Athena and Amazon EventBridge, which can be a more complex and potentially costlier solution compared to AWS Budgets for this specific use case. It's also more suitable for fine-grained, custom analytics rather than straightforward threshold-based alerts.

upvoted 2 times

 **TariqKipkemei** 2 months ago

Selected Answer: C

AWS Budgets was designed to handle this scenario.

upvoted 1 times

 **Undisputed** 4 months ago

Selected Answer: C

Use AWS Budgets to create a cost budget for each account. Set the period to monthly. Set the scope to EC2 instances. Set an alert threshold for the budget. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: C

By creating a cost budget for each account, specifying the period as monthly and scoping it to EC2, you can track and monitor the costs associated with EC2 specifically. Set an alert threshold in the budget, which will trigger a notification when the specified threshold is exceeded. Configure an SNS to receive the notification, which can be subscribed to by the company to receive immediate alerts.

A and B are not the most cost-effective solutions as they involve using Cost Explorer to create reports, which may not provide real-time notifications when the threshold is exceeded. Additionally, A. suggests using a daily report, while B. suggests using a monthly report, which may not provide the desired level of granularity for immediate notifications.

D involves using Cost and Usage Reports with Athena and EventBridge. This solution provides more flexibility and data analysis capabilities, it is more complex and may incur additional costs for using Athena and generating hourly reports.

upvoted 1 times

 **Samuel03** 9 months, 1 week ago

Selected Answer: D

I go with D. It says "as soon as", "daily" reports seems to be a bit longer time frame to wait in my opinion.

upvoted 1 times

 **Bofi** 8 months, 4 weeks ago

Athena can only be used in s3, that is enough to discard D

upvoted 1 times

 **Samuel03** 9 months, 1 week ago

Actually, I take that back. It clearly says "Cost effective."

upvoted 3 times

 **alexleely** 10 months, 1 week ago

C: AWS Budgets allows you to set a budget for costs and usage for your accounts and you can set alerts when the budget threshold is exceeded in real-time which meets the requirement.

Why not B: B would be the most cost-effective if the requirements didn't ask for real-time notification. You would not incur additional costs for the daily or monthly reports and the notifications. But doesn't provide real-time alerts.

upvoted 4 times

 **mp165** 10 months, 2 weeks ago

Selected Answer: C

Agree...C

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

 **venice1234** 10 months, 2 weeks ago

Selected Answer: C

<https://aws.amazon.com/getting-started/hands-on/control-your-costs-free-tier-budgets/>

upvoted 1 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: C

AWS budget IMO, it's done for it

upvoted 2 times

A solutions architect needs to design a new microservice for a company's application. Clients must be able to call an HTTPS endpoint to reach the microservice. The microservice also must use AWS Identity and Access Management (IAM) to authenticate calls. The solutions architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x.

Which solution will deploy the function in the MOST operationally efficient way?

- A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.
- B. Create a Lambda function URL for the function. Specify AWS_IAM as the authentication type.
- C. Create an Amazon CloudFront distribution. Deploy the function to Lambda@Edge. Integrate IAM authentication logic into the Lambda@Edge function.
- D. Create an Amazon CloudFront distribution. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

Correct Answer: A

Community vote distribution

A (72%)

B (28%)

 **mhmt4438**  10 months, 2 weeks ago

Selected Answer: A

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API. This option is the most operationally efficient as it allows you to use API Gateway to handle the HTTPS endpoint and also allows you to use IAM to authenticate the calls to the microservice. API Gateway also provides many additional features such as caching, throttling, and monitoring, which can be useful for a microservice.

upvoted 16 times

 **google_platform_team**  4 days, 22 hours ago

Selected Answer: B

I think it is B - most operationally efficient. A is a better answer, but more complicated.

upvoted 1 times

 **swap001** 1 month, 2 weeks ago

Selected Answer: B

There is no need of an additional API gateway when Lambda itself can support the need. This is more operationally efficient.

upvoted 2 times

 **OlehKom** 1 month, 3 weeks ago

Why not B? I agree that A is a nice choice, but it clearly says "MOST operationally efficient way", there is nothing said about API. B in this case suits absolutely fine, it's simpler and cheaper.

upvoted 1 times

 **TariqKipkemei** 2 months ago

Selected Answer: A

Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API. This option is the most operationally efficient as it allows you to use API Gateway to handle the HTTPS endpoint and also allows you to use IAM to authenticate the calls to the microservice. API Gateway also provides many additional features such as caching, throttling, and monitoring, which can be useful for a microservice.

upvoted 1 times

 **Smart** 3 months, 4 weeks ago

Selected Answer: B

C & D (incorrect) - what will be the origin for CDN? Plus Go is not supported. Plus for option D, IAM is not supported.

A, why develop and manage API in API GW?

Just enable Lambda function URL...

upvoted 2 times

 **Zeezie** 4 months ago

B -- MOST operationally efficient. Just look at the Lambda Create function console...

Enable function URL >

Use function URLs to assign HTTP(S) endpoints to your Lambda function.

Auth type

Choose the auth type for your function URL. >

AWS_IAM

Only authenticated IAM users and roles can make requests to your function URL.

upvoted 2 times

✉️ **testopesto** 4 months ago

Selected Answer: B

The MOST operationally efficient way

<https://docs.aws.amazon.com/lambda/latest/dg/urls-auth.html>

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

upvoted 2 times

✉️ **Undisputed** 4 months ago

Selected Answer: A

Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.

upvoted 1 times

✉️ **cookieMr** 5 months ago

Selected Answer: A

By creating an API Gateway REST API, you can define the HTTPS endpoint that clients can call to reach the microservice. Enable IAM authentication on the API to enforce authentication for the API calls. This ensures that only authenticated requests are allowed to reach the microservice. This solution is operationally efficient as it leverages the built-in capabilities of API Gateway to handle the HTTP endpoint, request routing, and IAM authentication. It provides a scalable and managed solution without the need for additional infrastructure components.

B suggests creating a Lambda URL and specifying AWS IAM as the authentication type. While this can provide IAM authentication, it lacks the benefits of API Gateway, such as request validation, rate limiting, and easy management of API configurations.

C and D involve using CloudFront, Lambda@Edge, and CloudFront Functions. While these services offer flexibility and the ability to run logic at the edge locations, they introduce additional complexity and may not be necessary for the given requirement.

upvoted 1 times

✉️ **Smart** 3 months, 4 weeks ago

The question is not asking for API Gateway benefits.

upvoted 2 times

✉️ **vassdlevi** 6 months ago

Selected Answer: B

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

upvoted 1 times

✉️ **PRASAD180** 9 months, 1 week ago

A is crt 100%

upvoted 2 times

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

Why c is not correct? ?

upvoted 3 times

✉️ **moiraqi** 6 months, 1 week ago

Lambda@Edge only support NodeJS or Python

upvoted 2 times

✉️ **vassdlevi** 5 months ago

AWS Lambda natively supports Java, Go, PowerShell, Node.js, C#, Python, and Ruby code, and provides a Runtime API which allows you to use any additional programming languages to author your functions.

upvoted 1 times

✉️ **bdp123** 9 months, 2 weeks ago

Selected Answer: A

<https://asanchez.dev/blog/deploy-api-go-aws-lambda-gateway/>

upvoted 1 times

✉️ **SanLi** 10 months, 2 weeks ago

D

<https://aws.amazon.com/premiumsupport/knowledge-center/iam-authentication-api-gateway/>

upvoted 1 times

✉️ **JayBee65** 10 months, 1 week ago

With CloudFront Functions in Amazon CloudFront, you can write lightweight functions in JavaScript for high-scale, latency-sensitive CDN customizations. But you are using Go 1.x. Lambda supports go. So A makes a lot more sense than D
upvoted 2 times

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

- A. Host the visualization tool on premises and query the data warehouse directly over the internet.
- B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.
- C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

Correct Answer: C

Community vote distribution

D (88%) 8%

 AlessandraSAA Highly Voted 9 months ago

Selected Answer: D

- A. --> No since if you access via internet you are creating egress traffic.
- B. --> It's a good choice to have both DWH and visualization in the same region to lower the egress transfer (i.e. data going egress/out of the region) but if you access over internet you might still have egress transfer.
- C. -> Valid but in this case you send out of AWS 50MB if you query the DWH instead of the visualization tool, D removes this need since puts the visualization tools in AWS with the DWH so reduces data returned out of AWS from 50MB to 500KB
- D. --> Correct, see explanation on answer C

Useful links:

AWS Direct Connect connection create a connection in an AWS Direct Connect location to establish a network connection from your premises to an AWS Region.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>

upvoted 6 times

 Ruffyt Most Recent 5 days, 21 hours ago

- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

upvoted 1 times

 TariqKipkemei 2 months ago

Selected Answer: D

Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region

upvoted 1 times

 Guru4Cloud 2 months, 2 weeks ago

Selected Answer: D

- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

upvoted 1 times

 jtexam 4 months, 2 weeks ago

Selected Answer: B

by hosting in same region, you have 500kb transfer charged on internet transfer tier, 50MB charged in inter-region tier.

using direct link, both are charged in direct link tier. direct link tier is not cheap.

so i go for B

upvoted 1 times

 Mmmmmmkkkk 4 months, 4 weeks ago

Aaaaaaaa

upvoted 1 times

 cookieMr 5 months ago

Selected Answer: D

Hosting the visualization tool in the same AWS Region as the data warehouse and accessing it over a Direct Connect connection within the same Region eliminates data transfer fees and ensures low-latency, high-bandwidth connectivity.

- A. Hosting the visualization tool on premises and querying the data warehouse over the internet incurs data transfer costs for every query result, as well as potential latency and bandwidth limitations.
- B. Hosting the visualization tool in the same AWS Region as the data warehouse but accessing it over the internet still incurs data transfer costs for each query result.
- C. Hosting the visualization tool on premises and querying the data warehouse over a Direct Connect connection within the same AWS Region incurs data transfer costs for every query result and adds complexity by requiring on-premises infrastructure.

upvoted 1 times

 **dexpos** 10 months ago

Selected Answer: D

D let you reduce at minimum the data transfer costs

upvoted 1 times

 **alexleely** 10 months, 1 week ago

Selected Answer: D

D: Direct Connect connection at a location in the same Region will provide the lowest data transfer egress cost, improved performance, and lower complexity

Why it is not C is because the visualization tool is hosted on-premises, as it's not hosted in the same region as the data warehouse the data transfer between them would occur over the internet, thus, would incur in egress data transfer costs.

upvoted 4 times

 **markw92** 5 months, 1 week ago

C option doesn't travel through internet because we have a direct connect. If you are hosting your visualization tool in same region why you need a direct connection which D has? Doesn't make sense. So, C is the right answer.

upvoted 1 times

 **Vickysss** 10 months, 2 weeks ago

Selected Answer: C

<https://www.nops.io/reduce-aws-data-transfer-costs-dont-get-stung-by-hefty-egress-fees/>

upvoted 2 times

 **JayBee65** 10 months, 1 week ago

Whilst "Direct Connect can help lower egress costs even after taking the installation costs into account. This is because AWS charges lower transfer rates." D removes the need to send the query results out of AWS and instead returns the web page, so reduces data returned from 50MB to 500KB, so D

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: D

Correct answer is D

upvoted 4 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: D

Should be D

<https://aws.amazon.com/directconnect/pricing/>

<https://aws.amazon.com/blogs/aws/aws-data-transfer-prices-reduced/>

upvoted 2 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/47140-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.

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

- A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
- B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
- C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
- D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Correct Answer: C

Community vote distribution

C (74%) B (26%)

✉  **Steve_4542636** Highly Voted 9 months ago

Selected Answer: C

Multi az is not the same as multi regional
upvoted 23 times

✉  **alexleely** Highly Voted 10 months, 1 week ago

Selected Answer: B

B: Amazon RDS Multi-AZ feature automatically creates a synchronous replica in another availability zone and failover to the replica in the event of an outage. This will provide high availability and data durability across multiple AWS regions which fit the requirements.

Though C may sound good, it in fact requires manual management and monitoring of the replication process due to the fact that Amazon RDS read replicas are asynchronous, meaning there is a delay between the primary and read replica. Therefore, there will be a need to ensure that the read replica is constantly up-to-date and someone still has to fix any read replica errors during the replication process which may cause data inconsistency. Lastly, you still have to configure additional steps to make it fail over to the read replica.

upvoted 14 times

✉  **Mahadeva** 10 months, 1 week ago

But the question is clearly asking for Multiple Regions. Multi-AZ is not across Regions.
upvoted 19 times

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

You are right, Multi-AZ is only within one Region. C would be the right answer.
upvoted 11 times

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

<https://aws.amazon.com/rds/features/multi-az/>

smartegnine 0 minutes ago Awaiting moderator approval

Selected Answer: B

In an Amazon RDS Multi-AZ deployment, Amazon RDS automatically creates a primary database (DB) instance and synchronously replicates the data to an instance in a different AZ.

upvoted 1 times

✉  **Rehan33** 9 months, 1 week ago

I go with option B because:
Multi-AZ is for high availability
Read replicas are for low-latency
in question they talk about available online
upvoted 4 times

✉  **vijaykamal** Most Recent 2 months ago

Selected Answer: B

Option C, while providing a read replica in another Region, adds complexity to the architecture and may introduce some additional operational overhead compared to Multi-AZ. Cross-Region replication involves setting up and managing replication between two separate RDS instances.
upvoted 1 times

✉  **TariqKipkemei** 2 months ago

Selected Answer: C

Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region

upvoted 1 times

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

Selected Answer: C

Multi-AZ is not the same as Multi-Regional

upvoted 3 times

✉ **Valder21** 2 months, 3 weeks ago

can someone explain why not D

upvoted 3 times

✉ **beginnercloud** 3 months ago

Selected Answer: C

key words "AWS Regions at all times" so C is correct

upvoted 1 times

✉ **fuzzycr** 4 months, 2 weeks ago

Selected Answer: C

key words "AWS Regions at all times"

upvoted 1 times

✉ **cookieMr** 5 months ago

Selected Answer: C

By migrating the PostgreSQL database to an RDS for PostgreSQL DB instance and creating a read replica in another AWS Region, you can achieve data availability and online access across multiple Regions. This solution requires less operational overhead compared to managing a PostgreSQL cluster on EC2 instances (Option A) or setting up manual replication using snapshots (Option D). Additionally, Amazon RDS handles the underlying infrastructure and replication setup, reducing the operational complexity for the company.

Option B, is a valid solution for achieving high availability within a single AWS Region. However, it does not meet the requirement of having the data available and online across multiple AWS Regions at all times, which is specified in the question. The Multi-AZ feature in RDS provides automatic failover within the same Region, but it does not replicate the data to multiple Regions.

upvoted 3 times

✉ **mal1903** 5 months, 2 weeks ago

Selected Answer: B

C and D just specify another single region. This does not translate to multiple regions.

B (Multi-AZ) means the solution will be highly available.

The data will be available in multiple regions for both B and C but B is a better solution!

upvoted 1 times

✉ **Guru4Cloud** 2 months, 1 week ago

its data is available and online across multiple AWS Regions at all times

upvoted 1 times

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

Selected Answer: C

Answer B is not right, because "RDS Multi-AZ" always spans at least two Availability Zones within a single region and the question requirement RDS DB should be available in multiple regions. Therefore, C is the most suitable answer for this question.

upvoted 2 times

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

I would like to change my answer to "B". The question has some distractor words: "its data is available and online across multiple AWS Regions at all times". We agree that AWS Lambda is a cold service available online around the world in 99 regions. So the option "B" is the most appropriate answer, since Multi-AZ focuses on the availability factor and it has the LEAST amount of operational overhead.

upvoted 1 times

✉ **abhishek2021** 5 months, 2 weeks ago

Selected Answer: B

B & C both make data available. However, B is less overhead.

What I think, the question is asking for data availability across multiple regions not for a DR solution. So, RDS being accessible over public IP will do the trick for data being available across regions.

upvoted 1 times

✉ **Guru4Cloud** 2 months, 1 week ago

Multi-AZ is not the same as Multi-Regional

upvoted 1 times

✉ **Bmarodi** 5 months, 2 weeks ago

Selected Answer: C

Option meets the requirements, ref. link: <https://aws.amazon.com/blogs/database/best-practices-for-amazon-rds-for-postgresql-cross-region-read-replicas/>

upvoted 1 times

 **smartegnine** 5 months, 2 weeks ago

Selected Answer: B

In an Amazon RDS Multi-AZ deployment, Amazon RDS automatically creates a primary database (DB) instance and synchronously replicates the data to an instance in a different AZ.

<https://aws.amazon.com/rds/features/multi-az/>

upvoted 1 times

 **ruqui** 6 months, 1 week ago

Selected Answer: C

B is wrong because Multi AZ feature don't allow to have replicas in another region!!!! (the requirement is that "data should be available and online across multiple AWS Regions at all times") ... only feasible option is C

upvoted 1 times

 **kaustubhBarhate** 6 months, 1 week ago

Multi-AZ provides redundancy within a single Region, it does not replicate data across multiple Regions. If the requirement specifically states the need for data availability across multiple Regions, creating a read replica in another Region (option C) would be the more appropriate choice.

upvoted 1 times

 **fakrap** 6 months, 3 weeks ago

Selected Answer: C

Multi region

upvoted 2 times

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.

Which policy should be used to meet this requirement?

- A. Simple routing policy
- B. Latency routing policy
- C. Multivalue routing policy
- D. Geolocation routing policy

Correct Answer: C

Community vote distribution

C (94%)	6%
---------	----

✉  **LuckyAro** Highly Voted 10 months, 1 week ago

Selected Answer: C

Use a multivalue answer routing policy to help distribute DNS responses across multiple resources. For example, use multivalue answer routing when you want to associate your routing records with a Route 53 health check. For example, use multivalue answer routing when you need to return multiple values for a DNS query and route traffic to multiple IP addresses.

<https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/>
upvoted 8 times

✉  **cookieMr** Highly Voted 5 months ago

The Multivalue routing policy allows Route 53 to respond to DNS queries with multiple healthy IP addresses for the same resource. This is particularly useful in scenarios where multiple instances are serving the same purpose and need to be load balanced or failover capable. With the Multivalue routing policy, Route 53 returns multiple IP addresses in a random order to distribute the traffic across all healthy instances.

Option A (Simple routing policy) would only return a single IP address in response to DNS queries and does not support returning multiple addresses.

Option B (Latency routing policy) is used to route traffic based on the lowest latency to the resource and does not fulfill the requirement of returning all healthy IP addresses.

Option D (Geolocation routing policy) is used to route traffic based on the geographic location of the user and does not fulfill the requirement of returning all healthy IP addresses.

Therefore, the Multivalue routing policy is the most suitable option for returning the IP addresses of all healthy EC2 instances in response to DNS queries.

upvoted 5 times

✉  **TariqKipkemei** Most Recent 2 months ago

Selected Answer: C

Use Multivalue answer routing policy when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
upvoted 1 times

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

Selected Answer: C

C. Multivalue routing policy
upvoted 1 times

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

Selected Answer: A

A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic
upvoted 1 times

✉  **animefan1** 4 months, 4 weeks ago

multivalue supports health checks
upvoted 1 times

✉  **MLCL** 8 months, 2 weeks ago

IP are returned RANDOMLY for multi-value Routing, is this what we want?
upvoted 4 times

 **Whericanstart** 8 months, 3 weeks ago

Selected Answer: C

Multivalue answer routing policy ...answer is C
upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C

Answer is C
upvoted 2 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: C

Should be C
upvoted 1 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/46491-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/46491-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

A medical research lab produces data that is related to a new study. The lab wants to make the data available with minimum latency to clinics across the country for their on-premises, file-based applications. The data files are stored in an Amazon S3 bucket that has read-only permissions for each clinic.

What should a solutions architect recommend to meet these requirements?

- A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic
- B. Migrate the files to each clinic's on-premises applications by using AWS DataSync for processing.
- C. Deploy an AWS Storage Gateway volume gateway as a virtual machine (VM) on premises at each clinic.
- D. Attach an Amazon Elastic File System (Amazon EFS) file system to each clinic's on-premises servers.

Correct Answer: C

Community vote distribution

A (94%) 6%

 **mhmt4438** Highly Voted  10 months, 2 weeks ago

Selected Answer: A

- A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. By deploying a file gateway as a virtual machine on each clinic's premises, the medical research lab can provide low-latency access to the data stored in the S3 bucket while maintaining read-only permissions for each clinic. This solution allows the clinics to access the data files directly from their on-premises file-based applications without the need for data transfer or migration.

upvoted 14 times

 **TariqKipkemei** Most Recent  2 months ago

Selected Answer: A

The Amazon S3 File Gateway enables you to store and retrieve objects in Amazon Simple Storage Service (S3) using file protocols such as Network File System (NFS) and Server Message Block (SMB). Objects written through S3 File Gateway can be directly accessed in S3.

upvoted 2 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

- A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

upvoted 2 times

 **cookieMr** 5 months ago

A. It allows the clinics to access the data files stored in the S3 bucket through a file interface. The file gateway caches frequently accessed data locally, reducing latency and providing fast access to the data.

B. It involves transferring the data files from the Amazon S3 bucket to each clinic's on-premises applications using AWS DataSync. While this enables data migration, it may not provide real-time access and may introduce additional latency.

C. It is suitable for block-level access to data rather than file-level access. It may not be the most efficient solution for file-based applications.

D. It involves using Amazon EFS, which is a scalable file storage service, to provide file-level access to the data. However, it may introduce additional complexity and latency compared to using a file gateway solution.

upvoted 4 times

 **Bmarodi** 6 months ago

Selected Answer: A

Option A meets the requirements.

upvoted 1 times

 **jaswantn** 7 months, 1 week ago

For File-based applications use File Gateway: (Option A)

upvoted 1 times

 **Grace83** 8 months, 2 weeks ago

Definitely A.

Why are there so many wrong answers by Admins?

upvoted 4 times

 **maggie135** 5 months ago

I guess to force us to read and think, so one can't just memorize the answer and go to exam ?)
upvoted 3 times

 **AlessandraSAA** 9 months ago

Selected Answer: A

Amazon S3 File Gateway enables you to store file data as objects in Amazon S3 cloud storage for data lakes, backups, and Machine Learning workflows. With Amazon S3 File Gateway, each file is stored as an object in Amazon S3 with a one-to-one mapping between a file and an object.

Volume Gateway provides block storage volumes over iSCSI, backed by Amazon S3, and provides point-in-time backups as Amazon EBS snapshots. Volume Gateway integrates with AWS Backup, an automated and centralized backup service, to protect Storage Gateway volumes.

So it's A

upvoted 4 times

 **Steve_4542636** 9 months ago

Selected Answer: A

A for answer

upvoted 1 times

 **bdp123** 9 months, 4 weeks ago

Selected Answer: A

<https://cloud.in28minutes.com/aws-certification-aws-storage-gateway>

upvoted 1 times

 **kbaruu** 10 months, 1 week ago

Selected Answer: A

A. Deploy an AWS Storage Gateway file gateway...

upvoted 1 times

 **imisioluwa** 10 months, 2 weeks ago

Selected Answer: A

The correct answer is A.

<https://www.knowledgehut.com/tutorials/aws/aws-storage-gateway#:~:text=AWS%20Storage%20Gateway%20helps%20in%20connecting,as%20well%20as%20providing%20data%20security.&text=AWS%20Storage%20Gateway%20helps,as%20providing%20data%20security.&text=Gateway%20helps%20in%20connecting,as%20well%20as%20providing>
<https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html>

upvoted 1 times

 **venice1234** 10 months, 2 weeks ago

Selected Answer: C

I think C (Volume Gateway) is correct as it has an option to have Local Storage with Asynchronous sync with S3. This would give low latency access to all local files not just cached/recent files.

upvoted 2 times

 **laicos** 10 months, 2 weeks ago

Selected Answer: A

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

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: A

A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

upvoted 1 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: A

It's A imo (file gateway)

upvoted 2 times

A company is using a content management system that runs on a single Amazon EC2 instance. The EC2 instance contains both the web server and the database software. The company must make its website platform highly available and must enable the website to scale to meet user demand.

What should a solutions architect recommend to meet these requirements?

- A. Move the database to Amazon RDS, and enable automatic backups. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer in the Availability Zone, and set the two instances as targets.
- B. Migrate the database to an Amazon Aurora instance with a read replica in the same Availability Zone as the existing EC2 instance. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer, and set the two EC2 instances as targets.
- C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.
- D. Move the database to a separate EC2 instance, and schedule backups to Amazon S3. Create an Amazon Machine Image (AMI) from the original EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

Correct Answer: C

Community vote distribution

C (95%) 5%

✉  **mhmt4438** Highly Voted 10 months, 2 weeks ago

Selected Answer: C

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

This approach will provide both high availability and scalability for the website platform. By moving the database to Amazon Aurora with a read replica in another availability zone, it will provide a failover option for the database. The use of an Application Load Balancer and an Auto Scaling group across two availability zones allows for automatic scaling of the website to meet increased user demand. Additionally, creating an AMI from the original EC2 instance allows for easy replication of the instance in case of failure.

upvoted 12 times

✉  **Bmarodi** 6 months ago

Very good explanations!
upvoted 1 times

✉  **TariqKipkemei** Most Recent 2 months ago

Selected Answer: C

Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

upvoted 1 times

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

Selected Answer: C

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

upvoted 1 times

✉  **MutiverseAgent** 4 months ago

Selected Answer: D

The question does not say if the current application is using a relational database, so how we can be sure that it can moved to RDS or aurora as answers A, B & C states? In my opinion the right answer is D.

upvoted 1 times

✉  **animefan1** 4 months, 4 weeks ago

Selected Answer: C

has all options needed for HA

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: C

Option A does not provide a solution for high availability or scalability. Manually launching another EC2 instance in the same AZ may not ensure high availability, as a failure in that AZ would result in downtime.

Option B improves database performance and provides a level of fault tolerance, it does not address the scalability aspect of the website platform.

Option C provides both high availability and fault tolerance. Creating an AMI allows for easy replication of the EC2 instance across AZs. Configuring an ALB in two AZs and attaching an ASG ensures scalability and load distribution across multiple instances.

Option D does not provide the high availability and scalability required by the company. Scheduled backups to S3 address data protection but do not contribute to website availability or scalability.

upvoted 1 times

 **Bmarodi** 6 months ago

Selected Answer: C

Option C meets the requirements.

upvoted 1 times

 **ssoffline** 6 months, 1 week ago

Why not D?

Are we just assuming that there will be no write to the db?

upvoted 1 times

 **antropaws** 6 months, 1 week ago

Selected Answer: C

Absolutely C.

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: C

C: This will allow the website platform to be highly available by using Aurora, which provides automatic failover and replication. Additionally, by creating an AMI from the original EC2 instance, the Auto Scaling group can automatically launch new instances in multiple availability zones and use the Application Load Balancer to distribute traffic across them. This way, the website will be able to handle the increased traffic, and will be less likely to go down due to a single point of failure.

upvoted 3 times

A company is launching an application on AWS. The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group. The instances are in an Auto Scaling group for each environment. The company requires a development environment and a production environment. The production environment will have periods of high traffic.

Which solution will configure the development environment MOST cost-effectively?

- A. Reconfigure the target group in the development environment to have only one EC2 instance as a target.
- B. Change the ALB balancing algorithm to least outstanding requests.
- C. Reduce the size of the EC2 instances in both environments.
- D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group.

Correct Answer: A

Community vote distribution

A (58%) D (40%)

 **mhmt4438** Highly Voted  10 months, 2 weeks ago

Selected Answer: D

D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group

This option will configure the development environment in the most cost-effective way as it reduces the number of instances running in the development environment and therefore reduces the cost of running the application. The development environment typically requires less resources than the production environment, and it is unlikely that the development environment will have periods of high traffic that would require a large number of instances. By reducing the maximum number of instances in the development environment's Auto Scaling group, the company can save on costs while still maintaining a functional development environment.

upvoted 11 times

 **JayBee65** 10 months, 1 week ago

No, it will not reduce the number of instances being used, since a minimum of 2 will be used at all times.

upvoted 8 times

 **Chef_couincouin** Most Recent  1 day, 18 hours ago

Answer is A but I'm not agree. We use only one instance with A and D.

But with D, by default, instance is terminated whereas with A, instance still exist.

Answer should be D

upvoted 1 times

 **ravinperera** 4 weeks, 1 day ago

Selected Answer: D

This option is specific to the development environment and focuses on reducing the number of instances that can be spun up during scaling events. This means cost savings because fewer instances will be used even if the scaling policies are triggered.

Given the goal to configure the development environment in the most cost-effective way, without compromising the production environment, the best option is D

upvoted 1 times

 **Mandar15** 2 months ago

Selected Answer: A

Option A

upvoted 1 times

 **TariqKipkemei** 2 months ago

Selected Answer: A

wont think much about this, option A is the most cost effective

upvoted 1 times

 **Its_SaKar** 2 months ago

Selected Answer: A

Option A because it can't be option D as there should be at least two EC2 instances in Auto scaling group, and can't be reduced to one as said in option D.

So, simply reconfigure the target group in the development environment to have only one EC2 instance as a target as said in option A to reduce cost.

upvoted 2 times

 **Its_SaKar** 2 months ago

Selected Answer: D

Option A because it can't be option D as there should be at least two EC2 instances in Auto scaling group, and can't be reduced to one as said in option D.

So, simply reconfigure the target group in the development environment to have only one EC2 instance as a target as said in option A to reduce cost.

upvoted 1 times

✉ **Its_SaKar** 2 months ago

plz remove this comment as i mistakenly voted option D here. I have posted another comment above.

upvoted 1 times

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

Selected Answer: A

A. Reconfigure the target group in the development environment to have only one EC2 instance as a target

upvoted 1 times

✉ **kwang312** 2 months, 3 weeks ago

Selected Answer: A

I choose A but cannot understand this question, which environment handles the traffic? The question is not clearly for have correct answer.

upvoted 1 times

✉ **yhonatan2288** 3 months, 2 weeks ago

Selected Answer: A

El entorno de desarrollo generalmente no necesita manejar la misma cantidad de tráfico que el entorno de producción y, por lo tanto, puede tener una infraestructura más pequeña para ahorrar costos. Al configurar solo una instancia EC2 como objetivo en el grupo de Auto Scaling del entorno de desarrollo, estarás reduciendo los costos operativos al tener menos recursos activos y consumiendo menos instancias EC2.

upvoted 1 times

✉ **cookieMr** 5 months ago

Selected Answer: A

By configuring the target group in the development environment to have only one EC2 instance as a target, you are effectively reducing the resources allocated to that environment. This helps minimize costs by utilizing fewer EC2 instances and associated resources.

Option B does not directly address the cost-effectiveness of the development environment. It focuses on load balancing strategies rather than cost optimization.

Option C may not be the most cost-effective solution unless the current instance sizes are over-provisioned or unnecessary for the application's requirements.

Option D can help reduce costs, but it may impact the environment's ability to handle traffic and scale efficiently, especially during periods of increased load.

Overall, option A provides a cost-effective approach by minimizing the resources allocated to the development environment while still maintaining a functional setup.

upvoted 2 times

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

I think option D is true, only in case we have multiple target groups, but remember in the question it has been mentioned that there is only single target group. If we do what option "D" indicated in a single target group, it will affect the production group too. Therefore, I think option A is more reasonable.

upvoted 1 times

✉ **ChrisAn** 5 months, 3 weeks ago

Selected Answer: A

A# By reducing the number of EC2 instances in the target group of the development environment to just one, you can lower the cost associated with running multiple instances. Since the development environment typically has lower traffic and does not require the same level of availability and scalability as the production environment, having a single instance is sufficient for testing and development purposes.

upvoted 3 times

✉ **markw92** 5 months, 1 week ago

I also thought D is the answer but after careful reading of the question, the current minimum number of ec2 are 2, so even though we reduce the auto scaling group to minimum, it still leaves 2 in dev env. I think A is the answer. Pretty tricky and we have to pay attention to small details.

upvoted 1 times

✉ **Bmarodi** 6 months ago

Selected Answer: A

Option A is most-effective.

upvoted 1 times

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

Selected Answer: A

Just A reduce the cost effectively. D COULD reduce, but not reduce immediately.

upvoted 2 times

 **ErfanKh** 7 months, 2 weeks ago

Selected Answer: A

I am voting A here, there is no need for Autoscaling since we can just set dev environment to 1 EC2 instance which would be the lowest cost.
upvoted 4 times

 **Kenzo** 7 months, 3 weeks ago

Honestly this question is useless, there's nothing wrong with the existing environment
upvoted 2 times

A company runs a web application on Amazon EC2 instances in multiple Availability Zones. The EC2 instances are in private subnets. A solutions architect implements an internet-facing Application Load Balancer (ALB) and specifies the EC2 instances as the target group. However, the internet traffic is not reaching the EC2 instances.

How should the solutions architect reconfigure the architecture to resolve this issue?

- A. Replace the ALB with a Network Load Balancer. Configure a NAT gateway in a public subnet to allow internet traffic.
- B. Move the EC2 instances to public subnets. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.
- C. Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.
- D. Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

Correct Answer: C

Community vote distribution

D (80%)	14%	4%
---------	-----	----

✉  **ktulu2602** Highly Voted 8 months, 4 weeks ago

I think either the question or the answers are not formulated correctly because of this document:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/load-balancer-stickiness/subnets-routing.html>

A - Might be possible but it's quite impractical

B - Not needed as the setup described should work as is provided the SGs of the EC2 instances accept traffic from the ALB

C - Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route - not needed as the EC2 instances would receive the traffic from the ALB ENIs. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0 - the default behaviour of the SG is to allow outbound traffic only.

D - Create public subnets in each Availability Zone. Associate the public subnets with the ALB - if it's a internet facing ALB these should already be in place. Update the route tables for the public subnets with a route to the private subnets - no need as the local prefix entry in the route tables would take care of this point

I'm 110% sure the question or answers or both are wrong. Prove me wrong! :)

upvoted 12 times

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

Completely agreed, I was looking for an option to allow HTTPS traffic on port 443 from the ALB to the EC2 instance's security group.

Either the question or the answers are wrong.

upvoted 5 times

✉  **bdp123** Highly Voted 9 months, 1 week ago

Selected Answer: D

I change my answer to 'D' because of following link:

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

upvoted 11 times

✉  **David_Ang** Most Recent 4 weeks ago

Selected Answer: A

this is a bad formulated question with gaps, but my reason tells me that if you want to connect something from a private subnet to internet you need a NAT (instance or gateway, bastion).

Creating public subnets in each Availability Zone and associating them with the Application Load Balancer (ALB) won't resolve the problem of allowing internet traffic to reach the private EC2 instances. Public subnets are typically used when you want your EC2 instances to have direct internet access, not when you want to keep them in private subnets with indirect access through a load balancer.

upvoted 2 times

✉  **vijaykamal** 2 months ago

Selected Answer: D

ption A (replace ALB with Network Load Balancer and add a NAT gateway) is not the most straightforward solution because it changes the load balancer type and introduces a NAT gateway, which might be unnecessary if the goal is to use an ALB for web traffic. ALBs are commonly used for internet-facing web applications.

Option B (move EC2 instances to public subnets and modify security group rules) involves placing instances in public subnets, which is generally not recommended for security reasons. Additionally, it suggests modifying security group rules for outbound traffic, which might not be the best practice to resolve the issue.

Option C (update route tables and security group rules) addresses the route table update, but it also suggests moving instances to public subnets, which is not ideal from a security perspective.

upvoted 1 times

✉ **TariqKipkemei** 2 months ago

Selected Answer: D

Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

upvoted 2 times

✉ **Its_SaKar** 2 months ago

Selected Answer: D

Option A is incorrect Internet traffic is http and https so it can't be configured to NLB

Option B and option C are incorrect because sending 0.0.0.0/0 is not best practices

Option D is correct because it's the only option left. And updating the route tables for the public subnets with a route to the private subnets ensures internet access to EC2 instances in private subnet.

upvoted 1 times

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

Selected Answer: D

D. is the correct solution. By creating public subnets and associating them with the ALB, inbound internet traffic can reach the ALB. The route tables for the public subnets are updated to include a route to the private subnets, allowing traffic to reach the EC2 instances in the private subnets. This setup enables secure access to the application while allowing internet traffic to reach the EC2 instances through the ALB.

upvoted 1 times

✉ **A1975** 4 months ago

Selected Answer: D

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-example-private-subnets-nat.html>

upvoted 2 times

✉ **cookieMr** 5 months ago

Selected Answer: D

A. suggests using a different type of load balancer and configuring a NAT gateway, but it does not address the issue of internet traffic reaching the EC2 instances.

B. suggests exposing the EC2 instances to the public internet, which may pose security risks and does not address the issue of inbound internet traffic reaching the instances.

C. suggests configuring the EC2 instances to have outbound internet access, but it does not solve the problem of inbound internet traffic reaching the instances.

D. is the correct solution. By creating public subnets and associating them with the ALB, inbound internet traffic can reach the ALB. The route tables for the public subnets are updated to include a route to the private subnets, allowing traffic to reach the EC2 instances in the private subnets. This setup enables secure access to the application while allowing internet traffic to reach the EC2 instances through the ALB.

upvoted 3 times

✉ **Vinhkewl** 5 months ago

Should be C

It would normally make sense to segregate your ALBs into public or private zones by security group and target group, but this is configuration rather than architectural placement - there is nothing preventing you from adding a rule to route specific paths or ports to a public subnet from an ALB that has until then been serving private subnets only.

upvoted 1 times

✉ **Abrar2022** 5 months, 3 weeks ago

Selected Answer: D

To attach Amazon EC2 instances that are located in a private subnet, first create public subnets

upvoted 4 times

✉ **Bmarodi** 6 months ago

Selected Answer: D

I vote with the option D.

upvoted 1 times

✉ **antropaws** 6 months, 1 week ago

D is not quite accurate because subnets in a VPC have a local route by default, meaning that all subnets are able to communicate with each other: "Every route table contains a local route for communication within the VPC. This route is added by default to all route tables". This question is poorly formulated.

upvoted 2 times

✉ **kraken21** 8 months ago

Selected Answer: D

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

upvoted 2 times

✉ **Theodorz** 8 months, 4 weeks ago

Selected Answer: C

I think C would be correct answer.
upvoted 1 times

 **AYap** 9 months, 1 week ago

Answer: D
<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>
upvoted 3 times

 **bdp123** 9 months, 2 weeks ago

Selected Answer: C

Just need to configure the outbound path from the servers back out to the Internet. Inbound path is already configured
upvoted 1 times

A company has deployed a database in Amazon RDS for MySQL. Due to increased transactions, the database support team is reporting slow reads against the DB instance and recommends adding a read replica.

Which combination of actions should a solutions architect take before implementing this change? (Choose two.)

- A. Enable binlog replication on the RDS primary node.
- B. Choose a failover priority for the source DB instance.
- C. Allow long-running transactions to complete on the source DB instance.
- D. Create a global table and specify the AWS Regions where the table will be available.
- E. Enable automatic backups on the source instance by setting the backup retention period to a value other than 0.

Correct Answer: AC

Community vote distribution

CE (83%)	Other
----------	-------

✉️  **fkie4** Highly Voted 8 months, 3 weeks ago

Who would know this stuff man...

upvoted 55 times

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

"Allow long-running transactions to complete on the source DB instance." -- Makes sense / Also a backup before changing anything again made a sense.

upvoted 1 times

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

exactly

upvoted 1 times

✉️  **KelvinEM** Highly Voted 10 months, 2 weeks ago

C,E

"An active, long-running transaction can slow the process of creating the read replica. We recommend that you wait for long-running transactions to complete before creating a read replica. If you create multiple read replicas in parallel from the same source DB instance, Amazon RDS takes only one snapshot at the start of the first create action."

When creating a read replica, there are a few things to consider. First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica"

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

upvoted 33 times

✉️  **xdkonorek2** Most Recent 4 days, 23 hours ago

Selected Answer: AE

A - it's essential for continuous replication

E - it's essential for setting up replication, initial data in replica is based on latest backup

other options:

B - we're not designing for HA, and it's related to multi-AZ RDS deployments

C - is this needed for adding read replica?

D - it's not a dynamodb to create global table

upvoted 1 times

✉️  **vijaykamal** 2 months ago

Selected Answer: CE

A. Enabling binlog replication is not something you need to do manually before creating a read replica. Amazon RDS for MySQL manages replication internally, and it's not necessary to enable binlog replication explicitly.

B. Choosing a failover priority is related to Multi-AZ configurations and automatic failover, but it is not specifically required when adding a read replica.

D. Creating a global table and specifying AWS Regions is related to Aurora Global Databases, which is not the same as creating a read replica for a standard RDS instance.

upvoted 1 times

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

Selected Answer: CE

**C. Long-running transactions can prevent the read replica from catching up with the source DB instance. Allowing these transactions to complete before creating the read replica can help ensure that the replica is able to stay synchronized with the source.

**E. Automatic backups must be enabled on the source DB instance for read replicas to be created. This is done by setting the backup retention period to a value other than 0.

upvoted 1 times

✉ **cd93** 3 months, 2 weeks ago

Bin log (binary log) is a specific terminology to MySQL, it is a write-only file that logs all history and used for purposes such as point-in-time recovery and transaction replication.

Option A is technically correct but on AWS RDS, this MySQL feature is turned on by setting backup retention period > 0, that is why we must enable backup before replication can work (for MySQL, at least) => Option E is the more general answer for AWS RDS.

Option C is just a recommendation from AWS official documentation, it is there to prevent data mismatch on primary and secondaries when the long-running transactions have not been complete yet.

upvoted 1 times

✉ **A1975** 4 months ago

Selected Answer: CE

Before a MySQL DB instance can serve as a replication source, make sure to enable automatic backups on the source DB instance. To do this, set the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica. Automatic backups are supported for read replicas running any version of MySQL. You can configure replication based on binary log coordinates for a MySQL DB instance

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html

upvoted 1 times

✉ **StacyY** 4 months ago

A E. Binlog is needed for on-going replication setup and DB backup is needed for setup the replication DB

upvoted 1 times

✉ **Mmmmmmkkkk** 4 months, 4 weeks ago

Correction: c and e

upvoted 1 times

✉ **Mmmmmmkkkk** 4 months, 4 weeks ago

A and e

upvoted 1 times

✉ **cookieMr** 5 months ago

Selected Answer: CE

A. enables the binary log replication feature on the RDS primary node, which is necessary for setting up a read replica.

B. determines the order in which DB instances are promoted to the primary role during a failover scenario. It is not directly related to adding a read replica to address slow reads.

C. ensures that any ongoing transactions on the source DB instance are allowed to finish before implementing the change. It helps maintain data integrity and consistency during the transition to the read replica.

D. is a feature specific to DynamoDB. It allows for multi-region replication and high availability in DynamoDB, but it is not applicable in this scenario.

E. ensures that regular backups are taken for the source DB instance. This is important for data protection and recovery purposes, as it allows for point-in-time restoration in case of any issues during or after the addition of the read replica.

upvoted 1 times

✉ **Abrar2022** 5 months, 3 weeks ago

Selected Answer: CE

Before adding read replicas, one needs to allow long-running transactions to complete on the source DB instance otherwise you might end up interrupting transactions. Then, you should enable automatic backups on the source instance and set the backup retention period to a value other than 0.

upvoted 1 times

✉ **Bmarodi** 6 months ago

Selected Answer: CE

The combination of actions should a solutions architect take before implementing this change are options C & E.

upvoted 1 times

✉ **omoakin** 6 months ago

AAAAAAAAAAAA EEEEEEEEEEEEEE

upvoted 1 times

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

Selected Answer: CE

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html#USER_ReadRepl.Create
upvoted 1 times

✉ **bdp123** 9 months, 2 weeks ago

Selected Answer: CE

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html#USER_ReadRepl.Create
upvoted 2 times

✉ **bdp123** 9 months, 4 weeks ago

Selected Answer: CE

When creating a Read Replica, there are a few things to consider. First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a Read Replica that is the source DB instance for another Read Replica.

After you enable automatic backups by modifying your read replica instance to have a backup retention period greater than 0 days, you'll find that the log_bin and binlog_format will align itself with the configuration specified in your parameter group dynamically and will not require the RDS instance to be restarted. You will also be able to create a read replica from your read replica instance with no further modification requirements.

<https://blog.pythian.com/enabling-binary-logging-rds-read-replica/>

upvoted 2 times

A company runs analytics software on Amazon EC2 instances. The software accepts job requests from users to process data that has been uploaded to Amazon S3. Users report that some submitted data is not being processed. Amazon CloudWatch reveals that the EC2 instances have a consistent CPU utilization at or near 100%. The company wants to improve system performance and scale the system based on user load.

What should a solutions architect do to meet these requirements?

- A. Create a copy of the instance. Place all instances behind an Application Load Balancer.
- B. Create an S3 VPC endpoint for Amazon S3. Update the software to reference the endpoint.
- C. Stop the EC2 instances. Modify the instance type to one with a more powerful CPU and more memory. Restart the instances.
- D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

Correct Answer: D

Community vote distribution

D (93%) 7%

 **mhmt4438** Highly Voted 10 months, 2 weeks ago

Selected Answer: D

D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

By routing incoming requests to Amazon SQS, the company can decouple the job requests from the processing instances. This allows them to scale the number of instances based on the size of the queue, providing more resources when needed. Additionally, using an Auto Scaling group based on the queue size will automatically scale the number of instances up or down depending on the workload. Updating the software to read from the queue will allow it to process the job requests in a more efficient manner, improving the performance of the system.

upvoted 9 times

 **TariqKipkemei** Most Recent 2 months ago

Selected Answer: D

Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

upvoted 1 times

 **Kill3rasp3r** 3 months, 1 week ago

Selected Answer: D

I would vote A if it was ALB targeting an EC2 auto scaling group.
I would vote D if the auto scaling group was based on CPU utilization rather than queue size.
So I think both answers are wrong but D is okay enough.

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: D

A. Creating a copy of the instance and placing all instances behind an ALB does not address the high CPU utilization issue or provide scalability based on user load.

B. Creating an S3 VPC endpoint for S3 and updating the software to reference the endpoint improves network performance but does not address the high CPU utilization or provide scalability based on user load.

C. Stopping the EC2 instances and modifying the instance type to one with a more powerful CPU and more memory may improve performance, but it does not address scalability based on user load.

D. Routing incoming requests to SQS, configuring an EC2 ASG based on queue size, and updating the software to read from the queue improves system performance and provides scalability based on user load.

Therefore, option D is the correct choice as it addresses the high CPU utilization, improves system performance, and enables scalability based on user load.

upvoted 1 times

 **WherecanIstart** 8 months, 3 weeks ago

Selected Answer: D

Autoscaling Group and SQS solves the problem.
SQS - Decouples the process
ASG - Autoscales the EC2 instances based on usage
upvoted 1 times

 **ak1ak** 9 months ago

Selected Answer: A

its definitely A
upvoted 1 times

 **wRhlH** 6 months, 1 week ago

You don't "scale the system by load" by choosing A
upvoted 1 times

 **AHUI** 10 months, 2 weeks ago

D is correct. Decouple the process. autoscale the EC2 based on query size. best choice
upvoted 3 times

 **Aninina** 10 months, 2 weeks ago

I think it's A " A. Create a copy of the instance. Place all instances behind an Application Load Balancer.
upvoted 1 times

A company is implementing a shared storage solution for a media application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.

Which AWS solution meets these requirements?

- A. Create an AWS Storage Gateway volume gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- B. Create an AWS Storage Gateway tape gateway. Configure tapes to use Amazon S3. Connect the application server to the tape gateway.
- C. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: D

Community vote distribution

D (100%)

✉  **Morinator** Highly Voted 10 months, 2 weeks ago

Selected Answer: D

SMB + fully managed = fsx for windows imo
upvoted 10 times

✉  **TariqKipkemei** Most Recent 2 months ago

Selected Answer: D

SMB = Amazon FSx for Windows File Server
upvoted 1 times

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

Selected Answer: D

D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system
upvoted 1 times

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

All who selected D. are correct - see more details from our community
upvoted 1 times

✉  **animefan1** 4 months, 4 weeks ago

Selected Answer: D

Fsx is fully managed. Plus it supports SMB protocol
upvoted 1 times

✉  **cookieMr** 5 months ago

Selected Answer: D

A. involves using Storage Gateway, but it does not specifically mention support for SMB clients. It may not meet the requirement of using SMB clients to access data.

B. involves using Storage Gateway with tape gateway configuration, which is primarily used for archiving data to S3. It does not provide native support for SMB clients to access data.

C. involves manually setting up and configuring a Windows file share on an EC2 Windows instance. While it allows SMB clients to access data, it is not a fully managed solution as it requires manual setup and maintenance.

D. involves creating an FSx for Windows File Server file system, which is a fully managed Windows file system that supports SMB clients. It provides an easy-to-use shared storage solution with native SMB support.

Based on the requirements of using SMB clients and needing a fully managed solution, option D is the most suitable choice.

upvoted 2 times

✉  **devonwho** 10 months ago

Selected Answer: D

Amazon FSx has native support for Windows file system features and for the industry-standard Server Message Block (SMB) protocol to access file storage over a network.

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>

upvoted 4 times

✉ **LuckyAro** 10 months, 1 week ago

Selected Answer: D

Amazon FSx for Windows File Server file system

upvoted 1 times

✉ **techhb** 10 months, 2 weeks ago

amazon fsx for smb connectivity.

upvoted 1 times

✉ **Aninina** 10 months, 2 weeks ago

Selected Answer: D

FSX is the ans

upvoted 1 times

✉ **mhmt4438** 10 months, 2 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/81115-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

✉ **bamishr** 10 months, 2 weeks ago

Selected Answer: D

D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.

upvoted 1 times

A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.

What should a solutions architect do to meet these requirements when configuring the logs?

- A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days
- B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
- C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
- D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Correct Answer: A*Community vote distribution*

D (93%)	7%
---------	----

 **LuckyAro** Highly Voted 10 months, 1 week ago

Selected Answer: D

D is the correct answer.

upvoted 5 times

 **TariqKipkemei** Most Recent 2 months ago

Selected Answer: D

Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

upvoted 1 times

 **animefan1** 4 months, 4 weeks ago

Selected Answer: D

S3 will store logs. With life cycle, we can move it to different class. With Option A, log groups expiration will simply remove the logs and failing the 2nd request in question

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: D

A. suggests using CloudWatch as the target for VPC Flow Logs. However, it does not provide a mechanism for managing the retention of the logs for 90 days and then accessing them intermittently.

B. suggests using Kinesis as the target for VPC Flow Logs. While it can retain the logs for 90 days, it does not address the requirement for intermittent access to the logs.

C. suggests using CloudTrail as the target for VPC Flow Logs. However, CloudTrail is designed for auditing and monitoring API activity, not for capturing network traffic logs. It does not meet the requirement of capturing VPC Flow Logs.

D. suggests using S3 as the target for VPC Flow Logs and leveraging S3 Lifecycle policies to transition the logs to a cost-effective storage class after 90 days. It meets the requirement of retaining the logs for 90 days and provides the flexibility for intermittent access while optimizing storage costs.

upvoted 3 times

 **markw92** 5 months, 1 week ago

A doesn't solve "90 days and then accessed intermittently" this statement. It sets expire after 90. Not sure otherwise A seems to be right choice since you can create dashboards etc.

upvoted 1 times

 **Bmarodi** 6 months ago

Selected Answer: A

Option A meets these requirements.

upvoted 1 times

 **ocbn3wby** 9 months, 3 weeks ago

Selected Answer: D

There's a table here that specifies that VPC Flow logs can go directly to S3. Does not need to go via CloudTrail and then to S3. Nor via CW.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AWS-logs-and-resource-policy.html#AWS-logs-infrastructure-S3>

upvoted 3 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: D

we need to preserve logs hence D

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogsConcepts.html>

upvoted 2 times

 **mp165** 10 months, 2 weeks ago

Selected Answer: D

D...agree that retention is the key word

upvoted 2 times

 **swolfgang** 10 months, 2 weeks ago

Selected Answer: D

a is not,retantion means delete after 90 days but questions say rarely access.

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: D

D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

By using Amazon S3 as the target for the VPC Flow Logs, the logs can be easily stored and accessed by the security team. Enabling an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days will automatically move the logs to a storage class that is optimized for infrequent access, reducing the storage costs for the company. The security team will still be able to access the logs as needed, even after they have been transitioned to S3 Standard-IA, but the storage cost will be optimized.

upvoted 4 times

 **laicos** 10 months, 2 weeks ago

Selected Answer: D

I prefer D

"accessed intermittently" need logs after 90 days

upvoted 1 times

 **Parsons** 10 months, 2 weeks ago

Selected Answer: D

No, D should be is correct.

"The logs will be frequently accessed for 90 days and then accessed intermittently." => We still need to store instead of deleting as the answer A.

upvoted 2 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: D

D looks correct. This will meet the requirements of frequently accessing the logs for the first 90 days and then intermittently accessing them after that. S3 standard-IA is a storage class that is less expensive than S3 standard for infrequently accessed data, so it would be a more cost-effective option for storing the logs after the first 90 days.

upvoted 1 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: A

Cloudwatch for this

<https://www.examtopics.com/discussions/amazon/view/59983-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.

What should a solutions architect do to meet these requirements?

- A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.
- B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.
- C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the NAT instance as the default route.
- D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

Correct Answer: B

Community vote distribution

B (88%) 6%

✉  **mhmt4438**  10 months, 2 weeks ago

Selected Answer: B

B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.

This approach will allow the EC2 instance to access the internet and download the monthly security updates while still being located in a private subnet. By creating a NAT gateway and placing it in a public subnet, it will allow the instances in the private subnet to access the internet through the NAT gateway. And then, configure the private subnet route table to use the NAT gateway as the default route. This will ensure that all outbound traffic is directed through the NAT gateway, allowing the EC2 instance to access the internet while still maintaining the security of the private subnet.

upvoted 7 times

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

NAT gateway does not allow internet on its own. It needs internet gateway too. None of the answers make sense

upvoted 8 times

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

refer below link

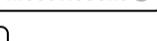
<https://aws.amazon.com/about-aws/whats-new/2021/06/aws-removes-nat-gateways-dependence-on-internet-gateway-for-private-communications/>

upvoted 2 times

✉  **TOR_0511** 4 days, 12 hours ago

lol, that's for 'private connections'

upvoted 1 times

✉  **xdkonorek2**  4 days, 22 hours ago

Selected Answer: C

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

Public subnet – The subnet has a direct route to an internet gateway. Resources in a public subnet can access the public internet.

Private subnet – The subnet does not have a direct route to an internet gateway. Resources in a private subnet require a NAT device to access the public internet.

Both B and C have caveats but are both viable:

C - NAT Instance is used as a NAT device instead of NAT gateway, but it's still viable option

B - Have 2 redundant components - IGW and public subnet, and NAT gateway still would route traffic to IGW, and if VPC is a custom VPC routing has to be set up

upvoted 1 times

✉  **oluolope** 1 month, 1 week ago

Selected Answer: D

A NAT Gateway should have one interface in each network it is connected to. I don't understand what it means when they say it is located either in the private or in the public network. It should be in both. Therefore, B and D do not really make sense.

I choose D over B because there is a requirement to access the internet and although it is possible for the NAT to exist without an internet gateway, the later is still needed when internet access is required which is the case in this scenario.

upvoted 1 times

✉  **TariqKipkemei** 2 months ago

Selected Answer: B

Internet Gateway is required anyway to access the internet.

Option B makes more sense: Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: B

B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.

upvoted 1 times

 **cookieMr** 5 months ago

A. provides direct internet access to the private subnet, which is not desired in this case as the goal is to restrict outbound internet access.

B. allows the EC2 in the private subnet to access the internet through the NAT gateway, which acts as a proxy. It provides controlled outbound internet access while maintaining the security of the private subnet.

C. is similar to using a NAT gateway, but it involves using a NAT instance. NAT instances require more manual configuration and management compared to NAT gateways, making them a less preferred option.

D. combines the use of an internet gateway and a NAT instance, which is not necessary. It introduces unnecessary complexity and adds a NAT instance that requires additional management.

Overall, option B is the most appropriate solution as it utilizes a NAT gateway placed in a public subnet to enable controlled outbound internet access for the EC2 instance in the private subnet.

NAT Gateways are preferred over NAT Instances by AWS and in general.

upvoted 3 times

 **Bmarodi** 6 months ago

Selected Answer: B

Option B meets the requirements, hence B is right choice.

upvoted 1 times

 **Manjunathkb** 7 months, 2 weeks ago

D would have been the answer if NAT gateway is installed in public subnet and not where EC2 is located. None of the answers are correct.

upvoted 1 times

 **AlessandraSAA** 8 months, 3 weeks ago

why not C?

upvoted 1 times

 **UnluckyDucky** 8 months, 2 weeks ago

Because NAT Gateways are preferred over NAT Instances by AWS and in general.

I have yet to find a situation where a NAT Instance would be more applicable than NAT Gateway which is fully managed and is overall an easier solution to implement - both in AWS questions or the real world.

upvoted 2 times

 **TungPham** 9 months, 3 weeks ago

Selected Answer: B

Require NAT gateway

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: B

Answer explained here <https://medium.com/@tshemku/aws-internet-gateway-vs-nat-gateway-vs-nat-instance-30523096df22>

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: B

NAT Gateway is right choice

upvoted 1 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/59966-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

A solutions architect needs to design a system to store client case files. The files are core company assets and are important. The number of files will grow over time.

The files must be simultaneously accessible from multiple application servers that run on Amazon EC2 instances. The solution must have built-in redundancy.

Which solution meets these requirements?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon S3 Glacier Deep Archive
- D. AWS Backup

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

my choice is A but I think a better alternative would be S3 standard if offered wouldn't it be?
upvoted 1 times

✉️  **TariqKipkemei** 2 months ago

Selected Answer: A

File system, scalable, multiple access = Amazon Elastic File System (Amazon EFS)
upvoted 1 times

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

Selected Answer: A

Amazon Elastic File System (Amazon EFS)
upvoted 1 times

✉️  **cookieMr** 5 months ago

Selected Answer: A

EFS provides a scalable and fully managed file storage service that can be accessed concurrently from multiple EC2. It offers built-in redundancy by storing data across multiple AZs within a region. With EFS, the client case files can be accessed by multiple application servers simultaneously, ensuring high availability and scalability as the number of files grows over time.

Option B, EBS, is a block-level storage service that is typically used for attaching to individual EC2 and does not provide concurrent access to multiple instances, making it unsuitable for this scenario.

Option C, S3 Glacier Deep Archive, is a long-term archival storage service and may not be suitable for active file access and simultaneous access from multiple application servers.

Option D, AWS Backup, is a centralized backup management service and does not provide the required simultaneous file access and redundancy features.

Therefore, the most suitable solution is Amazon EFS (option A).

upvoted 4 times

✉️  **Bmarodi** 6 months ago

Selected Answer: A

Option A meets the requirements, hence A is correct answer.
upvoted 1 times

✉️  **moiraqi** 6 months, 1 week ago

What does "The solution must have built-in redundancy" mean
upvoted 1 times

✉️  **KZM** 9 months ago

If the application servers are running on Linux or UNIX operating systems, EFS is the most suitable solution for the given requirements.
upvoted 1 times

 **TungPham** 9 months, 3 weeks ago

Selected Answer: A

"accessible from multiple application servers that run on Amazon EC2 instances"

upvoted 3 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: A

EFS Amazon Elastic File System (EFS) automatically grows and shrinks as you add and remove files with no need for management or provisioning.

upvoted 4 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/68833-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.

Policy 1

```
{
  "Version": "2012-10-17",  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:Get*",
        "iam>List*",
        "kms>List*",
        "ec2:*",
        "ds:*",
        "logs:Get*",
        "logs:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Policy 2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ds>Delete*",
      "Resource": "*"
    }
  ]
}
```

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

- A. Deleting IAM users
- B. Deleting directories
- C. Deleting Amazon EC2 instances
- D. Deleting logs from Amazon CloudWatch Logs

Correct Answer: C

Community vote distribution

C (100%)

 **JayBee65** Highly Voted 10 months, 1 week ago

ec2:* Allows full control of EC2 instances, so C is correct

The policy only grants get and list permission on IAM users, so not A

ds>Delete deny denies delete-directory, so not B, see <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ds/index.html>

The policy only grants get and describe permission on logs, so not D

upvoted 8 times

 **TariqKipkemei** Most Recent 2 months ago

Selected Answer: C

Deleting Amazon EC2 instances

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: C

C : Deleting Amazon EC2 instances

upvoted 1 times

✉  **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 2 times

✉  **Aninina** 10 months, 2 weeks ago

C : Deleting Amazon EC2 instances

upvoted 1 times

✉  **bamishr** 10 months, 2 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/27873-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

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

Selected Answer: C

Explicit deny on directories, only available action for deleting is EC2

upvoted 3 times

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

- A. Create security group rules using the instance ID as the source or destination.
- B. Create security group rules using the security group ID as the source or destination.
- C. Create security group rules using the VPC CIDR blocks as the source or destination.
- D. Create security group rules using the subnet CIDR blocks as the source or destination.

Correct Answer: B

Community vote distribution

B (100%)

 **Aninina** Highly Voted 10 months, 2 weeks ago

Selected Answer: B

B. Create security group rules using the security group ID as the source or destination.

This way, the security team can ensure that the least privileged access is given to the application tiers by allowing only the necessary communication between the security groups. For example, the web tier security group should only allow incoming traffic from the load balancer security group and outgoing traffic to the application tier security group. This approach provides a more granular and secure way to control traffic between the different tiers of the application and also allows for easy modification of access if needed.

It's also worth noting that it's good practice to minimize the number of open ports and protocols, and use security groups as a first line of defense, in addition to network access control lists (ACLs) to control traffic between subnets.

upvoted 7 times

 **Wael216** Highly Voted 9 months ago

Selected Answer: B

By using security group IDs, the ingress and egress rules can be restricted to only allow traffic from the necessary source or destination, and to deny all other traffic. This ensures that only the minimum required traffic is allowed between the application tiers.

Option A is not the best choice because using the instance ID as the source or destination would allow traffic from any instance with that ID, which may not be limited to the specific application tier.

Option C is also not the best choice because using VPC CIDR blocks would allow traffic from any IP address within the VPC, which may not be limited to the specific application tier.

Option D is not the best choice because using subnet CIDR blocks would allow traffic from any IP address within the subnet, which may not be limited to the specific application tier.

upvoted 5 times

 **Guru4Cloud** Most Recent 2 months, 2 weeks ago

Selected Answer: B

Create security group rules using the security group ID as the source or destination.

This way, the security team can ensure that the least privileged access is given to the application tiers by allowing only the necessary communication between the security groups. For example, the web tier security group should only allow incoming traffic from the load balancer security group and outgoing traffic to the application tier security group. This approach provides a more granular and secure way to control traffic between the different tiers of the application and also allows for easy modification of access if needed.

It's also worth noting that it's good practice to minimize the number of open ports and protocols, and use security groups as a first line of defense, in addition to network access control lists (ACLs) to control traffic between subnets.

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: B

A. would limit the traffic based on specific instances, which may not be the most suitable solution for applying the principle of least privilege between application tiers.

B. By using security group IDs in the rules, you can precisely control the traffic between application tiers, allowing only the necessary communication and adhering to the principle of least privilege.

C. would apply broad rules based on the entire VPC CIDR blocks, which may not provide the necessary level of granularity required for secure communication between specific application tiers.

D. would limit the traffic based on subnet CIDR blocks, which may not be sufficient for ensuring proper security between application tiers.

In summary, using security group IDs (Option B) is the recommended approach as it allows for precise control of traffic between application tiers, aligning with the principle of least privilege.

upvoted 3 times

 **Bmarodi** 6 months ago

Selected Answer: B

I vote for option B.

upvoted 1 times

 **LuckyAro** 10 months, 1 week ago

Selected Answer: B

. Create security group rules using the security group ID as the source or destination

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Security Group Rulesapply to instances

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: B

Correct answer is B

upvoted 2 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/46463-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: B

B right

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>

upvoted 1 times

A company has an ecommerce checkout workflow that writes an order to a database and calls a service to process the payment. Users are experiencing timeouts during the checkout process. When users resubmit the checkout form, multiple unique orders are created for the same desired transaction.

How should a solutions architect refactor this workflow to prevent the creation of multiple orders?

- A. Configure the web application to send an order message to Amazon Kinesis Data Firehose. Set the payment service to retrieve the message from Kinesis Data Firehose and process the order.
- B. Create a rule in AWS CloudTrail to invoke an AWS Lambda function based on the logged application path request. Use Lambda to query the database, call the payment service, and pass in the order information.
- C. Store the order in the database. Send a message that includes the order number to Amazon Simple Notification Service (Amazon SNS). Set the payment service to poll Amazon SNS, retrieve the message, and process the order.
- D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.

Correct Answer: D

Community vote distribution

D (100%)

 **Aninina** Highly Voted 10 months, 2 weeks ago

Selected Answer: D

D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.
This approach ensures that the order creation and payment processing steps are separate and atomic. By sending the order information to an SQS FIFO queue, the payment service can process the order one at a time and in the order they were received. If the payment service is unable to process an order, it can be retried later, preventing the creation of multiple orders. The deletion of the message from the queue after it is processed will prevent the same message from being processed multiple times.
It's worth noting that FIFO queues guarantee that messages are processed in the order they are received, and prevent duplicates.

upvoted 7 times

 **TariqKipkemei** Most Recent 2 months ago

Selected Answer: D

if the backend can not keep up, queue the tasks.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.

upvoted 1 times

 **animefan1** 4 months, 4 weeks ago

Selected Answer: D

The question is related in breaking down the flow. SQS is go-to choice to decouple & DB will be used to store

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: D

A. is not a suitable solution for preventing the creation of multiple orders. This approach does not guarantee the sequential and reliable processing of orders.

B. is not an appropriate solution for preventing the creation of multiple orders. CloudTrail is primarily used for logging and auditing API activity, and invoking a Lambda based on the logged request does not ensure the correct order processing.

C. is not a suitable solution. SNS is a publish-subscribe messaging service, and polling it may result in delayed processing and potential order duplication.

D. is the correct solution. Using an SQS FIFO ensures that the orders are processed in a sequential and reliable manner, preventing the creation of multiple orders for the same transaction.

upvoted 4 times

 **antropaws** 5 months, 1 week ago

Why not A?

upvoted 1 times

 **Wael216** 9 months ago

Selected Answer: D

The use of a FIFO queue in Amazon SQS ensures that messages are processed in the order they are received.

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/95026-exam-aws-certified-solutions-architect-associate-saa-c03/>

upvoted 3 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: D

asnwer is d

upvoted 2 times

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Correct Answer: BD

Community vote distribution

BD (100%)

 **TariqKipkemei** 2 months ago

Selected Answer: BD

Prevent accidental deletion of the documents = Enable MFA Delete on the bucket
Ensure that all versions of the documents are available = Enable versioning on the bucket
upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: BD

Options B & D are the correct answers.
upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: BD

B. allows multiple versions of objects in the S3 bucket to be stored. This ensures that all versions of the documents are available, even if they are accidentally overwritten or deleted.

D. adds an extra layer of protection against accidental deletion of objects in the bucket. With MFA Delete enabled, a user would need to provide an additional authentication factor to successfully delete objects from the bucket. This helps prevent accidental or unauthorized deletions and provides an extra level of security for critical documents.

A. would restrict users from modifying or uploading documents. It would not meet the requirement of allowing users to download, modify, and upload documents.

C. can control access permissions to the bucket, it does not specifically address the requirement of preventing accidental deletion or ensuring availability of all versions of the documents.

E. Encryption focuses on data protection rather than versioning and deletion prevention.

upvoted 3 times

 **Bmarodi** 6 months ago

Selected Answer: BD

Options B & D are the correct answers.
upvoted 1 times

 **Wael216** 9 months ago

Selected Answer: BD

no doubts
upvoted 2 times

 **MinHyeok** 9 months, 2 weeks ago

아몰랑 ㅇㅁㄹ ㅇㅁㄹ

upvoted 3 times

 **akdavsan** 10 months, 1 week ago

Selected Answer: BD

b and d ofc

upvoted 1 times

✉  **LuckyAro** 10 months, 1 week ago

Selected Answer: BD

B & D Definitely.

upvoted 1 times

✉  **david76x** 10 months, 1 week ago

Selected Answer: BD

B & D is correct

upvoted 1 times

✉  **Aninina** 10 months, 2 weeks ago

Selected Answer: BD

B and D for sure guys

upvoted 2 times

✉  **mhmt4438** 10 months, 2 weeks ago

Selected Answer: BD

<https://www.examtopics.com/discussions/amazon/view/21969-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

A company is building a solution that will report Amazon EC2 Auto Scaling events across all the applications in an AWS account. The company needs to use a serverless solution to store the EC2 Auto Scaling status data in Amazon S3. The company then will use the data in Amazon S3 to provide near-real-time updates in a dashboard. The solution must not affect the speed of EC2 instance launches.

How should the company move the data to Amazon S3 to meet these requirements?

- A. Use an Amazon CloudWatch metric stream to send the EC2 Auto Scaling status data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
- B. Launch an Amazon EMR cluster to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
- C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.
- D. Use a bootstrap script during the launch of an EC2 instance to install Amazon Kinesis Agent. Configure Kinesis Agent to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

Correct Answer: A

Community vote distribution

A (75%)

C (25%)

 **TariqKipkemei** 2 months ago

Selected Answer: A

You can use metric streams to continually stream CloudWatch metrics to a destination of your choice, with near-real-time delivery and low latency. Supported destinations include AWS destinations such as Amazon Simple Storage Service and several third-party service provider destinations. Main usage scenarios for CloudWatch metric streams: Data lake—Create a metric stream and direct it to an Amazon Kinesis Data Firehose delivery stream that delivers your CloudWatch metrics to a data lake such as Amazon S3.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Metric-Streams.html#:~:text=CloudWatch%20metric%20streams>

upvoted 2 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

This solution meets the requirements because it is serverless and does not affect the speed of EC2 instance launches. Amazon CloudWatch metric streams can continuously stream CloudWatch metrics to destinations such as Amazon S3. Amazon Kinesis Data Firehose can capture, transform, and deliver streaming data into data lakes, data stores, and analytics services. It can directly put the data into Amazon S3, which can then be used for near-real-time updates in a dashboard.

upvoted 2 times

 **Valder21** 2 months, 3 weeks ago

Selected Answer: C

Kinesis is for data streams not events. So, C

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: A

B. introduces unnecessary complexity and overhead for collecting and sending the EC2 Auto Scaling status data to S3. It is not the most efficient serverless solution for this specific requirement.

C. would introduce delays in data updates, as it is not triggered in real-time. Additionally, it adds unnecessary overhead and complexity compared to using a direct data stream.

D. introduces additional dependencies and management overhead. It may also impact the speed of EC2 instance launches, which is a requirement that needs to be avoided.

Overall, option A provides a streamlined and serverless solution by leveraging CloudWatch metric streams and Kinesis Data Firehose to efficiently capture and store the EC2 Auto Scaling status data in S3 without affecting the speed of EC2 instance launches.

upvoted 2 times

 **markw92** 5 months, 1 week ago

A: I was thinking D is the answer but the solution should not impact ec2 launches will make the difference and i fast read the question. A is a right choice.

upvoted 1 times

 **Rahulbit34** 6 months, 3 weeks ago

A because of near real time scenario
upvoted 3 times

 **UnluckyDucky** 8 months, 2 weeks ago

Selected Answer: C

Both A and C are applicable - no doubt there.

C is more straightforward and to the point of the question imho.

upvoted 3 times

 **UnluckyDucky** 8 months, 2 weeks ago

Changing my answer to *A* as the dashboard will provide near-real updates.

Unless the lambda is configured to run every minute which is not common with schedules - it is not considered near real-time.

upvoted 3 times

 **bdp123** 9 months, 2 weeks ago

Selected Answer: A

Serverless solution and near real time
upvoted 2 times

 **Stanislav4907** 9 months, 2 weeks ago

Selected Answer: A

near real time -eliminates c
upvoted 1 times

 **akashkumar1999** 9 months, 3 weeks ago

Selected Answer: A

Answer is A
upvoted 1 times

 **devonwho** 10 months ago

Selected Answer: A

You can use metric streams to continually stream CloudWatch metrics to a destination of your choice, with near-real-time delivery and low latency. One of the use cases is Data Lake: create a metric stream and direct it to an Amazon Kinesis Data Firehose delivery stream that delivers your CloudWatch metrics to a data lake such as Amazon S3.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Metric-Streams.html>

upvoted 2 times

 **Stanislav4907** 10 months ago

Selected Answer: A

Option C, using an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule to send the EC2 Auto Scaling status data directly to Amazon S3, may not be the best choice because it may not provide real-time updates to the dashboard.

A schedule-based approach with an EventBridge rule and Lambda function may not be able to deliver the data in near real-time, as the EC2 Auto Scaling status data is generated dynamically and may not always align with the schedule set by the EventBridge rule.

Additionally, using a schedule-based approach with EventBridge and Lambda also has the potential to create latency, as there may be a delay between the time the data is generated and the time it is sent to S3.

In this scenario, using Amazon CloudWatch and Kinesis Data Firehose as described in Option A, provides a more reliable and near real-time solution.

upvoted 1 times

 **MikelH93** 10 months ago

Selected Answer: A

A seems to be the right answer. Don't think C could be correct as it says "near real-time" and C is on schedule

upvoted 1 times

 **KAUS2** 10 months ago

Selected Answer: C

C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: A

A seemsright choice but serverless keyword confuses, and cloud watch metric steam is server less too.

upvoted 2 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: A

A. Use an Amazon CloudWatch metric stream to send the EC2 Auto Scaling status data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C

C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.

This approach will use a serverless solution (AWS Lambda) which will not affect the speed of EC2 instance launches. It will use the EventBridge rule to invoke the Lambda function on schedule to send the data to S3. This will meet the requirement of near-real-time updates in a dashboard as well. The Lambda function can be triggered by CloudWatch events that are emitted when Auto Scaling events occur. The function can then collect the necessary data and store it in S3. This direct sending of data to S3 will reduce the number of steps and hence it is more efficient and cost-effective.

upvoted 2 times

 **Aninina** 10 months, 2 weeks ago

ChatGPT is not correct here

upvoted 3 times

A company has an application that places hundreds of .csv files into an Amazon S3 bucket every hour. The files are 1 GB in size. Each time a file is uploaded, the company needs to convert the file to Apache Parquet format and place the output file into an S3 bucket.

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

- A. Create an AWS Lambda function to download the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Invoke the Lambda function for each S3 PUT event.
- B. Create an Apache Spark job to read the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the Spark job.
- C. Create an AWS Glue table and an AWS Glue crawler for the S3 bucket where the application places the .csv files. Schedule an AWS Lambda function to periodically use Amazon Athena to query the AWS Glue table, convert the query results into Parquet format, and place the output files into an S3 bucket.
- D. Create an AWS Glue extract, transform, and load (ETL) job to convert the .csv files to Parquet format and place the output files into an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the ETL job.

Correct Answer: A

Community vote distribution

D (86%) 14%

 **Parsons** Highly Voted  10 months, 2 weeks ago

Selected Answer: D

No, D should be correct.

"LEAST operational overhead" => Should you fully manage service like Glue instead of manually like the answer A.
upvoted 11 times

 **TariqKipkemei** Most Recent  2 months ago

Selected Answer: D

AWS Glue can run your extract, transform, and load (ETL) jobs as new data arrives. For example, you can configure AWS Glue to initiate your ETL jobs to run as soon as new data becomes available in Amazon Simple Storage Service (S3).
Clearly you don't need a lambda function to initiate the ETL job.

<https://aws.amazon.com/glue/#:~:text=to%20initiate%20your-,ETL,-jobs%20to%20run>

Option A requires writing code to perform the file conversion.

In the exam option D would be the best answer.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

This solution meets the requirements with the least operational overhead because AWS Glue is a fully managed ETL service that makes it easy to move data between data stores. AWS Glue can read .csv files from an S3 bucket and write the data into Parquet format in another S3 bucket. The AWS Lambda function can be triggered by an S3 PUT event when a new .csv file is uploaded, and it can start the AWS Glue ETL job to convert the file to Parquet format. This solution does not require managing any servers or clusters, which reduces operational overhead.

upvoted 2 times

 **cookieMr** 5 months ago

D is correct

upvoted 1 times

 **cookieMr** 5 months ago

A. introduces significant operational overhead. This approach requires managing the Lambda, handling concurrency, and ensuring proper error handling for large file sizes, which can be challenging.

B. adds unnecessary complexity and operational overhead. Managing the Spark job, handling scalability, and coordinating the Lambda invocations for each file upload can be cumbersome.

C. introduces additional complexity and may not be the most efficient solution. It involves managing Glue resources, scheduling Lambda, and querying data even when no new files are uploaded.

Option D leverages AWS Glue's ETL capabilities, allowing you to define and execute a data transformation job at scale. By invoking the ETL job using an Lambda function for each S3 PUT event, you can ensure that files are efficiently converted to Parquet format without the need for manual intervention. This approach minimizes operational overhead and provides a streamlined and scalable solution.

upvoted 3 times

✉ **F629** 5 months, 1 week ago

Selected Answer: A

Both A and D can work, but A is more simple. It's more close to the "Least Operational effort".

upvoted 1 times

✉ **shanwford** 7 months, 3 weeks ago

Selected Answer: D

The maximum size for a Lambda event payload is 256 KB - so (A) didn't work with 1GB Files. Glue is recommended for the Parquet Transformation of AWS.

upvoted 2 times

✉ **jennyka76** 9 months, 3 weeks ago

ANS - d

<https://aws.amazon.com/blogs/database/how-to-extract-transform-and-load-data-for-analytic-processing-using-aws-glue-part-2/>

- READ ARTICLE -

upvoted 2 times

✉ **aws4myself** 10 months, 1 week ago

Here A is the correct answer. The reason here is the least operational overhead.

A ==> S3 - Lambda - S3

D ==> S3 - Lambda - Glue - S3

Also, glue cannot convert on fly automatically, you need to write some code there. If you write the same code in lambda it will convert the same and push the file to S3

Lambda has max memory of 128 MB to 10 GB. So, it can handle it easily.

And we need to consider cost also, glue cost is more. Hope many from this forum realize these differences.

upvoted 4 times

✉ **nder** 9 months ago

Cost is not a factor. AWS Glue is a fully managed service therefore, it's the least operational overhead

upvoted 2 times

✉ **LuckyAro** 10 months ago

We also need to stay with the question, cost was not a consideration in the question.

upvoted 1 times

✉ **JayBee65** 10 months, 1 week ago

A is unlikely to work as Lambda may struggle with 1GB size: "< 64 MB, beyond which lambda is likely to hit memory caps", see <https://stackoverflow.com/questions/41504095/creating-a-parquet-file-on-aws-lambda-function>

upvoted 2 times

✉ **jainparag1** 10 months, 1 week ago

Should be D as Glue is self managed service and provides tel job for converting cab files to parquet off the shelf.

upvoted 1 times

✉ **Joxtat** 10 months, 2 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>

upvoted 1 times

✉ **techhb** 10 months, 2 weeks ago

AWS Glue is right solution here.

upvoted 1 times

✉ **mp165** 10 months, 2 weeks ago

Selected Answer: D

I am thinking D.

A says lambda will download the .csv...but to where? that seem manual based on that

upvoted 1 times

✉ **mhmt4438** 10 months, 2 weeks ago

Selected Answer: A

I think A

upvoted 1 times

✉ **bamishr** 10 months, 2 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/83201-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.

Which solution should a solutions architect recommend to meet these requirements?

- A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.
- B. Configure a backup window for the RDS DB instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions.
- C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years.
- D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target. Configure S3 Lifecycle policies to delete the snapshots after 2 years.

Correct Answer: A

Community vote distribution

A (96%) 4%

 **vijaykamal** 2 months ago

Selected Answer: B

Here's why Option B is the best choice:

Backup Window: Configuring a backup window for daily snapshots ensures that consistent backups are taken at the specified time each day. This helps maintain data integrity and consistency.

Snapshot Retention Policy: Assigning a snapshot retention policy of 2 years to each RDS DB instance ensures that the backups are retained for the required duration.

Amazon Data Lifecycle Manager (Amazon DLM): Amazon DLM can be used to automate the management of EBS snapshots, including RDS snapshots. You can configure Amazon DLM to schedule snapshot deletions, making it easier to manage the retention policy without manual intervention.

Option A (AWS Backup) is primarily used for managing backups of resources that may not have built-in backup capabilities, but for Amazon RDS, it's better to use the built-in snapshot capabilities and Amazon DLM for snapshot retention.

upvoted 1 times

 **TariqKipkemei** 2 months ago

Selected Answer: A

Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan

upvoted 1 times

 **animefan1** 4 months, 4 weeks ago

Selected Answer: A

Backups work with EBS, FSX, RDS. Its managed & can has vault option for more better control over backup retention

upvoted 3 times

 **cookieMr** 5 months ago

Selected Answer: A

A. suggests using AWS Backup, a centralized backup management service, to retain RDS backups. A backup vault is created, and a backup plan is defined with a daily schedule and a 2-year retention period for backups. RDS DB instances are assigned to this backup plan.

B. it does not address the requirement for consistent and restorable backups. Snapshots are point-in-time backups and may not provide the desired level of consistency.

C. it is not designed to provide the backup and restore functionality required for databases. It does not ensure the backups are consistent or provide an easy restore mechanism.

D. it does not address the requirement for daily backups and retention of consistent backups. It focuses more on replication and change data capture rather than backup and restore.

upvoted 4 times

 **markw92** 5 months, 1 week ago

Why not B?

upvoted 2 times

 **_deepsi_dee29** 6 months ago

Selected Answer: A

A is correct

upvoted 1 times

 **antropaws** 6 months, 1 week ago

Why not D?

Creating tasks for ongoing replication using AWS DMS: You can create an AWS DMS task that captures ongoing changes from the source data store. You can do this capture while you are migrating your data. You can also create a task that captures ongoing changes after you complete your initial (full-load) migration to a supported target data store. This process is called ongoing replication or change data capture (CDC). AWS DMS uses this process when replicating ongoing changes from a source data store.

upvoted 1 times

 **gold4otas** 8 months ago

Selected Answer: A

A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: A

A is right choice

upvoted 3 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: A

A A A A A

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: A

Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.

upvoted 4 times

A company's compliance team needs to move its file shares to AWS. The shares run on a Windows Server SMB file share. A self-managed on-premises Active Directory controls access to the files and folders.

The company wants to use Amazon FSx for Windows File Server as part of the solution. The company must ensure that the on-premises Active Directory groups restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS. The company has created an FSx for Windows File Server file system.

Which solution will meet these requirements?

- A. Create an Active Directory Connector to connect to the Active Directory. Map the Active Directory groups to IAM groups to restrict access.
- B. Assign a tag with a Restrict tag key and a Compliance tag value. Map the Active Directory groups to IAM groups to restrict access.
- C. Create an IAM service-linked role that is linked directly to FSx for Windows File Server to restrict access.
- D. Join the file system to the Active Directory to restrict access.

Correct Answer: D

Community vote distribution

D (86%) 14%

 **mhmt4438**  10 months, 2 weeks ago

Selected Answer: D

D. Join the file system to the Active Directory to restrict access.

Joining the FSx for Windows File Server file system to the on-premises Active Directory will allow the company to use the existing Active Directory groups to restrict access to the file shares, folders, and files after the move to AWS. This option allows the company to continue using their existing access controls and management structure, making the transition to AWS more seamless.

upvoted 14 times

 **wrmari**  1 month, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html>

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

This allows the on-premises Active Directory to manage permissions to the FSx file shares, meeting the key requirement to use existing AD groups to control access after migrating to AWS.

Joining FSx to the AD domain allows the native file system permissions, users, and groups to be applied from Active Directory. Access is handled seamlessly via the trust relationship between FSx and AD.

The other options would not leverage the existing AD identities and groups

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

The other options would not leverage the existing AD identities and groups:

- A) AD Connector and IAM groups would require re-mapping AD groups to IAM, adding complexity. Native AD integration is simpler.
- B) Tags and IAM groups also don't use native AD semantics.
- C) Service-linked roles are not applicable for managing end user access.

So D is the correct option to meet the requirements using the native Active Directory integration built into FSx for Windows.

upvoted 1 times

 **mtmayer** 3 months, 3 weeks ago

Selected Answer: A

The AD is on-premises... You need the connector.

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: D

D. allows the file system to leverage the existing AD infrastructure for authentication and access control.

Option A is incorrect because mapping the AD groups to IAM groups is not applicable in this scenario. IAM is primarily used for managing access to AWS resources, while the requirement is to integrate with the on-premises AD for access control.

Option B is incorrect because assigning a tag with a Restrict tag key and a Compliance tag value does not provide the necessary integration with the on-premises AD for access control. Tags are used for organizing and categorizing resources and do not provide authentication or access control mechanisms.

Option C is incorrect because creating an IAM service-linked role linked directly to FSx for Windows File Server does not integrate with the on-premises AD. IAM roles are used within AWS for managing permissions and do not provide the necessary integration with external AD systems.

upvoted 4 times

✉ **Mia2009687** 5 months ago

Selected Answer: D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>

upvoted 1 times

✉ **kraken21** 8 months ago

Selected Answer: D

Other options are referring to IAM based control which is not possible. Existing AD should be used without IAM.

upvoted 1 times

✉ **Abhineet9148232** 8 months, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/storage/using-amazon-fsx-for-windows-file-server-with-an-on-premises-active-directory/>

upvoted 2 times

✉ **somsundar** 8 months, 3 weeks ago

Answer D. Amazon FSx does not support Active Directory Connector .

upvoted 2 times

✉ **Abhineet9148232** 8 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html>

upvoted 3 times

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

Selected Answer: D

Note:

Amazon FSx does not support Active Directory Connector and Simple Active Directory.

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>

upvoted 3 times

✉ **aakashkumar1999** 9 months, 3 weeks ago

Selected Answer: A

The answer will be AD connector so : A, it will create a proxy between your onpremises AD which you can use to restrict access

upvoted 2 times

✉ **Stanislav4907** 10 months ago

Selected Answer: D

Option D: Join the file system to the Active Directory to restrict access.

Joining the FSx for Windows File Server file system to the on-premises Active Directory allows the company to use the existing Active Directory groups to restrict access to the file shares, folders, and files after the move to AWS. By joining the file system to the Active Directory, the company can maintain the same access control as before the move, ensuring that the compliance team can maintain compliance with the relevant regulations and standards.

Options A and B involve creating an Active Directory Connector or assigning a tag to map the Active Directory groups to IAM groups, but these options do not allow for the use of the existing Active Directory groups to restrict access to the file shares in AWS.

Option C involves creating an IAM service-linked role linked directly to FSx for Windows File Server to restrict access, but this option does not take advantage of the existing on-premises Active Directory and its access control.

upvoted 3 times

✉ **KAUS2** 10 months ago

Selected Answer: A

A is correct

Use AD Connector if you only need to allow your on-premises users to log in to AWS applications and services with their Active Directory credentials. You can also use AD Connector to join Amazon EC2 instances to your existing Active Directory domain.

Pls refer - https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html#adconnector

upvoted 3 times

✉ **mbuck2023** 5 months, 3 weeks ago

wrong, answer is D. Amazon FSx does not support Active Directory Connector and Simple Active Directory. See also <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html>.

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Going with D here

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: D

D. Join the file system to the Active Directory to restrict access.

The best way to restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS is to join the file system to the on-premises Active Directory. This will allow the company to continue using the Active Directory groups to restrict access to the files and folders, without the need to create additional IAM groups or roles.

By joining the file system to the Active Directory, the company can continue to use the same access control mechanisms it already has in place and the security configuration will not change.

Option A and B are not applicable to FSx for Windows File Server because it doesn't support the use of IAM groups or tags to restrict access.

Option C is not appropriate in this case because FSx for Windows File Server does not support using IAM service-linked roles to restrict access.

upvoted 4 times

A company recently announced the deployment of its retail website to a global audience. The website runs on multiple Amazon EC2 instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones.

The company wants to provide its customers with different versions of content based on the devices that the customers use to access the website.

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

- A. Configure Amazon CloudFront to cache multiple versions of the content.
- B. Configure a host header in a Network Load Balancer to forward traffic to different instances.
- C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.
- D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.
- E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.

Correct Answer: AC

Community vote distribution

AC (100%)

✉️  **Parsons** Highly Voted 10 months, 2 weeks ago

Selected Answer: AC

A, C is correct.

NLB lister rule only supports Protocol & Port (Not host/based routing like ALB) => D, E is incorrect.
NLB just works layer 4 (TCP/UDP) instead of Layer 7 (HTTP) => B is incorrect.

After eliminating, AC should be the answer.

upvoted 11 times

✉️  **Ruffyit** Most Recent 2 weeks, 2 days ago

A C

Configure Amazon CloudFront to cache multiple versions of the content.

Configure a function to send specific objects to users based on the User-Agent header.

upvoted 1 times

✉️  **sunhouse** 1 month, 1 week ago

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html>

upvoted 1 times

✉️  **rrbrish73** 1 month, 3 weeks ago

<https://medium.com/swlh/serve-different-content-based-on-user-agent-in-aws-cloudfront-using-lambda-edge-28877294340b>

upvoted 1 times

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

Selected Answer: AC

A. allows customers to receive the appropriate version of the content based on their location and device type.

C. By creating a Lambda@Edge, you can inspect the User-Agent header of incoming requests and determine the type of device being used. Based on this information, you can customize the response and send the appropriate version of the content to the user.

upvoted 2 times

✉️  **cookieMr** 5 months ago

Selected Answer: AC

A. allows customers to receive the appropriate version of the content based on their location and device type.

C. By creating a Lambda@Edge, you can inspect the User-Agent header of incoming requests and determine the type of device being used. Based on this information, you can customize the response and send the appropriate version of the content to the user.

B. does not address the requirement of serving different content versions based on device types.

D. & E. do not address the device-specific content requirement.

Therefore, options A and C are the correct combination of actions to meet the requirement of providing different versions of content based on the devices that customers use to access the website.

upvoted 3 times

 **Yadav_Sanjay** 6 months, 2 weeks ago

Selected Answer: AC
NLB does not support routing
upvoted 1 times

 **omoakin** 6 months, 3 weeks ago

A C
Configure Amazon CloudFront to cache multiple versions of the content.
Configure a function to send specific objects to users based on the User-Agent header.
upvoted 1 times

 **omoakin** 6 months, 3 weeks ago

C
Configure a function to send specific objects to users based on the User-Agent header.
upvoted 1 times

 **GalileoEC2** 8 months, 1 week ago

Using a Directory Connector to connect the on-premises Active Directory to AWS is one way to enable access to AWS resources, including Amazon FSx for Windows File Server. However, joining the Amazon FSx for Windows File Server file system to the on-premises Active Directory is a separate step that allows you to control access to the file shares using the same Active Directory groups that are used on-premises.

upvoted 1 times

 **LoXeras** 8 months, 1 week ago

I guess this belongs to the question before #260
upvoted 2 times

 **wors** 9 months, 2 weeks ago

So will this mean the entire architecture needs to move to lambda in order to leverage off lambda edge? This doesn't make sense as the question outlines the architecture already in ec2, asg and elb?

Just looking for clarification if I am missing something

upvoted 1 times

 **devonwho** 10 months ago

Selected Answer: AC
AC are the correct answers.

For C:

IMPROVED USER EXPERIENCE

Lambda@Edge can help improve your users' experience with your websites and web applications across the world, by letting you personalize content for them without sacrificing performance.

Real-time Image Transformation

You can customize your users' experience by transforming images on the fly based on the user characteristics. For example, you can resize images based on the viewer's device type—mobile, desktop, or tablet. You can also cache the transformed images at CloudFront Edge locations to further improve performance when delivering images.

<https://aws.amazon.com/lambda/edge/>

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: AC
Correct answer is A,C
upvoted 3 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: AC
C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.

Lambda@Edge allows you to run a Lambda function in response to specific CloudFront events, such as a viewer request, an origin request, a response, or a viewer response.

upvoted 2 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: AC
<https://www.examtopics.com/discussions/amazon/view/67881-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

A company plans to use Amazon ElastiCache for its multi-tier web application. A solutions architect creates a Cache VPC for the ElastiCache cluster and an App VPC for the application's Amazon EC2 instances. Both VPCs are in the us-east-1 Region.

The solutions architect must implement a solution to provide the application's EC2 instances with access to the ElastiCache cluster.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
- B. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
- C. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the peering connection's security group to allow inbound connection from the application's security group.
- D. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the Transit VPC's security group to allow inbound connection from the application's security group.

Correct Answer: A

Community vote distribution

A (100%)

 **mhmt4438** Highly Voted 10 months, 2 weeks ago

Selected Answer: A

A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

Creating a peering connection between the VPCs allows the application's EC2 instances to communicate with the ElastiCache cluster directly and efficiently. This is the most cost-effective solution as it does not involve creating additional resources such as a Transit VPC, and it does not incur additional costs for traffic passing through the Transit VPC. Additionally, it is also more secure as it allows you to configure a more restrictive security group rule to allow inbound connection from only the application's security group.

upvoted 12 times

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

A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

Creating a peering connection between the VPCs allows the application's EC2 instances to communicate with the ElastiCache cluster directly and efficiently. This is the most cost-effective solution as it does not involve creating additional resources such as a Transit VPC, and it does not incur additional costs for traffic passing through the Transit VPC. Additionally, it is also more secure as it allows you to configure a more restrictive security group rule to allow inbound connection from only the application's security group.

upvoted 1 times

 **TariqKipkemei** 2 months ago

Selected Answer: A

Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

Create a VPC peering connection between the Cache VPC and App VPC. This allows private IP connectivity between the VPCs. Add route table entries in each VPC to route traffic destined to the other VPC via the peering connection. This enables network routing. Configure security groups to allow inbound connections from the application instances to the ElastiCache cluster.

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: A

Creating a peering connection between the VPCs is a cost-effective way to establish connectivity. By adding a route table entry for the peering connection in both VPCs, traffic can flow between them. Configuring an inbound rule in the ElastiCache cluster's security group allows inbound connections from the application's security group, enabling access to the ElastiCache cluster from the EC2 instances in the App VPC.

Option B suggests creating a Transit VPC, which adds unnecessary complexity and cost for this scenario.

Option C suggests configuring an inbound rule for the peering connection's security group, which is not necessary as the security group for the

ElastiCache cluster should be used to control inbound connections.

Option D suggests configuring an inbound rule for the Transit VPC's security group, which is not needed in this case and adds unnecessary complexity.

Therefore, option A is the most cost-effective solution to provide the application's EC2 instances with access to the ElastiCache cluster.
upvoted 1 times

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

Selected Answer: A

A is correct,

1. VPC transit is used for more complex architecture and can do VPCs to VPCs connectivity. But for simple VPC 2 VPC can use peer connection.
2.To enable private IPv4 traffic between instances in peered VPCs, you must add a route to the route tables associated with the subnets for both instances.

So base on 1, B and D are out, base on 2 C is out
upvoted 1 times

✉ **wRhlH** 5 months, 3 weeks ago

Why not C ? any explanation?

upvoted 1 times

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

Application read from ElasticCache, not viseversa, so inbound rule should be ElasticCach

upvoted 2 times

✉ **Cor5in** 5 months ago

Thank you Sir!

upvoted 1 times

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

To enable private IPv4 traffic between instances in peered VPCs, you must add a route to the route tables associated with the subnets for both instances.

<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-routing.html>

upvoted 1 times

✉ **nder** 9 months ago

Selected Answer: A

Cost Effectively!

upvoted 1 times

A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

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

- A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.
- B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.
- C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.
- D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.
- E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Correct Answer: AD

Community vote distribution

AD (100%)

✉️  **TariqKipkemei** 2 months ago

Selected Answer: AD

Company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling = Serverless = ECS with Fargate.
upvoted 1 times

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

Selected Answer: AD

ECS allows deploying and managing containers without having to provision the underlying infrastructure. This minimizes maintenance effort. Using Fargate launch type means ECS will handle provisioning and scaling the infrastructure automatically. This removes the management overhead for the company.

Running multiple tasks and specifying desired count ≥ 2 will provide high availability across Availability Zones.

Together, ECS plus Fargate provide a fully managed container platform. The company doesn't need to provision or manage servers.
upvoted 2 times

✉️  **cookieMr** 5 months ago

Selected Answer: AD

Options B and E suggest deploying the Kubernetes control plane and worker nodes on EC2 instances, which would require managing the infrastructure and add ongoing maintenance overhead, contrary to the requirement of minimizing effort.

Option C suggests using the Amazon EC2 launch type for ECS, which still requires managing EC2 instances and is not as cost-effective and scalable as using Fargate.

Therefore, the combination of deploying an Amazon ECS cluster and an ECS service with a Fargate launch type (options A and D) is the most suitable for minimizing maintenance and scaling effort without managing additional infrastructure.
upvoted 3 times

✉️  **LoXeras** 8 months, 1 week ago

Selected Answer: AD

AWS Fargate is server less solution to use on ECS: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/AWS_Fargate.html
upvoted 2 times

✉️  **lambda15** 8 months, 1 week ago

why is c is incorrect ?

upvoted 1 times

✉️  **Julio98** 8 months, 1 week ago

Because in the question says, "minimizes the amount of ongoing effort for maintenance and scaling", and EC2 instances you need effort to maintain the infrastructure unlike fargate that is serverless.
upvoted 2 times

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

Selected Answer: AD

Amazon Fargate is a service that is fully manageable by Amazon; it offers provisioning, configuration and scaling feature. It is "serverless".

upvoted 1 times

✉  **AlessandraSAA** 8 months, 4 weeks ago

Selected Answer: AD

ECS has 2 launch type, EC2 (you maintain the infra) and Fargate (serverless). Since the question ask for no additional infra to manage it should be Fargate.

upvoted 2 times

✉  **devonwho** 10 months ago

Selected Answer: AD

AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers.

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

upvoted 3 times

✉  **Aninina** 10 months, 2 weeks ago

A D is the correct answer

upvoted 1 times

✉  **mhmt4438** 10 months, 2 weeks ago

Selected Answer: AD

A,D is correct answer

upvoted 2 times

✉  **AHUI** 10 months, 2 weeks ago

AD:

<https://www.examtopics.com/discussions/amazon/view/60032-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

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

Selected Answer: AD

AD - EC2 out for this, cluster + fargate is the right answer

upvoted 3 times

A company has a web application hosted over 10 Amazon EC2 instances with traffic directed by Amazon Route 53. The company occasionally experiences a timeout error when attempting to browse the application. The networking team finds that some DNS queries return IP addresses of unhealthy instances, resulting in the timeout error.

What should a solutions architect implement to overcome these timeout errors?

- A. Create a Route 53 simple routing policy record for each EC2 instance. Associate a health check with each record.
- B. Create a Route 53 failover routing policy record for each EC2 instance. Associate a health check with each record.
- C. Create an Amazon CloudFront distribution with EC2 instances as its origin. Associate a health check with the EC2 instances.
- D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

Correct Answer: D

Community vote distribution

D (65%)	B (27%)	8%
---------	---------	----

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

Selected Answer: B

It is not clear from the question whether the 10 EC2s are running within the same region. ALB can only direct traffic within region, while route 53 can route traffic to multiple locations, hence C and D are wrong.

upvoted 5 times

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

Selected Answer: D

ALB performs health checks on the EC2 instances, so it will only route traffic to healthy instances. This avoids the timeout errors.

ALB provides load balancing across the instances, improving performance and availability.

Route 53 routes to the ALB DNS name, so you don't have to manage records for each EC2 instance.

This is a standard and robust architecture for public-facing web applications. The ALB acts as the entry point and handles health checks and scaling.

upvoted 5 times

✉  **Ruffyit**  2 weeks, 2 days ago

B is wrong.

The DNS cache in clients could drive to timeouts. With ALB this issue won't happen since the DNS register will be the same and ALB will take care of unhealthy nodes.

upvoted 1 times

✉  **rlamberti** 1 month ago

Selected Answer: D

B is wrong.

The DNS cache in clients could drive to timeouts. With ALB this issue won't happen since the DNS register will be the same and ALB will take care of unhealthy nodes.

upvoted 2 times

✉  **daniel1** 1 month, 2 weeks ago

Selected Answer: D

D. **Application Load Balancer (ALB) with Health Checks, Routed via Route 53**:

- Creating an ALB in front of the EC2 instances and configuring health checks on the ALB will ensure that only healthy instances receive traffic. Route 53 can then direct traffic to the ALB, which in turn, routes traffic to healthy instances based on the health check results.

Among the provided options, the one that directly addresses the issue of routing traffic only to healthy instances is:

D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

upvoted 3 times

✉  **TariqKipkemei** 2 months ago

Selected Answer: B

Clearly the question is all about Amazon Route 53 that has Failover routing policy that is used when you want to configure active-passive failover.

upvoted 1 times

✉  **slackbot** 2 months, 3 weeks ago

I was looking at A, but indeed D is the best option, because the usually the TTL of the records is at least 60 seconds (nobody sets lower unless testing something), because there is a charge per number of unique requests. ALB health check can be set as low as desired, which helps exclude the problematic ec2 faster than the DNS TTL expires

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: D

By creating an ALB and configuring health checks, the architect ensures that only healthy instances receive traffic. The ALB periodically checks the health of the EC2 instances based on the configured health check settings.

Routing traffic to the ALB from Route 53 ensures that DNS queries return the IP address of the ALB instead of individual instances. This allows the ALB to distribute traffic only to healthy instances, avoiding timeouts caused by unhealthy instances.

A & B: While associating health checks with each record can help identify unhealthy instances, it does not provide automatic load balancing and distribution of traffic to healthy instances.

C: While CloudFront can improve performance and availability, it is primarily a CDN and may not directly address the issue of load balancing and distributing traffic to healthy instances.

Therefore, option D is the most appropriate solution to overcome the timeout errors by implementing an ALB with health checks and routing traffic through Route 53.

upvoted 3 times

 **joechen2023** 5 months, 1 week ago

Selected Answer: C

I believe both C and D will work, but C seems less complex.

hopefully somebody here is more advanced(not an old student learning AWS like me) to explain why not C.

upvoted 3 times

 **Abrar2022** 6 months ago

Selected Answer: D

Option D allows for the creation of an Application Load Balancer which can detect unhealthy instances and redirect traffic away from them.

upvoted 2 times

 **Steve_4542636** 9 months ago

Selected Answer: D

I vote d

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: D

Its D only

upvoted 1 times

 **techhb** 10 months, 2 weeks ago

Selected Answer: B

Why not B

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

upvoted 4 times

 **techhb** 10 months, 2 weeks ago

Its D,found the root cause

Option B is not the best option to overcome these timeout errors because it is not designed to handle traffic directed by Amazon Route 53.

Option B creates a failover routing policy record for each EC2 instance, which is designed to route traffic to a backup EC2 instance if one of the EC2 instances becomes unhealthy. This is not ideal for routing traffic from Route 53 as it does not allow for the redirection of traffic away from unhealthy instances. Option D would be the best choice as it allows for the creation of an Application Load Balancer which can detect unhealthy instances and redirect traffic away from them.

upvoted 5 times

 **F629** 5 months, 1 week ago

I think the problem of Failover routing policy is that it always send the requests to the same primary instance, not spread into all healthy instances.

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

 **AHUI** 10 months, 2 weeks ago

Ans: D

<https://www.examtopics.com/discussions/amazon/view/83982-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: D

D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

An Application Load Balancer (ALB) allows you to distribute incoming traffic across multiple backend instances, and can automatically route traffic to healthy instances while removing traffic from unhealthy instances. By using an ALB in front of the EC2 instances and routing traffic to it from Route 53, the load balancer can perform health checks on the instances and only route traffic to healthy instances, which should help to reduce or eliminate timeout errors caused by unhealthy instances.

upvoted 4 times

A solutions architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.

Which solution meets these requirements and is MOST secure?

- A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- B. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
- C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Correct Answer: C

Community vote distribution

C (100%)

 **Aninina** Highly Voted 10 months, 2 weeks ago

C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.

This solution meets the requirements for a highly available application with web, application, and database tiers, as well as providing edge-based content delivery. Additionally, it maximizes security by having the ALB in a private subnet, which limits direct access to the web servers, while still being able to serve traffic over the Internet via the public ALB. This will ensure that the web servers are not exposed to the public Internet, which reduces the attack surface and provides a secure way to access the application.

upvoted 12 times

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

C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.

This solution meets the requirements for a highly available application with web, application, and database tiers, as well as providing edge-based content delivery. Additionally, it maximizes security by having the ALB in a private subnet, which limits direct access to the web servers, while still being able to serve traffic over the Internet via the public ALB. This will ensure that the web servers are not exposed to the public Internet, which reduces the attack surface and provides a secure way to access the application.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: C

Keyword: Instances in private, ALB in public, point cloudfront to the public ALB

upvoted 1 times

 **cookieMr** 5 months ago

Selected Answer: C

A. exposes the EC2 instances directly to the public internet, which may compromise security.

B. lacks a load balancer in the public subnet, which is required for efficient load distribution and high availability.

D. provides load balancing and HTTPS content delivery, it exposes the EC2 instances directly to the public internet, which may pose security risks.

C. provides high availability, secure access through private subnets, and optimized HTTPS content delivery using CloudFront with a public ALB as the origin.

upvoted 4 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 3 times

 **AHUI** 10 months, 2 weeks ago

ans: C

<https://www.examtopics.com/discussions/amazon/view/46401-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: C

Instances in private, ALB in public, point cloudfront to the public ALB

upvoted 4 times

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.

Which solution meets these requirements?

- A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
- B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.

Correct Answer: A

Community vote distribution

A (100%)

 **Aninina**  10 months, 2 weeks ago

Selected Answer: A

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.

AWS Global Accelerator directs traffic to the optimal healthy endpoint based on health checks, it can also route traffic to the closest healthy endpoint based on geographic location of the client. By configuring an accelerator and attaching it to a Regional endpoint in each Region, and adding the ALB as the endpoint, the solution will redirect traffic to healthy endpoints, improving the user experience by reducing latency and ensuring that the application is running optimally. This solution will ensure that traffic is directed to the closest healthy endpoint and will help to improve the overall user experience.

upvoted 14 times

 **Bhrino**  9 months, 1 week ago

Selected Answer: A

Global accelerators can be used for non http cases such as UDP, tcp , gaming , or voip

upvoted 7 times

 **Ruffyit**  2 weeks, 2 days ago

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.

AWS Global Accelerator directs traffic to the optimal healthy endpoint based on health checks, it can also route traffic to the closest healthy endpoint based on geographic location of the client. By configuring an accelerator and attaching it to a Regional endpoint in each Region, and adding the ALB as the endpoint, the solution will redirect traffic to healthy endpoints, improving the user experience by reducing latency and ensuring that the application is running optimally. This solution will ensure that traffic is directed to the closest healthy endpoint and will help to improve the overall user experience.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: A

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint

upvoted 1 times

 **bjexamprep** 4 months ago

Is any answer relevant to the question?

upvoted 3 times

 **cookieMr** 5 months ago

Selected Answer: A

B. While CloudFront can help with caching and content delivery, it does not provide the mechanism to monitor the health of the application or perform traffic redirection based on health checks.

C. This configuration is suitable for static content delivery but does not address the health monitoring and traffic redirection requirements of the application.

D. While this can enhance performance, it does not monitor the health of the application or redirect traffic based on health checks.

Therefore, option A is the most suitable solution as it leverages AWS Global Accelerator to monitor application health, route traffic to healthy endpoints, and optimize the user experience while addressing latency concerns.

upvoted 2 times

 **antropaws** 6 months, 1 week ago

Selected Answer: A

Agree with A

upvoted 1 times

 **michellemeloc** 6 months, 2 weeks ago

Selected Answer: A

Delivery gaming content --> AWS GLOBAL ACCELERATOR

upvoted 5 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **AHUI** 10 months, 2 weeks ago

A:

<https://www.examtopics.com/discussions/amazon/view/46403-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **alanp** 10 months, 2 weeks ago

A. When you have an Application Load Balancer or Network Load Balancer that includes multiple target groups, Global Accelerator considers the load balancer endpoint to be healthy only if each target group behind the load balancer has at least one healthy target. If any single target group for the load balancer has only unhealthy targets, Global Accelerator considers the endpoint to be unhealthy.

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-health-check-options.html>

upvoted 7 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-health-check-options.html>

upvoted 1 times

A company has one million users that use its mobile app. The company must analyze the data usage in near-real time. The company also must encrypt the data in near-real time and must store the data in a centralized location in Apache Parquet format for further processing.

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

- A. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data. Invoke an AWS Lambda function to send the data to the Kinesis Data Analytics application.
- B. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data. Invoke an AWS Lambda function to send the data to the EMR cluster.
- C. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data.
- D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

Correct Answer: D

Community vote distribution

D (100%)

 **mhmt4438**  10 months, 2 weeks ago

Selected Answer: D

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

This solution will meet the requirements with the least operational overhead as it uses Amazon Kinesis Data Firehose, which is a fully managed service that can automatically handle the data collection, data transformation, encryption, and data storage in near-real time. Kinesis Data Firehose can automatically store the data in Amazon S3 in Apache Parquet format for further processing. Additionally, it allows you to create an Amazon Kinesis Data Analytics application to analyze the data in near real-time, with no need to manage any infrastructure or invoke any Lambda function. This way you can process a large amount of data with the least operational overhead.

upvoted 34 times

 **jainparag1** 10 months, 1 week ago

Nicely explained. Thanks.

upvoted 3 times

 **antropaws** 6 months, 1 week ago

<https://aws.amazon.com/blogs/big-data/analyzing-apache-parquet-optimized-data-using-amazon-kinesis-data-firehose-amazon-athena-and-amazon-redshift/>

upvoted 1 times

 **WhericanIstart** 8 months, 2 weeks ago

Thanks for the explanation!

upvoted 1 times

 **LuckyAro** 10 months, 1 week ago

Apache Parquet format processing was not mentioned in the answer options. Strange.

upvoted 6 times

 **cookieMr**  5 months ago

Selected Answer: D

A. requires invoking an Lambda to send the data to the analytics application. This introduces additional operational overhead and complexity.

B. While EMR is a powerful tool for big data processing, it requires more operational management and configuration compared to Kinesis Data Analytics.

C. introduces unnecessary complexity by involving EMR for data analysis when Kinesis Data Analytics can perform the analysis in a more streamlined and automated manner.

Therefore, option D is the most suitable solution as it leverages Kinesis Data Firehose for data ingestion, stores the data in S3, and utilizes Kinesis Data Analytics for near-real-time analysis, providing a low operational overhead solution for data usage analysis and encryption.

upvoted 5 times

 **Ruffyit**  2 weeks, 2 days ago

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

This solution will meet the requirements with the least operational overhead as it uses Amazon Kinesis Data Firehose, which is a fully managed service that can automatically handle the data collection, data transformation, encryption, and data storage in near-real time. Kinesis Data Firehose can automatically store the data in Amazon S3 in Apache Parquet format for further processing. Additionally, it allows you to create an Amazon Kinesis Data Analytics application to analyze the data in near real-time, with no need to manage any infrastructure or invoke any Lambda function. This way you can process a large amount of data with the least operational overhead.

upvoted 1 times

 **TariqKipkemei** 2 months ago

Selected Answer: D

Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data

upvoted 1 times

 **AHUI** 10 months, 2 weeks ago

D:

<https://www.examtopics.com/discussions/amazon/view/82022-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: D

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

Amazon Kinesis Data Firehose can automatically encrypt and store the data in Amazon S3 in Apache Parquet format for further processing, which reduces the operational overhead. It also allows for near-real-time data analysis using Kinesis Data Analytics, which is a fully managed service that makes it easy to analyze streaming data using SQL. This solution eliminates the need for setting up and maintaining an EMR cluster, which would require more operational overhead.

upvoted 2 times

A gaming company has a web application that displays scores. The application runs on Amazon EC2 instances behind an Application Load Balancer. The application stores data in an Amazon RDS for MySQL database. Users are starting to experience long delays and interruptions that are caused by database read performance. The company wants to improve the user experience while minimizing changes to the application's architecture.

What should a solutions architect do to meet these requirements?

- A. Use Amazon ElastiCache in front of the database.
- B. Use RDS Proxy between the application and the database.
- C. Migrate the application from EC2 instances to AWS Lambda.
- D. Migrate the database from Amazon RDS for MySQL to Amazon DynamoDB.

Correct Answer: A

Community vote distribution

B (52%)

A (48%)

✉  **Steve_4542636**  9 months ago

Selected Answer: A

Rds proxy is for too many connections, not for performance
upvoted 17 times

✉  **vipyodha** 5 months, 1 week ago

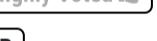
to use elasticache , you need to perform heavy code change ,and also elasticache do chaching that can improve read perfomance but will not provide scalability
upvoted 3 times

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

Can't use cache as score gates updated. If data would have been static then definitely can go with A. But here score is dynamic...
upvoted 6 times

✉  **r felipem** 6 months ago

Users are starting to experience long delays and interruptions caused by the "read performance" of the database... While the score is dynamic, there is also read activity in the DB that is causing the delays and outages and this can be improved with Elastic Cache.
upvoted 4 times

✉  **kraken21**  8 months ago

Selected Answer: B

RDX proxy will :"improve the user experience while minimizing changes".
upvoted 15 times

✉  **xdkonorek2**  4 days, 19 hours ago

Selected Answer: A

I'd go for B at first but gaming score data is written once and is highly cachable
upvoted 1 times

✉  **Abobaloyi** 5 days, 2 hours ago

Using RDS Proxy, you can handle unpredictable surges in database traffic. Otherwise, these surges might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool.
upvoted 1 times

✉  **hungta** 1 week, 1 day ago

Selected Answer: B

A. Use Amazon ElastiCache in front of the database:

ElastiCache can improve performance by caching frequently accessed data, reducing the load on the database.
This solution might alleviate some read performance issues but might not entirely solve delays caused by database read performance.
-> So, vote B
upvoted 1 times

✉  **dilaaziz** 1 week, 5 days ago

Selected Answer: B

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

upvoted 1 times

✉  **Pankaj_007** 3 weeks, 6 days ago

Selected Answer: A

ElastiCache can help speed up the read performance of the database by caching frequently accessed data, reducing latency and allowing the application to access the data more quickly. This solution requires minimal modifications to the current architecture, as ElastiCache can be used in conjunction with the existing Amazon RDS for MySQL database.

upvoted 1 times

✉  **canonlycontainletters1** 1 month, 1 week ago

Selected Answer: A

A for performance
upvoted 2 times

✉  **rvca231** 1 month, 1 week ago

Seems like RDS Proxy is used for too many connections, while ElastiCache is general performance improvement.

Q: Can I use Amazon ElastiCache for use cases other than caching?

Yes. ElastiCache for Redis can be used as a primary in-memory key-value data store, providing fast, sub millisecond data performance, high availability and scalability. You can choose to configure a 500-node cluster that ranges between 83 shards (one master and five replicas per shard) and 500 shards (single master and no replicas), giving you up to 340 TB of memory. Support for 500-node cluster is available with Amazon ElastiCache for Redis starting with Redis version 5.0.6. See here for other use cases, such as leaderboards, rate limiting, queues, and chat.

from: <https://aws.amazon.com/elasticsearch/faqs/>

upvoted 1 times

✉  **suflam3** 1 month, 1 week ago

Selected Answer: A

A. Use Amazon ElastiCache in front of the database.

It does not say the score is in real time, so elasticache is the choice

upvoted 1 times

✉  **daniel1** 1 month, 2 weeks ago

Selected Answer: A

A. Use Amazon ElastiCache in front of the database.

By implementing Amazon ElastiCache, the company can alleviate the load on the RDS instance by caching frequent query results, which should improve database read performance and enhance the user experience with minimal architectural changes. --By ChatGPT4

upvoted 1 times

✉  **prabhjot** 1 month, 3 weeks ago

Ans B - Amazon RDS Proxy: Amazon RDS Proxy is a fully managed database proxy service that helps improve the scalability and availability of your RDS databases. It can help reduce the load on your database and improve connection management.

upvoted 1 times

✉  **vijaykamal** 2 months ago

Selected Answer: B

Option A suggests using Amazon ElastiCache, which is a good solution for caching frequently accessed data but may require more application changes compared to RDS Proxy.

upvoted 1 times

✉  **TariqKipkemei** 2 months ago

Selected Answer: A

Read performance = Amazon ElastiCache
DB connection timeouts = RDS Proxy
upvoted 2 times

✉  **JKevin778** 2 months ago

Selected Answer: A

"The application stores data in an Amazon RDS for MySQL database"
There is only one database used in this case, therefore no where to use RDS Proxy.
SO A.

upvoted 1 times

✉  **LazyTs** 2 months, 3 weeks ago

Selected Answer: A

It should be A, question said low performance due to "read" -> elasticache
upvoted 1 times

✉  **oguzbeliren** 3 months, 3 weeks ago

Answer is A:

B also would be an option but in order to use RDS Proxy we need an additional configuration in the server. The question is specifically asking us to

avoid from it.
upvoted 1 times

An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.

What should the solutions architect recommend?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Correct Answer: C

Community vote distribution

C (100%)

 **Ruffyit** 2 weeks, 1 day ago

- . While DynamoDB is a scalable NoSQL database, it requires changes to the application's data model and query patterns.
- B. ElastiCache is an in-memory data store that can improve query performance, but it is primarily used for caching rather than running complex queries.
- D. Redshift is a powerful data warehousing solution, but migrating the data and adapting the queries to Redshift's columnar architecture would require significant changes to the application and query logic.

Therefore, option C is the most appropriate recommendation as it leverages read replicas in RDS to offload read-only query traffic from the primary database, allowing the business analysts to run their queries without impacting the performance of the web application. It provides a scalable and efficient solution with minimal changes to the existing web application.

upvoted 1 times

 **nileeka97** 2 months ago

- Selected Answer: C**
- C. Create a read replica of the primary database and have the business analysts run their queries

upvoted 1 times

 **cookieMr** 5 months ago

- Selected Answer: C**
- A. While DynamoDB is a scalable NoSQL database, it requires changes to the application's data model and query patterns.
 - B. ElastiCache is an in-memory data store that can improve query performance, but it is primarily used for caching rather than running complex queries.
 - D. Redshift is a powerful data warehousing solution, but migrating the data and adapting the queries to Redshift's columnar architecture would require significant changes to the application and query logic.

Therefore, option C is the most appropriate recommendation as it leverages read replicas in RDS to offload read-only query traffic from the primary database, allowing the business analysts to run their queries without impacting the performance of the web application. It provides a scalable and efficient solution with minimal changes to the existing web application.

upvoted 1 times

 **antropaws** 6 months, 1 week ago

- Selected Answer: C**
- C, no doubt.

upvoted 2 times

 **mhmt4438** 10 months, 2 weeks ago

- Selected Answer: C**
- C is correct answer

upvoted 2 times

 **Aninina** 10 months, 2 weeks ago

- Selected Answer: C**
- C. Create a read replica of the primary database and have the business analysts run their queries.

Creating a read replica of the primary RDS database will offload the read-only SQL queries from the primary database, which will help to improve

the performance of the web application. Read replicas are exact copies of the primary database that can be used to handle read-only traffic, which will reduce the load on the primary database and improve the performance of the web application. This solution can be implemented with minimal changes to the existing web application, as the business analysts can continue to run their queries on the read replica without modifying the code.

upvoted 4 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: C

Create a read replica of the primary database and have the business analysts run their queries.

upvoted 1 times

A company is using a centralized AWS account to store log data in various Amazon S3 buckets. A solutions architect needs to ensure that the data is encrypted at rest before the data is uploaded to the S3 buckets. The data also must be encrypted in transit.

Which solution meets these requirements?

- A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- C. Create bucket policies that require the use of server-side encryption with S3 managed encryption keys (SSE-S3) for S3 uploads.
- D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.

Correct Answer: A

Community vote distribution

A (97%)

techhb Highly Voted 10 months, 1 week ago

Selected Answer: A

here keyword is "before" "the data is encrypted at rest before the data is uploaded to the S3 buckets."

upvoted 17 times

palthainon Most Recent 1 month ago

Selected Answer: C

HTTPs would encrypt in transe, SSE3 managed keys fulfills requirement for at rest. This is an aws exam, not a best practices exam.

upvoted 1 times

peterang224 1 month, 2 weeks ago

Its_SaKar

upvoted 1 times

prabhjot 1 month, 3 weeks ago

Ans is B - Server-Side Encryption (SSE): ensure data is encrypted at rest and also Encryption in Transit: When you upload data to Amazon S3 using standard HTTPS requests.

upvoted 3 times

TariqKipkemei 2 months ago

Selected Answer: A

Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets

upvoted 1 times

Guru4Cloud 2 months, 3 weeks ago

Selected Answer: A

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.

upvoted 1 times

Guru4Cloud 2 months, 3 weeks ago

Selected Answer: A

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.

upvoted 1 times

Abobaloyi 5 months, 1 week ago

Selected Answer: A

data must be encrypted before uploaded , which means the client need to do it before uploading the data to S3

upvoted 2 times

datz 7 months, 3 weeks ago

Selected Answer: A

A, would meet requirements.

upvoted 1 times

nder 9 months, 1 week ago

Selected Answer: A

Because the data must be encrypted while in transit

upvoted 2 times

 **LuckyAro** 10 months ago

Selected Answer: A

A is correct IMO

upvoted 1 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/53840-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: A

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.

upvoted 2 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: A

Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets

upvoted 2 times

 **Kesha** 3 months, 4 weeks ago

B. With server-side encryption, it automatically encrypts the data at rest using encryption keys managed by AWS.

upvoted 1 times

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the 'same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.

What should the solutions architect do to meet these requirements?

- A. Increase the minimum capacity for the Auto Scaling group.
- B. Increase the maximum capacity for the Auto Scaling group.
- C. Configure scheduled scaling to scale up to the desired compute level.
- D. Change the scaling policy to add more EC2 instances during each scaling operation.

Correct Answer: C

Community vote distribution

C (100%)

 **ManOnTheMoon** Highly Voted 9 months, 3 weeks ago

GOOD LUCK EVERYONE :) YOU CAN DO THIS

upvoted 18 times

 **david76x** Highly Voted 10 months, 1 week ago

Selected Answer: C

C is correct. Goodluck everybody!

upvoted 8 times

 **Guru4Cloud** Most Recent 2 months, 3 weeks ago

Selected Answer: C

Configuring scheduled scaling actions allows the Auto Scaling group to scale up to the desired capacity at a scheduled time (1 AM in this case) when the batch jobs start. This ensures the desired compute capacity is reached immediately.

The Auto Scaling group can then scale down based on metrics after the batch jobs complete.

upvoted 3 times

 **hsinchang** 4 months, 1 week ago

Selected Answer: C

The time is given, use scheduled for optimal cost

upvoted 1 times

 **qacollin** 7 months, 2 weeks ago

just scheduled my exam :)

upvoted 5 times

 **awscerts023** 9 months, 3 weeks ago

Reached here ! Did anyone schedule the real exam now ? How was it ?

upvoted 4 times

 **pal40sg** 9 months, 3 weeks ago

Thanks to everyone who contributed with answers :)

upvoted 4 times

 **ProfXsamson** 10 months ago

Selected Answer: C

C. I'm here at the end, leaving this here for posterity sake 02/01/2023.

upvoted 3 times

 **dedline** 10 months, 1 week ago

GL ALL!

upvoted 4 times

 **mhmt4438** 10 months, 2 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/27868-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Aninina** 10 months, 2 weeks ago

Selected Answer: C

C. Configure scheduled scaling to scale up to the desired compute level.

By configuring scheduled scaling, the solutions architect can set the Auto Scaling group to automatically scale up to the desired compute level at a specific time (1AM) when the batch job starts and then automatically scale down after the job is complete. This will allow the desired EC2 capacity to be reached quickly and also help in reducing the cost.

upvoted 4 times

 **bamishr** 10 months, 2 weeks ago

Selected Answer: C

Configure scheduled scaling to scale up to the desired compute level.

upvoted 1 times

 **Morinator** 10 months, 2 weeks ago

Selected Answer: C

predictable = schedule scaling

upvoted 4 times

A company serves a dynamic website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The website needs to support multiple languages to serve customers around the world. The website's architecture is running in the us-west-1 Region and is exhibiting high request latency for users that are located in other parts of the world.

The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.

What should a solutions architect do to meet these requirements?

- A. Replace the existing architecture with a website that is served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.
- B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.
- C. Create an Amazon API Gateway API that is integrated with the ALB. Configure the API to use the HTTP integration type. Set up an API Gateway stage to enable the API cache based on the Accept-Language request header.
- D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the EC2 instances and the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Correct Answer: B

Community vote distribution

B (100%)

✉️  **Yechi** Highly Voted 9 months, 1 week ago

Selected Answer: B

Configuring caching based on the language of the viewer

If you want CloudFront to cache different versions of your objects based on the language specified in the request, configure CloudFront to forward the Accept-Language header to your origin.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html>

upvoted 8 times

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

Isn't CloudFront for static websites though? Question specifically states the content is dynamic

upvoted 1 times

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

Selected Answer: B

By caching content based on the Accept-Language request header, CloudFront can serve the appropriate version of the website to users based on their language preferences. This solution allows the company to improve the website's performance for users around the world without having to recreate the existing architecture in multiple Regions.

upvoted 2 times

✉️  **A1975** 3 months, 4 weeks ago

Selected Answer: B

CloudFront allows you to customize cache behavior based on various request headers. By setting the cache behavior to cache based on the Accept-Language request header, CloudFront can store and serve language-specific versions of the website content, reducing the need to repeatedly fetch the content from the ALB for users with the same language preference.

upvoted 1 times

✉️  **kraken21** 8 months ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html#header-caching-web-language>

upvoted 1 times

✉️  **vherman** 9 months ago

Selected Answer: B

B is correct

upvoted 1 times

✉️  **Steve_4542636** 9 months ago

Selected Answer: B

I think it's b

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: B

B is the correct answer

upvoted 1 times

A rapidly growing ecommerce company is running its workloads in a single AWS Region. A solutions architect must create a disaster recovery (DR) strategy that includes a different AWS Region. The company wants its database to be up to date in the DR Region with the least possible latency. The remaining infrastructure in the DR Region needs to run at reduced capacity and must be able to scale up if necessary.

Which solution will meet these requirements with the LOWEST recovery time objective (RTO)?

- A. Use an Amazon Aurora global database with a pilot light deployment.
- B. Use an Amazon Aurora global database with a warm standby deployment.
- C. Use an Amazon RDS Multi-AZ DB instance with a pilot light deployment.
- D. Use an Amazon RDS Multi-AZ DB instance with a warm standby deployment.

Correct Answer: B

Community vote distribution

B (97%)

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

Selected Answer: B

Option A is incorrect because while Amazon Aurora global database is a good solution for disaster recovery, pilot light deployment provides only a minimalistic setup and would require manual intervention to make the DR Region fully operational, which increases the recovery time.

Option B is a better choice than Option A as it provides a warm standby deployment, which is an automated and more scalable setup than pilot light deployment. In this setup, the database is replicated to the DR Region, and the standby instance can be brought up quickly in case of a disaster.

Option C is incorrect because Multi-AZ DB instances provide high availability, not disaster recovery.

Option D is a good choice for high availability, but it does not meet the requirement for DR in a different region with the least possible latency.
upvoted 18 times

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

Selected Answer: B

Note: The difference between pilot light and warm standby can sometimes be difficult to understand. Both include an environment in your DR Region with copies of your primary Region assets. The distinction is that pilot light cannot process requests without additional action taken first, whereas warm standby can handle traffic (at reduced capacity levels) immediately. The pilot light approach requires you to "turn on" servers, possibly deploy additional (non-core) infrastructure, and scale up, whereas warm standby only requires you to scale up (everything is already deployed and running). Use your RTO and RPO needs to help you choose between these approaches.

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>
upvoted 15 times

 **TariqKipkemei** Most Recent 2 months ago

Selected Answer: B

The warm standby approach involves ensuring that there is a scaled down, but fully functional, copy of your production environment in another Region.

With the pilot light approach, you replicate your data from one Region to another and provision a copy of your core workload infrastructure. Resources required to support data replication and backup, such as databases and object storage, are always on. Other elements, such as application servers, are loaded with application code and configurations, but are "switched off".

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

An Amazon Aurora global database with a warm standby deployment provides continuous replication from one AWS Region to another, keeping the DR database up-to-date with minimal latency.

upvoted 1 times

 **A1975** 3 months, 4 weeks ago

Selected Answer: B

In a Pilot Light scenario, only an EC2 Instance and a DB may be running. In Warm Standby, however, everything is running — in a much smaller capacity. This means the load balancer, gateways, databases, all subnets, and everything else are ready to go on a moment's notice.

with reference to below statement Option B is a better choice than Option A.

"The remaining infrastructure in the DR Region needs to run at reduced capacity and must be able to scale up if necessary".

upvoted 1 times

 **krisfromtw** 9 months, 2 weeks ago

Selected Answer: D

should be D.

upvoted 1 times

 **leoattf** 9 months, 1 week ago

No, my friend. The question asks for deployment in another Region. Hence, it cannot be C or D.

The answer is B because is Global (different regions) and Ward Standby has faster RTO than Pilot Light.

upvoted 7 times

A company runs an application on Amazon EC2 instances. The company needs to implement a disaster recovery (DR) solution for the application. The DR solution needs to have a recovery time objective (RTO) of less than 4 hours. The DR solution also needs to use the fewest possible AWS resources during normal operations.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS Lambda and custom scripts.
- B. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation.
- C. Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times.
- D. Launch EC2 instances in a secondary Availability Zone. Keep the EC2 instances in the secondary Availability Zone active at all times.

Correct Answer: D

Community vote distribution

B (100%)

 **NolaHolla**  9 months, 2 weeks ago

Guys, sorry but I don't really have time to deepdive as my exam is soon. Based on chatGPT and my previous study the answer should be B "Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation," would likely be the most suitable solution for the given requirements.

This option allows for the creation of Amazon Machine Images (AMIs) to back up the EC2 instances, which can then be copied to a secondary AWS region to provide disaster recovery capabilities. The infrastructure deployment in the secondary region can be automated using AWS CloudFormation, which can help to reduce the amount of time and resources needed for deployment and management.

upvoted 7 times

 **NBone** 4 months, 1 week ago

please how do you use chatGPT to study for these questions?

upvoted 3 times

 **nickolaj**  9 months, 1 week ago

Selected Answer: B

Option B would be the most operationally efficient solution for implementing a DR solution for the application, meeting the requirement of an RTO of less than 4 hours and using the fewest possible AWS resources during normal operations.

By creating Amazon Machine Images (AMIs) to back up the EC2 instances and copying them to a secondary AWS Region, the company can ensure that they have a reliable backup in the event of a disaster. By using AWS CloudFormation to automate infrastructure deployment in the secondary Region, the company can minimize the amount of time and effort required to set up the DR solution.

upvoted 6 times

 **vijaykamal**  2 months ago

Selected Answer: B

Option D suggests launching EC2 instances in a secondary Availability Zone (AZ), but AZs are not separate AWS Regions. While it provides high availability within a Region, it doesn't offer geographic redundancy, which is essential for disaster recovery.

upvoted 1 times

 **TariqKipkemei** 2 months ago

Selected Answer: B

needs to use the fewest possible AWS resources during normal operations = backup & restore

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation

upvoted 1 times

 **AMYMY** 2 months, 3 weeks ago

B SHOULD BE RIGHT

upvoted 1 times

 **A1975** 3 months, 4 weeks ago

Selected Answer: B

Option A: Add complexity and management overhead.

Option B: Creating AMIs for backup and using AWS CloudFormation for infrastructure deployment in the secondary Region is a more streamlined and automated approach. CloudFormation allows you to define and provision resources in a declarative manner, making it easier to maintain and update your infrastructure. This solution is more operationally efficient compared to Option A.

Option C: could be expensive and not fully aligned with the requirement of using the fewest possible AWS resources during normal operations.

Option D: might not be sufficient for meeting the DR requirements, as Availability Zones are still within the same AWS Region and might be subject to the same regional-level failures.

upvoted 1 times

✉ **NBone** 4 months, 1 week ago

Please I would really appreciate clarification with this question. The community has voted 100% that the right answer is B. However, option D is shown to be the correct answer. So, who sets the correct answer? Which one should new comers like myself believe? the community's or the other (which am guessing is set by the moderators????) Please help.

upvoted 2 times

✉ **SimiTik** 7 months, 1 week ago

C may satisfy the requirement of using the fewest possible AWS resources during normal operations, it may not be the most operationally efficient or cost-effective solution in the long term.

upvoted 2 times

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

So Weird , they have product for this > Elastic Disaster Recovery , but option is not given .

upvoted 1 times

✉ **Yechi** 9 months, 1 week ago

Selected Answer: B

https://docs.aws.amazon.com/zh_cn/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore

upvoted 4 times

✉ **Joan111edu** 9 months, 2 weeks ago

Selected Answer: B

the answer should be B

--->recovery time objective (RTO) of less than 4 hours.

https://docs.aws.amazon.com/zh_cn/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore

upvoted 3 times

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Correct Answer: A*Community vote distribution*

C (62%)

A (38%)

✉  **asoli**  8 months, 2 weeks ago

Selected Answer: C

At first, I thought the answer is A. But it is C.

It seems that there is no information in the question about CPU or Memory usage.

So, we might think the answer is A. why? because what we need is to have the required (desired) number of instances. It already has scheduled scaling that works well in this scenario. Scale down after working hours and scale up in working hours. So, it just needs to adjust the desired number to start from 20 instances.

But here is the point it shows A is WRONG!!!

If it started with desired 20 instances, it will keep it for the whole day. What if the load is reduced? We do not need to keep the 20 instances always. That 20 is the MAXIMUM number we need, no the DESIRE number. So it is against COST that is the main objective of this question.

So, the answer is C

upvoted 14 times

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

If it starts with 20 instances it will not keep it all day. It will scale down based on demand. The scheduled action in Option A simply ensures that there are enough instances running to handle the increased traffic when the day begins, while still allowing the Auto Scaling group to scale up or down based on demand during the rest of the day. <https://docs.aws.amazon.com/autoscaling/ec2/userguide/scale-your-group.html>

upvoted 8 times

✉  **xdkonorek2** 4 days, 16 hours ago

This is right, setting desired capacity doesn't turn off autoscaling policies

upvoted 1 times

✉  **wearrexdzw3123**  1 week, 6 days ago

My mistake, I should have chosen c. A lower threshold can expand in advance, and lowering cooling can increase the expansion frequency.

upvoted 1 times

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

Selected Answer: A

I choose option A because the root of the problem is the inability of the scaling speed in the morning to meet the demand, rather than what criteria to use for scaling.

upvoted 1 times

✉  **TariqKipkemei** 2 months ago

To keep costs to a minimum target tracking is the best option.

For example the scaling metric is the average CPU utilization of the EC2 auto scaling instances, and their average during the day should always be 80%. When CloudWatch detects that the average CPU utilization is beyond 80% at start of day, it will trigger the target tracking policy to scale out the auto scaling group to meet this target utilization. Once everything is settled and the average CPU utilization has gone below 80% at night, another scale in action will kick in and reduce the number of auto scaling instances in the auto scaling group.

upvoted 3 times

✉  **TariqKipkemei** 2 months ago

Option C is best

upvoted 1 times

 **Ramdi1** 2 months, 1 week ago

Selected Answer: A

I am going A based on it stating upto 20 so you already know what they maximum they use which is n a sense consistent. however i can see why people have put C. I think they need more clarification on the questions.

upvoted 2 times

 **Uzbekistan** 2 months, 2 weeks ago

Selected Answer: A

A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.

upvoted 2 times

 **Uzbekistan** 2 months, 2 weeks ago

CHATGPT says Answers is A

A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.

upvoted 1 times

 **BrijMohan08** 2 months, 3 weeks ago

Selected Answer: A

Scaling Out: In the morning when you schedule the AWS EC2 scaling to have a minimum and maximum of 20 instances, if the load on your application increases beyond the current number of instances, AWS Auto Scaling will automatically launch new instances to meet the demand up to the maximum of 20 instances.

Scaling In: As the load on your application decreases in the afternoon or night, AWS Auto Scaling will continuously monitor the health and load of your instances. If the instances are underutilized and can be terminated without affecting your application's performance, AWS Auto Scaling will automatically scale in by terminating excess instances,

Why not D? If you specify the min instance, AWS will always keep the minimum number of instances (20 in this case) running.

upvoted 2 times

 **LazyTs** 2 months, 3 weeks ago

It's A, C will not be fast enough with the sudden influx of the users, if C is fast enough then the original scenario should already be good enough as the 20 is already the max which set to start at working hours(when CPU starts to spin up)

upvoted 1 times

 **kapalulz** 3 months, 3 weeks ago

Selected Answer: C

C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period

upvoted 1 times

 **Mia2009687** 4 months, 3 weeks ago

Selected Answer: C

I was in team A. But from the definition of desired capacity, it seems once we set it as 20, it will try to keep it as 20 which is not saving cost.

Desired capacity: Represents the initial capacity of the Auto Scaling group at the time of creation. An Auto Scaling group attempts to maintain the desired capacity. It starts by launching the number of instances that are specified for the desired capacity, and maintains this number of instances as long as there are no scaling policies or scheduled actions attached to the Auto Scaling group.

upvoted 2 times

 **DrWatson** 5 months, 4 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/consolidated-view-of-warm-up-and-cooldown-settings.html>

DefaultCooldown

Only needed if you use simple scaling policies.

API operation: CreateAutoScalingGroup, UpdateAutoScalingGroup

The amount of time, in seconds, between one scaling activity ending and another one starting due to simple scaling policies. For more information, see Scaling cooldowns for Amazon EC2 Auto Scaling (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scaling-cooldowns.html>)

Default: 300 seconds.

upvoted 2 times

 **Konb** 6 months, 1 week ago

Selected Answer: A

I think the "cost" part that talks against A is a catch. No information why the EC2s are slow - maybe it's not CPU?

On the other hand we know that "Auto Scaling group scales up to 20 instances during work hours". A seems to be the only option that kinda satisfies requirements.

upvoted 1 times

 **xmark443** 6 months, 2 weeks ago

There may be days when the demand is lower. So schedule scaling is more cost than target tracking.

upvoted 1 times

 **justhereforccna** 6 months, 3 weeks ago

Selected Answer: A

Have to go with A on this one
upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: C

This option will scale up capacity faster in the morning to improve performance, but will still allow capacity to scale down during off hours. It achieves this as follows:

- A target tracking action scales based on a CPU utilization target. By triggering at a lower CPU threshold in the morning, the Auto Scaling group will start scaling up sooner as traffic ramps up, launching instances before utilization gets too high and impacts performance.
- Decreasing the cooldown period allows Auto Scaling to scale more aggressively, launching more instances faster until the target is reached. This speeds up the ramp-up of capacity.
- However, unlike a scheduled action to set a fixed minimum/maximum capacity, with target tracking the group can still scale down during off hours based on demand. This helps minimize costs.

upvoted 3 times

✉  **Dr_Chomp** 7 months, 3 weeks ago

Selected Answer: A

I'm going with A - it tells us that 20 instances is the normal capacity during the work day - so scheduling that at the start of the work day means you don't need to put load on the system to trigger scale-out. So this is like a warm start. Cool down has nothing to do with anything and it doesn't mention anything about CPU/resources for target setting.

upvoted 1 times

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.

What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose two.)

- A. Configure storage Auto Scaling on the RDS for Oracle instance.
- B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
- C. Configure an alarm on the RDS for Oracle instance for low free storage space.
- D. Configure the Auto Scaling group to use the average CPU as the scaling metric.
- E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

Correct Answer: AC

Community vote distribution

AD (91%) 9%

 **klayytech**  8 months ago

Selected Answer: AD

- A) Configure storage Auto Scaling on the RDS for Oracle instance.
= Makes sense. With RDS Storage Auto Scaling, you simply set your desired maximum storage limit, and Auto Scaling takes care of the rest.
- B) Migrate the database to Amazon Aurora to use Auto Scaling storage.
= Scenario specifies application's data layer uses Oracle-specific PL/SQL functions. This rules out migration to Aurora.
- C) Configure an alarm on the RDS for Oracle instance for low free storage space.
= You could do this but what does it fix? Nothing. The CW notification isn't going to trigger anything.
- D) Configure the Auto Scaling group to use the average CPU as the scaling metric.
= Makes sense. The CPU utilization is the precursor to the storage outage. When the ec2 instances are overloaded, the RDS instance storage hits its limits, too.

upvoted 12 times

 **TariqKipkemei**  1 month, 4 weeks ago

Selected Answer: AD

Configure storage Auto Scaling on the RDS for Oracle instance and Configure the Auto Scaling group to use the average CPU as the scaling metric to accommodate the increased traffic automatically.

upvoted 1 times

 **vijaykamal** 2 months ago

Selected Answer: AD

Option B (Migrate the database to Amazon Aurora) may be a good long-term solution, but it involves database migration, which can be complex and time-consuming. For immediate scalability and to address the storage issue, configuring storage Auto Scaling on the existing RDS instance is a more immediate and straightforward solution.

Option C (Configure an alarm on the RDS for Oracle instance for low free storage space) is useful for monitoring, but it doesn't proactively address the storage issue by automatically expanding storage as needed.

Option E (Configure the Auto Scaling group to use the average free memory as the scaling metric) is less common as a scaling metric for EC2 instances compared to CPU utilization. While memory can be an important factor for application performance, CPU utilization is typically a more commonly used metric for scaling decisions. It also doesn't directly address the RDS storage issue.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: AD

A. By enabling storage Auto Scaling on the RDS for Oracle instance, it will automatically add more storage when the existing storage is running out, ensuring the application's data layer can handle the increased data storage requirements.

D. By configuring the Auto Scaling group to use the average CPU utilization as the scaling metric, it can automatically add more EC2 instances to the Auto Scaling group when the CPU utilization exceeds a certain threshold. This will help handle the increased traffic and workload on the EC2 instances in the multi-tier application.

upvoted 1 times

 **A1975** 3 months, 4 weeks ago

Selected Answer: AD

A. By enabling storage Auto Scaling on the RDS for Oracle instance, it will automatically add more storage when the existing storage is running out, ensuring the application's data layer can handle the increased data storage requirements.

D. By configuring the Auto Scaling group to use the average CPU utilization as the scaling metric, it can automatically add more EC2 instances to the Auto Scaling group when the CPU utilization exceeds a certain threshold. This will help handle the increased traffic and workload on the EC2 instances in the multi-tier application.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: AD

These options will allow the system to scale both the compute tier (EC2 instances) and the data tier (RDS storage) automatically as traffic increases:

A. Storage Auto Scaling will allow the RDS for Oracle instance to automatically increase its allocated storage when free storage space gets low. This ensures the database does not run out of capacity and can continue serving data to the application.

D. Configuring the EC2 Auto Scaling group to scale based on average CPU utilization will allow it to launch additional instances automatically as traffic causes higher CPU levels across the instances. This scales the compute tier to handle increased demand.

upvoted 2 times

 **kraken21** 8 months ago

Selected Answer: AD

Auto scaling storage RDS will ease storage issues and migrating Oracle PL/SQL to Aurora is cumbersome. Also Aurora has auto storage scaling by default.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PIOPS.Autoscaling

upvoted 2 times

 **Nel8** 9 months ago

Selected Answer: BD

My answer is B & D...

B. Migrate the database to Amazon Aurora to use Auto Scaling Storage. --- Aurora storage is also self-healing. Data blocks and disks are continuously scanned for errors and repaired automatically.

D. Configure the Auto Scaling group to use the average CPU as the scaling metric. -- Good choice.

I believe either A & C or B & D options will work.

upvoted 3 times

 **FourOfAKind** 8 months, 4 weeks ago

In this question, you have Oracle DB, and Amazon Aurora is for MySQL/PostgreSQL. A and D are the correct choices.

upvoted 5 times

 **dcp** 8 months, 1 week ago

You can migrate Oracle PL/SQL to Aurora:

<https://docs.aws.amazon.com/dms/latest/oracle-to-aurora-mysql-migration-playbook/chap-oracle-aurora-mysql.sql.html>

upvoted 1 times

 **dcp** 8 months, 1 week ago

I still think A is the answer, because RDS for Oracle auto scaling once enabled it will automatically adjust the storage capacity.

upvoted 1 times

 **Ja13** 9 months, 1 week ago

Selected Answer: AD

a and d

upvoted 3 times

 **KZM** 9 months, 1 week ago

A and D.

upvoted 3 times

 **GwonLEE** 9 months, 1 week ago

Selected Answer: AD

a and d

upvoted 3 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: AD

A and D

upvoted 2 times

 **Joan111edu** 9 months, 2 weeks ago

Selected Answer: AD

<https://www.examtopics.com/discussions/amazon/view/46534-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **ChrisG1454** 9 months, 2 weeks ago

answer is A and D

upvoted 1 times

✉ **ChrisG1454** 9 months, 2 weeks ago

<https://www.examtopics.com/discussions/amazon/view/46534-exam-aws-certified-solutions-architect-associate-saa-c02/#:~:text=%22This%20overloads%20the%20EC2%20instances%20and%20causes%20the,the%20RDS%20for%20Oracle%20instance%20upvoted%202%20times>

upvoted 1 times

✉ **rrharris** 9 months, 2 weeks ago

A and D are the Answers

upvoted 1 times

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

- A. Use AWS Storage Gateway for files to store and process the video content.
- B. Use AWS Storage Gateway for volumes to store and process the video content.
- C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
- D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing.

Correct Answer: A

Community vote distribution

D (81%)

A (19%)

 **bdp123**  9 months, 2 weeks ago

Selected Answer: D

Storage gateway is not used for storing content - only to transfer to the Cloud
upvoted 18 times

 **kraken21**  8 months ago

Selected Answer: D

There is no on-prem/non Aws infrastructure to create a gateway. Also, EFS+EBS is more expensive than EFS and S3. So D is the best option.
upvoted 6 times

 **liux99**  3 weeks ago

Storage gateway is intended for on-premises applications to access cloud storage, so A, B is out. The question explicitly states that the files are uploaded and stored in EFS, not S3, so D is not correct. The answer is C. The EFS storage costs 10 times more than EBS, so moving files to EBS after processing is the solution.

upvoted 1 times

 **beginnercloud** 1 month ago

Selected Answer: D

Answer D is correct.
Storage gateway is not used for storing content - only to transfer to the Cloud
upvoted 1 times

 **TariqKipkemei** 1 month, 4 weeks ago

Selected Answer: D

Cost effective = Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing
upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: D

Amazon S3 provides low-cost object storage for storing large amounts of unstructured data like videos. The videos can be stored in S3 durably and reliably.

For processing, the video files can be temporarily copied from S3 to an EBS volume attached to the EC2 instance. EBS provides low latency block storage for high performance video processing.

Once processing is complete, the output can be stored back in S3.

upvoted 2 times

 **bjexamprep** 3 months, 3 weeks ago

Selected Answer: D

The question doesn't give enough information. Well, quite a few AWS exam questions don't provide enough info.
Ideally, A could be the best answer if it mentions S3 as the backend of storage gateway. Because if it doesn't mention S3 as the backend, that implies either Storage gateway as the storage(which is impossible) or continue using EFS(also impossible).
D is not ideal, because it will introduce video download cost for downloading files from S3 to EBS temporary storage. But it is the best option we have.

upvoted 1 times

✉️ **Undisputed** 4 months ago

Selected Answer: D

A more cost-effective storage solution for this scenario would be Amazon Simple Storage Service (Amazon S3). Amazon S3 is an object storage service that offers high scalability, durability, and availability at a lower cost compared to Amazon EFS. By using Amazon S3, you only pay for the storage you use, and it is typically more cost-efficient for scenarios where data is accessed less frequently, such as video storage for processing.

upvoted 1 times

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

Selected Answer: A

The result should be A.

Amazon storage gateway has 4 types, S3 File Gateway, FSx file gateway, Type Gateway and Volume Gateway.

If not specific reference file gateway should be default as S3 gateway, which sent file over to S3 the most cost effective storage in AWS.

Why not D, the reason is last sentence, there are multiple EC2 servers for processing the video and EBS can only attach to 1 EC2 instance at a time, so if you use EBS, which mean for each EC2 instance you will have 1 EBS. This rule out D.

upvoted 1 times

✉️ **argl1995** 5 months ago

We can use multi-attach feature of EBS to attach one EBS volume to multiple Ec2 instances

upvoted 2 times

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

AWS Storage Gateway = extend storage to onprem

upvoted 1 times

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

Selected Answer: D

D: MOST cost-effective of these options = S3

upvoted 1 times

✉️ **omoakin** 6 months ago

CCCCCCCCCC

upvoted 1 times

✉️ **kruasan** 7 months ago

Selected Answer: D

he most cost-effective storage solution in this scenario would be:

D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing.

This option provides the lowest-cost storage by using:

- Amazon S3 for large-scale, durable, and inexpensive storage of the video content. S3 storage costs are significantly lower than EFS.
- Amazon EBS only temporarily during processing. By mounting an EBS volume only when a video needs to be processed, and unmounting it after, the time the content spends on the higher-cost EBS storage is minimized.
- The EBS volume can be sized to match the workload needs for active processing, keeping costs lower. The volume does not need to store the entire video library long-term.

upvoted 1 times

✉️ **GalileoEC2** 8 months, 1 week ago

Option A, which uses AWS Storage Gateway for files to store and process the video content, would be the most cost-effective solution.

With this approach, you would use an AWS Storage Gateway file gateway to access the video content stored in Amazon S3. The file gateway presents a file interface to the EC2 instances, allowing them to access the video content as if it were stored on a local file system. The video processing tasks can be performed on the EC2 instances, and the processed files can be stored back in S3.

This approach is cost-effective because it leverages the lower cost of Amazon S3 for storage while still allowing for easy access to the video content from the EC2 instances using a file interface. Additionally, Storage Gateway provides caching capabilities that can further improve performance by reducing the need to access S3 directly.

upvoted 1 times

✉️ **scs50** 8 months, 1 week ago

Selected Answer: A

Amazon S3 File gateway is using S3 behind the scene.

<https://docs.aws.amazon.com/filegateway/latest/files3/what-is-file-s3.html>

upvoted 1 times

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

Amazon S3 File Gateway

Amazon S3 File Gateway presents a file interface that enables you to store files as objects in Amazon S3 using the industry-standard NFS and SMB file protocols, and access those files via NFS and SMB from your data center or Amazon EC2, or access those files as objects directly in Amazon S3. POSIX-style metadata, including ownership, permissions, and timestamps are durably stored in Amazon S3 in the user-metadata of the object associated with the file. Once objects are transferred to S3, they can be managed as native S3 objects and bucket policies such as lifecycle management and Cross-Region Replication (CRR), and can be applied directly to objects stored in your bucket. Amazon S3 File Gateway also

publishes audit logs for SMB file share user operations to Amazon CloudWatch.

Customers can use Amazon S3 File Gateway to back up on-premises file data as objects in Amazon S3 (including Microsoft SQL Server and Oracle databases and logs), and for hybrid cloud workflows using data generated by on-premises applications for processing by AWS services such as machine learning or big data analytics.

upvoted 1 times

 **Brak** 8 months, 3 weeks ago

Selected Answer: A

It can't be D, since there are multiple servers accessing the video files which rules out EBS. File Gateway provides a shared filesystem to replace EFS, but uses S3 for storage to reduce costs.

upvoted 5 times

 **KZM** 9 months, 1 week ago

Using Amazon S3 for storing video content is the best way for cost-effectiveness I think. But I am still confused about why moved the data to EBS.

upvoted 3 times

 **KZM** 9 months, 1 week ago

A better solution would be to use a transcoding service like Amazon Elastic Transcoder to process the video content directly from Amazon S3. This would eliminate the need for storing the content on an EBS volume, reduce storage costs, and simplify the architecture by removing the need for managing EBS volumes.

upvoted 2 times

A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must protect any sensitive data. The company also needs to receive monthly email messages if any financial information is present in the employee data.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Use Amazon Redshift to store the employee data in hierarchies. Unload the data to Amazon S3 every month.
- B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.
- C. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.
- D. Use Amazon Athena to analyze the employee data in Amazon S3. Integrate Athena with Amazon QuickSight to publish analysis dashboards and share the dashboards with users.
- E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

Correct Answer: CD

Community vote distribution

BE (100%)

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

Selected Answer: BE

Data in hierarchies : Amazon DynamoDB

B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.

Sensitive Info: Amazon Macie

E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

upvoted 10 times

 **gold4otas** 8 months ago

Can someone please provide explanation why options "B" & "C" are the correct options?

upvoted 1 times

 **smartegnine** 5 months, 2 weeks ago

C is half statement once event sent to Lambda what is next? Should send email right, but it does not say it.

upvoted 1 times

 **beginnercloud** Most Recent 1 month ago

Selected Answer: BE

B and E are the steps to meet all of the requirements.

upvoted 1 times

 **TariqKipkemei** 1 month, 4 weeks ago

Selected Answer: BE

Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: BE

B and E are the steps to meet all of the requirements.

B meets the need to store hierarchical employee data in DynamoDB for low latency queries at high traffic. DynamoDB can handle the access patterns for hierarchical data. Exporting to S3 monthly provides an audit trail.

E sets up Macie to analyze sensitive data and integrate with EventBridge to trigger monthly SNS notifications when financial data is present.

upvoted 2 times

 **A1975** 3 months, 4 weeks ago

Selected Answer: BE

J. Amazon DynamoDB is a fully managed NoSQL database service that provides low-latency, high-performance storage for hierarchical data. It handles high-traffic queries and delivering fast responses to retrieve employee data efficiently.

E. Amazon Macie is a service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Integrating Macie with Amazon EventBridge allows you to receive events whenever any financial information is identified in the employee data. By using Amazon SNS, you can receive these notifications via email.

upvoted 2 times

✉ **cesargalindo123** 5 months, 1 week ago

AE

<https://aws.amazon.com/es/blogs/big-data/query-hierarchical-data-models-within-amazon-redshift/>

upvoted 1 times

✉ **kruasan** 7 months ago

Selected Answer: BE

, the combination of DynamoDB for fast data queries, S3 for durable storage and backups, Macie for sensitive data monitoring, and EventBridge + SNS for email notifications satisfies all needs: fast query response, sensitive data protection, and monthly alerts. The solutions architect should implement DynamoDB with export to S3, and configure Macie with integration to send SNS email notifications.

upvoted 1 times

✉ **kruasan** 7 months ago

Generally, for building a hierarchical relationship model, a graph database such as Amazon Neptune is a better choice. In some cases, however, DynamoDB is a better choice for hierarchical data modeling because of its flexibility, security, performance, and scale.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/dynamodb-hierarchical-data-model/introduction.html>

upvoted 2 times

✉ **darn** 7 months, 1 week ago

why Dynamo and not Redshift?

upvoted 2 times

✉ **kruasan** 7 months ago

3. Hierarchical data - DynamoDB supports hierarchical (nested) data structures well in a NoSQL data model. Defining hierarchical employee data may be more complex in Redshift's columnar SQL data warehouse structure. DynamoDB is built around flexible data schemas that can represent complex relationships.

4. Data export - Both DynamoDB and Redshift allow exporting data to S3, so that requirement could be met with either service. However, overall DynamoDB is the better fit based on the points above regarding latency, scalability, and support for hierarchical data.

upvoted 4 times

✉ **kruasan** 7 months ago

1. Low latency - DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with single-digit millisecond latency. Redshift is a data warehouse solution optimized for complex analytical queries, so query latency would typically be higher. Since the requirements specify minimum latency for high-traffic queries, DynamoDB is better suited.

2. Scalability - DynamoDB is highly scalable, able to handle very high read and write throughput with no downtime. Redshift also scales, but may experience some downtime during rescale operations. For a high-traffic application, DynamoDB's scalability and availability are better matched.

upvoted 2 times

✉ **PRASAD180** 9 months, 1 week ago

BE is crt 100%

upvoted 1 times

✉ **KZM** 9 months, 1 week ago

B and E

To send monthly email messages, an SNS service is required.

upvoted 2 times

✉ **skiwili** 9 months, 1 week ago

Selected Answer: BE

B and E

upvoted 3 times

A company has an application that is backed by an Amazon DynamoDB table. The company's compliance requirements specify that database backups must be taken every month, must be available for 6 months, and must be retained for 7 years.

Which solution will meet these requirements?

- A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.
- B. Create a DynamoDB on-demand backup of the DynamoDB table on the first day of each month. Transition the backup to Amazon S3 Glacier Flexible Retrieval after 6 months. Create an S3 Lifecycle policy to delete backups that are older than 7 years.
- C. Use the AWS SDK to develop a script that creates an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the script on the first day of each month. Create a second script that will run on the second day of each month to transition DynamoDB backups that are older than 6 months to cold storage and to delete backups that are older than 7 years.
- D. Use the AWS CLI to create an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the command on the first day of each month with a cron expression. Specify in the command to transition the backups to cold storage after 6 months and to delete the backups after 7 years.

Correct Answer: B

Community vote distribution

A (78%)

B (22%)

 **beginnercloud** 1 month ago

Selected Answer: A

<https://aws.amazon.com/blogs/database/set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/>

upvoted 1 times

 **vijaykamal** 2 months ago

Selected Answer: A

Option B mentions using Amazon S3 Glacier Flexible Retrieval, but DynamoDB doesn't natively support transitioning backups to Amazon S3 Glacier. Options C and D involve custom scripts and EventBridge rules, which add complexity and may not be as reliable or efficient as using AWS Backup for this purpose.

upvoted 3 times

 **chanchal133** 3 months ago

Selected Answer: A

A is right ans

upvoted 1 times

 **MNotABot** 4 months, 3 weeks ago

All except A are "On-demand"

upvoted 1 times

 **narddrer** 4 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/BackupRestore.html>

Using DynamoDB with AWS Backup, you can copy your on-demand backups across AWS accounts and Regions, add cost allocation tags to on-demand backups, and transition on-demand backups to cold storage for lower costs. To use these advanced features, you must opt in to AWS Backup.

upvoted 4 times

 **kruasan** 7 months ago

Selected Answer: A

This solution satisfies the requirements in the following ways:

- AWS Backup will automatically take full backups of the DynamoDB table on the schedule defined in the backup plan (the first of each month).
- The lifecycle policy can transition backups to cold storage after 6 months, meeting that requirement.
- Setting a 7-year retention period in the backup plan will ensure each backup is retained for 7 years as required.
- AWS Backup manages the backup jobs and lifecycle policies, requiring no custom scripting or management.

upvoted 2 times

 **TariqKipkemei** 8 months ago

Answer is A

upvoted 1 times

 **TariqKipkemei** 1 month, 4 weeks ago

Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years

upvoted 1 times

 **mmustafa4455** 8 months, 1 week ago

Selected Answer: A
The correct Answer is A

<https://aws.amazon.com/blogs/database/set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/>

upvoted 1 times

 **mmustafa4455** 8 months, 1 week ago

Its B.

<https://aws.amazon.com/blogs/database/set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/>

upvoted 2 times

 **Wael216** 9 months, 1 week ago

Selected Answer: A
A is the answer
upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: A
A is the answer.
upvoted 1 times

 **skiwili** 9 months, 1 week ago

Selected Answer: A
A is the correct answe
upvoted 1 times

 **rrharris** 9 months, 1 week ago

A is the Answer

can be used to create backup schedules and retention policies for DynamoDB tables

upvoted 2 times

 **kpato87** 9 months, 1 week ago

Selected Answer: A
A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.
upvoted 3 times

A company is using Amazon CloudFront with its website. The company has enabled logging on the CloudFront distribution, and logs are saved in one of the company's Amazon S3 buckets. The company needs to perform advanced analyses on the logs and build visualizations.

What should a solutions architect do to meet these requirements?

- A. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
- B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.
- C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
- D. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.

Correct Answer: A

Community vote distribution

B (88%) 13%

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

Answer is B - Quicksite creating data visualizations

<https://docs.aws.amazon.com/quicksight/latest/user/welcome.html>
upvoted 5 times

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

Selected Answer: B

OptionB: Amazon Athena allows you to run standard SQL queries directly on the data stored in the S3 bucket.
Amazon QuickSight is a business intelligence (BI) service that allows you to create interactive and visual dashboards to analyze data. You can connect Amazon QuickSight to Amazon Athena to visualize the results of your SQL queries from the CloudFront logs.
upvoted 1 times

✉  **A1975** 3 months, 4 weeks ago

Selected Answer: B

OptionB: Amazon Athena allows you to run standard SQL queries directly on the data stored in the S3 bucket.
Amazon QuickSight is a business intelligence (BI) service that allows you to create interactive and visual dashboards to analyze data. You can connect Amazon QuickSight to Amazon Athena to visualize the results of your SQL queries from the CloudFront logs.
upvoted 1 times

✉  **ajay258** 6 months, 2 weeks ago

Answer is B
upvoted 1 times

✉  **FFO** 7 months, 3 weeks ago

Selected Answer: B

Athena and Quicksight. Glue is for ETL transformation
upvoted 1 times

✉  **TariqKipkemei** 8 months ago

Answer is B
Analysis on S3 = Athena
Visualizations = Quicksight
upvoted 1 times

✉  **GalileoEC2** 8 months, 1 week ago

Why the Hell A?
upvoted 1 times

✉  **GalileoEC2** 8 months, 2 weeks ago

Why AI as far as I know Glue is not used for visualization
upvoted 1 times

✉  **Bhrino** 9 months, 1 week ago

Selected Answer: B

B because athena can be used to analyse data in s3 buckets and AWS quicksight is literally used to create visual representation of data
upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: B

Using Athena to query the CloudFront logs in the S3 bucket and QuickSight to visualize the results is the best solution because it is cost-effective, scalable, and requires no infrastructure setup. It also provides a robust solution that enables the company to perform advanced analysis and build interactive visualizations without the need for a dedicated team of developers.

upvoted 1 times

 **skiwili** 9 months, 1 week ago

Selected Answer: B

Yes B is the answer

upvoted 1 times

 **obatunde** 9 months, 1 week ago

Selected Answer: B

Correct answer should be B.

upvoted 1 times

 **Namrash** 9 months, 1 week ago

B is correct

upvoted 1 times

 **kpato87** 9 months, 1 week ago

Selected Answer: B

Amazon Athena can be used to analyze data in S3 buckets using standard SQL queries without requiring any data transformation. By using Athena, a solutions architect can easily and efficiently query the CloudFront logs stored in the S3 bucket. The results of the queries can be visualized using Amazon QuickSight, which provides powerful data visualization capabilities and easy-to-use dashboards. Together, Athena and QuickSight provide a cost-effective and scalable solution to analyze CloudFront logs and build visualizations.

upvoted 4 times

 **Joan111edu** 9 months, 2 weeks ago

Selected Answer: B

should be B

upvoted 3 times

 **bdp123** 9 months, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/big-data/harmonize-query-and-visualize-data-from-various-providers-using-aws-glue-amazon-athena-and-amazon-quicksight/>

<https://docs.aws.amazon.com/comprehend/latest/dg/tutorial-reviews-visualize.html>

upvoted 2 times

 **tellmenowwww** 9 months ago

attached file realted with B

upvoted 1 times

A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.

Which solution meets these requirements?

- A. Enable a Multi-AZ deployment for the DB instance.
- B. Enable auto scaling for the DB instance in one Availability Zone.
- C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.
- D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Correct Answer: D

Community vote distribution

A (93%) 7%

✉️  **KZM** Highly Voted 9 months, 1 week ago

A:

By using Multi-AZ deployment, the company can achieve an RPO of less than 1 second because the standby instance is always in sync with the primary instance, ensuring that data changes are continuously replicated.

upvoted 10 times

✉️  **rrharris** Highly Voted 9 months, 2 weeks ago

Correct Answer is A

upvoted 7 times

✉️  **A1975** Most Recent 3 months, 3 weeks ago

Selected Answer: A

Read Replicas:

Read Replicas are asynchronous and support read scalability.

It is used to improve performance.

Read Replicas can be in the same region or in a different region for disaster recovery purposes, but this involves manual intervention, which means Read Replicas do not provide automatic failover and requires DNS updates and application changes

Multi-AZ:

Multi-AZ maintains a synchronous standby replica of the primary instance in a different Availability Zone within the same region.

Multi-AZ deployments provide high availability and automatic failover.

Option A is better choice with respect to below statement,

"the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases."

upvoted 4 times

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

Selected Answer: D

option A doesn't provide Data integrity only achieved in Option D using CDC.

upvoted 1 times

✉️  **FF0** 7 months, 3 weeks ago

Selected Answer: A

Used for DR. Every single change is replicated in a standby AZ. If we lose the main AZ, (uses the same DNS name) standby becomes automatic failover and the new main DB.

upvoted 3 times

✉️  **TariqKipkemei** 8 months ago

Answer is A

High availability = Multi AZ

upvoted 1 times

✉️  **Steve_4542636** 9 months ago

Selected Answer: A

My vote is A

upvoted 1 times

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

Agree with A

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: A

Multi-AZ is a synchronous communication with the Master in "real time" and fail over will be almost instant.

upvoted 2 times

 **GwonLEE** 9 months, 1 week ago

Selected Answer: A

correct is A

upvoted 1 times

 **Namrash** 9 months, 1 week ago

A should be correct

upvoted 2 times

 **Joan111edu** 9 months, 2 weeks ago

Selected Answer: A

should be A

upvoted 2 times

A company runs a web application that is deployed on Amazon EC2 instances in the private subnet of a VPC. An Application Load Balancer (ALB) that extends across the public subnets directs web traffic to the EC2 instances. The company wants to implement new security measures to restrict inbound traffic from the ALB to the EC2 instances while preventing access from any other source inside or outside the private subnet of the EC2 instances.

Which solution will meet these requirements?

- A. Configure a route in a route table to direct traffic from the internet to the private IP addresses of the EC2 instances.
- B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.
- C. Move the EC2 instances into the public subnet. Give the EC2 instances a set of Elastic IP addresses.
- D. Configure the security group for the ALB to allow any TCP traffic on any port.

Correct Answer: C

Community vote distribution

B (100%)

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB
upvoted 1 times

 **awslearner7** 4 months, 1 week ago

can anybody explains the question?
upvoted 1 times

 **David_Ang** 3 weeks, 5 days ago

is just admins fault dont worry, he just made a mistake, because "C" doesnt make any sence
upvoted 1 times

 **Abrar2022** 6 months ago

Read the discussion, that's the whole point why examtopics picks the wrong answer. Follow most voted answer not examtopics answer
upvoted 4 times

 **antropaws** 6 months, 1 week ago

Selected Answer: B

It's very confusing that the system marks C as correct.
upvoted 1 times

 **FF0** 7 months, 3 weeks ago

Selected Answer: B

This is B. Question already tells us they only want ONLY traffic from the ALB.
upvoted 1 times

 **TariqKipkemei** 8 months ago

Answer is B
upvoted 1 times

 **TariqKipkemei** 1 month, 4 weeks ago

A security group acts as a firewall that controls the traffic allowed to and from the resources in your virtual private cloud (VPC).
upvoted 1 times

 **GalileoEC2** 8 months, 2 weeks ago

Why C! another crazy answer , If i am concern about security why I would want to expose my EC2 to the public internet, not make sense at all, am I correct with this? I also go with B
upvoted 2 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: B

B is the correct answer.
upvoted 2 times

 **kpato87** 9 months, 1 week ago

Selected Answer: B

configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB. This ensures that only the traffic originating from the ALB is allowed access to the EC2 instances in the private subnet, while denying any other traffic from other sources. The other options do not provide a suitable solution to meet the stated requirements.

upvoted 3 times

 **Bhawesh** 9 months, 2 weeks ago

Selected Answer: B

B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.

upvoted 3 times

A research company runs experiments that are powered by a simulation application and a visualization application. The simulation application runs on Linux and outputs intermediate data to an NFS share every 5 minutes. The visualization application is a Windows desktop application that displays the simulation output and requires an SMB file system.

The company maintains two synchronized file systems. This strategy is causing data duplication and inefficient resource usage. The company needs to migrate the applications to AWS without making code changes to either application.

Which solution will meet these requirements?

- A. Migrate both applications to AWS Lambda. Create an Amazon S3 bucket to exchange data between the applications.
- B. Migrate both applications to Amazon Elastic Container Service (Amazon ECS). Configure Amazon FSx File Gateway for storage.
- C. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon Simple Queue Service (Amazon SQS) to exchange data between the applications.
- D. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon FSx for NetApp ONTAP for storage.

Correct Answer: D

Community vote distribution

D (96%) 4%

 **LuckyAro**  9 months, 1 week ago

Selected Answer: D

Amazon FSx for NetApp ONTAP provides shared storage between Linux and Windows file systems.

upvoted 13 times

 **rrharris**  9 months, 2 weeks ago

Answer is D

upvoted 7 times

 **TariqKipkemei**  1 month, 4 weeks ago

Selected Answer: D

One of the use cases for Amazon FSx for NetApp ONTAP is when you need to move workloads running on NetApp or other NFS/SMB/iSCSI servers to AWS without modifying application code or how you manage data.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: D

The key requirements are:

Simulation app runs on Linux, outputs data to NFS
Visualization app runs on Windows, requires SMB file system
Migrate apps to AWS without code changes
Eliminate data duplication and inefficient resource usage
upvoted 1 times

 **Abrar2022** 6 months ago

For shared storage between Linux and windows you need to implement Amazon FSx for NetApp ONTAP

upvoted 2 times

 **kruasan** 7 months ago

Selected Answer: D

This solution satisfies the needs in the following ways:

- Amazon EC2 provides a seamless migration path for the existing server-based applications without code changes. The simulation app can run on Linux EC2 instances and the visualization app on Windows EC2 instances.
- Amazon FSx for NetApp ONTAP provides highly performant file storage that is accessible via both NFS and SMB. This allows the simulation app to write to NFS shares as currently designed, and the visualization app to access the same data via SMB.
- FSx for NetApp ONTAP ensures the data is synchronized and up to date across the file systems. This addresses the data duplication issues of the current setup.
- Resources can be scaled efficiently since EC2 and FSx provide scalable compute and storage on demand.

upvoted 5 times

 **kruasan** 7 months ago

The other options would require more significant changes:

- A. Migrating to Lambda would require re-architecting both applications and not meet the requirement to avoid code changes. S3 does not provide file system access.
- B. While ECS could run the apps without code changes, FSx File Gateway only provides S3 or EFS storage, neither of which offer both NFS and SMB access. Data exchange would still be an issue.
- C. Using SQS for data exchange between EC2 instances would require code changes to implement a messaging system rather than a shared file system.

upvoted 1 times

✉  **mr_kanchan** 3 months, 3 weeks ago

How does the data duplication issue get addressed on selecting D ?

upvoted 1 times

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

Maybe I'm wrong, but I feel like the data is duplicated between the two types of EC2 instances. By using the FSX ONTAP will address this issue.

upvoted 1 times

✉  **Wael216** 9 months ago

Selected Answer: D

windows => FSX

we didn't mention containers => can't be ECS

upvoted 1 times

✉  **everfly** 9 months, 1 week ago

Selected Answer: D

Amazon FSx for NetApp ONTAP is a fully managed service that provides shared file storage built on NetApp's popular ONTAP file system. It supports NFS, SMB, and iSCSI protocols² and also allows multi-protocol access to the same data

upvoted 1 times

✉  **Yechi** 9 months, 1 week ago

Selected Answer: D

Amazon FSx for NetApp ONTAP is a fully-managed shared storage service built on NetApp's popular ONTAP file system. Amazon FSx for NetApp ONTAP provides the popular features, performance, and APIs of ONTAP file systems with the agility, scalability, and simplicity of a fully managed AWS service, making it easier for customers to migrate on-premises applications that rely on NAS appliances to AWS. FSx for ONTAP file systems are similar to on-premises NetApp clusters. Within each file system that you create, you also create one or more storage virtual machines (SVMs). These are isolated file servers each with their own endpoints for NFS, SMB, and management access, as well as authentication (for both administration and end-user data access). In turn, each SVM has one or more volumes which store your data.

<https://aws.amazon.com/de/blogs/storage/getting-started-cloud-file-storage-with-amazon-fsx-for-netapp-ontap-using-netapp-management-tools/>

upvoted 3 times

✉  **zTopic** 9 months, 2 weeks ago

Selected Answer: B

B is correct I believe

upvoted 1 times

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.

Which solution meets these requirements?

- A. Run a query with Amazon Athena to generate the report.
- B. Create a report in Cost Explorer and download the report.
- C. Access the bill details from the billing dashboard and download the bill.
- D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

Cost Explorer looks at the usage pattern or history
upvoted 5 times

 **TariqKipkemei** Most Recent 1 month, 4 weeks ago

Selected Answer: B

Create a report in Cost Explorer and download the report
upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

- ° Cost Explorer is a AWS service that allows you to view, analyze, and manage your AWS costs and usage. It provides a variety of reports that you can use to track your costs, including a report of AWS billed items listed by user.
- ° Creating a report in Cost Explorer is a quick and easy way to get the information you need. You can customize the report to include the specific data you want, and you can download the report in a variety of formats, including CSV, Excel, and PDF.

upvoted 2 times

 **Guru4Cloud** 2 months, 3 weeks ago

This is trick question -

You need to know the differences between the billing services.

upvoted 1 times

 **Wheretostart** 8 months, 2 weeks ago

Selected Answer: B

Cost Explorer
upvoted 1 times

 **pcops** 9 months, 1 week ago

Answer is B

upvoted 2 times

 **fulingyu288** 9 months, 2 weeks ago

Selected Answer: B

Answer is B
upvoted 3 times

 **rrharris** 9 months, 2 weeks ago

Answer is B
upvoted 2 times

A company hosts its static website by using Amazon S3. The company wants to add a contact form to its webpage. The contact form will have dynamic server-side components for users to input their name, email address, phone number, and user message. The company anticipates that there will be fewer than 100 site visits each month.

Which solution will meet these requirements MOST cost-effectively?

- A. Host a dynamic contact form page in Amazon Elastic Container Service (Amazon ECS). Set up Amazon Simple Email Service (Amazon SES) to connect to any third-party email provider.
- B. Create an Amazon API Gateway endpoint with an AWS Lambda backend that makes a call to Amazon Simple Email Service (Amazon SES).
- C. Convert the static webpage to dynamic by deploying Amazon Lightsail. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.
- D. Create a t2.micro Amazon EC2 instance. Deploy a LAMP (Linux, Apache, MySQL, PHP/Perl/Python) stack to host the webpage. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.

Correct Answer: B

Community vote distribution

B (89%)	11%
---------	-----

✉  **obatunde** Highly Voted 9 months, 1 week ago

Selected Answer: B

Correct answer is B. <https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/>

upvoted 6 times

✉  **Guru4Cloud** Most Recent 2 months, 3 weeks ago

Selected Answer: B

B is the most cost-effective solution for this use case.

The key requirements are:

Static website hosted on S3
Add a contact form with server-side processing
Low traffic website (<100 visits per month.)

upvoted 1 times

✉  **rogerHS** 4 months, 3 weeks ago

why not C

upvoted 2 times

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

Option C uses Lightsail which incurs charges even at low usage. Not cost effective for low traffic sites.

upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: B

This solution is the most cost-efficient for the anticipated 100 monthly visits because:

- API Gateway charges are based on API calls. With only 100 visits, charges would be minimal.
- AWS Lambda provides compute time for the backend code in increments of 100ms, so charges would also be negligible for this workload.
- Amazon SES is used only for sending emails from the submitted contact forms. SES has a generous free tier of 62,000 emails per month, so there would be no charges for sending the contact emails.
- No EC2 instances or other infrastructure needs to be run and paid for.

upvoted 3 times

✉  **datz** 7 months, 3 weeks ago

Selected Answer: B

B would be cheaper than option D,

Member only 100 site visits per month, so you are comparing API GW used 100 times a month with constantly running EC2...

upvoted 1 times

✉  **Steve_4542636** 9 months ago

Selected Answer: B

Both api gateway and lambda are serverless so charges apply only on the 100 form submissions per month

upvoted 1 times

✉ **bdp123** 9 months, 1 week ago

Selected Answer: B

After looking at cost of Workmail compared to SES - probably 'B' is better

upvoted 2 times

✉ **bdp123** 9 months, 1 week ago

Selected Answer: D

Create a t2 micro Amazon EC2 instance. Deploy a LAMP (Linux Apache MySQL, PHP/Perl/Python) stack to host the webpage (free open-source). Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail. This solution will provide the company with the necessary components to host the contact form page and integrate it with Amazon WorkMail at the lowest cost. Option A requires the use of Amazon ECS, which is more expensive than EC2, and Option B requires the use of Amazon API Gateway, which is also more expensive than EC2. Option C requires the use of Amazon Lightsail, which is more expensive than EC2.

<https://aws.amazon.com/what-is/lamp-stack/>

upvoted 1 times

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

Option D uses EC2 which has a higher monthly cost than serverless options. LAMP stack adds complexity for a simple contact form.

upvoted 1 times

✉ **SkyZeroZx** 7 months ago

3 million API Gateway == 3,50 USD (EE.UU. Este (Ohio))

Is more cheaper letter B

<https://aws.amazon.com/es/api-gateway/pricing/>

<https://aws.amazon.com/es/lambda/pricing/>

upvoted 1 times

✉ **Palanda** 9 months, 1 week ago

Selected Answer: B

It's B

upvoted 1 times

✉ **LuckyAro** 9 months, 1 week ago

Selected Answer: B

B allows the company to create an API endpoint using AWS Lambda, which is a cost-effective and scalable solution for a contact form with low traffic. The backend can make a call to Amazon SES to send email notifications, which simplifies the process and reduces complexity.

upvoted 1 times

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

it is B : <https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/>

upvoted 3 times

✉ **bdp123** 9 months, 2 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html>

Using AWS Lambda with Amazon API Gateway - AWS Lambda

<https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html>

<https://aws.amazon.com/lambda/faqs/>

AWS Lambda FAQs

<https://aws.amazon.com/lambda/faqs/>

upvoted 1 times

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

Option D uses EC2 which has a higher monthly cost than serverless options. LAMP stack adds complexity for a simple contact form.

upvoted 1 times

A company has a static website that is hosted on Amazon CloudFront in front of Amazon S3. The static website uses a database backend. The company notices that the website does not reflect updates that have been made in the website's Git repository. The company checks the continuous integration and continuous delivery (CI/CD) pipeline between the Git repository and Amazon S3. The company verifies that the webhooks are configured properly and that the CI/CD pipeline is sending messages that indicate successful deployments.

A solutions architect needs to implement a solution that displays the updates on the website.

Which solution will meet these requirements?

- A. Add an Application Load Balancer.
- B. Add Amazon ElastiCache for Redis or Memcached to the database layer of the web application.
- C. Invalidate the CloudFront cache.
- D. Use AWS Certificate Manager (ACM) to validate the website's SSL certificate.

Correct Answer: B

Community vote distribution

C (94%) 6%

 **fulingyu288**  9 months, 2 weeks ago

Selected Answer: C

Invalidate the CloudFront cache: The solutions architect should invalidate the CloudFront cache to ensure that the latest version of the website is being served to users.

upvoted 8 times

 **TariqKipkemei**  1 month, 4 weeks ago

Selected Answer: C

Invalidate the CloudFront cache so that it can read the updated static page from S3.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: C

C. Invalidate the CloudFront cache

upvoted 1 times

 **Damdom** 3 months, 2 weeks ago

C. Invalidate the CloudFront cache.

Explanation:

Invalidate the CloudFront cache to ensure that the latest updates from the Git repository are reflected on the static website. When updates are made to the website's Git repository and deployed to Amazon S3, the CloudFront cache may still be serving the old cached content to users. By invalidating the CloudFront cache, you're instructing CloudFront to fetch fresh content from the origin (Amazon S3) and serve it to users.

upvoted 4 times

 **riccardoto** 3 months, 3 weeks ago

Selected Answer: C

C is the most reasonable cause, though the question is not well-written - "The static website uses a database backend." does not make a lot of sense to me.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: B

Since the static website is hosted behind CloudFront, updates made to the S3 bucket will not be visible on the site until the CloudFront cache expires or is invalidated. By invalidating the CloudFront cache after deploying updates, the latest version in S3 will be pulled and the updates will then appear on the live site.

upvoted 1 times

 **RoroJ** 6 months, 1 week ago

Isn't that C?

upvoted 2 times

 **Namrash** 9 months, 1 week ago

B should be the right one

upvoted 1 times

 **Neorem** 9 months, 2 weeks ago

Selected Answer: C

We need to create an Cloudfront invalidation

upvoted 2 times

 **Bhawesh** 9 months, 2 weeks ago

Selected Answer: C

C. Invalidate the CloudFront cache.

Problem is the CF cache. After invalidating the CloudFront cache, CF will be forced to read the updated static page from the S3 and the S3 changes will start being visible.

upvoted 3 times

A company wants to migrate a Windows-based application from on premises to the AWS Cloud. The application has three tiers: an application tier, a business tier, and a database tier with Microsoft SQL Server. The company wants to use specific features of SQL Server such as native backups and Data Quality Services. The company also needs to share files for processing between the tiers.

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

- A. Host all three tiers on Amazon EC2 instances. Use Amazon FSx File Gateway for file sharing between the tiers.
- B. Host all three tiers on Amazon EC2 instances. Use Amazon FSx for Windows File Server for file sharing between the tiers.
- C. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.
- D. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume for file sharing between the tiers.

Correct Answer: B

Community vote distribution

B (83%)	C (17%)
---------	---------

✉  **KZM**  9 months, 1 week ago

It is B:

A: Incorrect > FSx file Gateway designed for low latency and efficient access to in-cloud FSx for Windows File Server file shares from your on-premises facility.

B: Correct > This solution will allow the company to host all three tiers on Amazon EC2 instances while using Amazon FSx for Windows File Server to provide Windows-based file sharing between the tiers. This will allow the company to use specific features of SQL Server, such as native backups and Data Quality Services, while sharing files for processing between the tiers.

C: Incorrect > Currently, Amazon EFS supports the NFSv4.1 protocol and does not natively support the SMB protocol, and can't be used in Windows instances yet.

D: Incorrect > Amazon EBS is a block-level storage solution that is typically used to store data at the operating system level, rather than for file sharing between servers.

upvoted 12 times

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

Selected Answer: B

B. Host all three tiers on Amazon EC2 instances. Use Amazon FSx for Windows File Server for file sharing between the tiers.

upvoted 1 times

✉  **Abrar2022** 6 months ago

The question mentions Microsoft = windows
EFS is Linux

upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: B

This design satisfies the needs in the following ways:

- Running all tiers on EC2 allows using SQL Server on EC2 with its native features like backups and Data Quality Services. SQL Server cannot be run directly on RDS.
- Amazon FSx for Windows File Server provides fully managed Windows file storage with SMB access. This allows sharing files between the Windows EC2 instances for all three tiers.
- FSx for Windows File Server has high performance, so it can handle file sharing needs between the tiers.

upvoted 1 times

✉  **fageroff** 1 month, 2 weeks ago

IO2 support multi-attach

upvoted 1 times

✉  **kruasan** 7 months ago

The other options would not meet requirements:

- A. FSx File Gateway only provides access to S3 or EFS storage. It cannot be used directly for Windows file sharing.
- C. RDS cannot run SQL Server or its native tools. The database tier needs to run on EC2.
- D. EBS volumes can only be attached to a single EC2 instance. They cannot be shared between tiers for file exchanges.

upvoted 1 times

 **Netgear** 2 months, 1 week ago

No, there is RDS for SQL Server.
<https://aws.amazon.com/rds/sqlserver/>
upvoted 1 times

 **ManOnTheMoon** 9 months, 1 week ago

Why not C?
upvoted 1 times

 **KZM** 9 months, 1 week ago

Currently, Amazon EFS supports the NFSv4.1 protocol and does not natively support the SMB protocol, and can't be used in Windows instances yet.
upvoted 2 times

 **AlmeroSenior** 9 months, 1 week ago

Selected Answer: B

Yup B . RDS will not work , Native Backup only to S3 , and Data Quality is not supported , so all EC2 .
<https://aws.amazon.com/premiumsupport/knowledge-center/native-backup-rds-sql-server/> and <https://www.sqlserver-dba.com/2021/07/aws-rds-sql-server-limitations.html>
upvoted 2 times

 **LuckyAro** 9 months, 1 week ago

After further research, I concur that the correct answer is B. Native Back up and Data Quality not supported on RDS for Ms SQL
upvoted 2 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: C

C.
Host the application tier and the business tier on Amazon EC2 instances.
Host the database tier on Amazon RDS.
Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.

This solution allows the company to use specific features of SQL Server such as native backups and Data Quality Services, by hosting the database tier on Amazon RDS. It also enables file sharing between the tiers using Amazon EFS, which is a fully managed, highly available, and scalable file system. Amazon EFS provides shared access to files across multiple instances, which is important for processing files between the tiers. Additionally, hosting the application and business tiers on Amazon EC2 instances provides the company with the flexibility to configure and manage the environment according to their requirements.

upvoted 2 times

 **rushi0611** 6 months, 3 weeks ago

How are you gonna connect the EFS to windows based ??
upvoted 1 times

 **Yechi** 9 months, 1 week ago

Selected Answer: B

Data Quality Services: If this feature is critical to your workload, consider choosing Amazon RDS Custom or Amazon EC2.
<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-sql-server/comparison.html>
upvoted 3 times

 **Bhawesh** 9 months, 2 weeks ago

Selected Answer: B

Correct Answer: B
upvoted 3 times

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. The company must not make any changes to the application.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 Standard bucket with access to the web servers.
- B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
- C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.
- D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Correct Answer: A

Community vote distribution

C (100%)

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

Selected Answer: C

Since no code change is permitted, below choice makes sense for the unix server's file sharing:

C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.

upvoted 12 times

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

Selected Answer: C

Rehost the application webservers on EC2 and Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: C

Since no code change is permitted, below choice makes sense for the unix server's file sharing:

upvoted 1 times

 **callmejaja** 4 months, 3 weeks ago

Selected Answer: C

Since no code change is permitted, below choice makes sense for the unix server's file sharing:

upvoted 1 times

 **antropaws** 6 months, 1 week ago

Selected Answer: C

C is correct.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: C

This solution satisfies the needs in the following ways:

- EFS provides a fully managed elastic network file system that can be mounted on multiple EC2 instances concurrently.
- The EFS file system appears as a standard file system mount on the Linux web servers, requiring no application changes. The servers can access shared files as if they were on local storage.
- EFS is highly available, durable, and scalable, providing a robust shared storage solution.

upvoted 2 times

 **kruasan** 7 months ago

The other options would require modifying the application or do not provide a standard file system:

- A. S3 does not provide a standard file system mount or share. The application would need to be changed to access S3 storage.
- B. CloudFront is a content delivery network and caching service. It does not provide a file system mount or share and would require application changes.
- D. EBS volumes can only attach to a single EC2 instance. They cannot be mounted by multiple servers concurrently and do not provide a shared file system.

upvoted 2 times

 **Steve_4542636** 9 months ago

Selected Answer: C

No application changes are allowed and EFS is compatible with Linux

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: C

C is the answer:

Create an Amazon Elastic File System (Amazon EFS) file system.

Mount the EFS file system on all web servers.

To meet the requirements of providing a shared file store for Linux-based web servers without making changes to the application, using an Amazon EFS file system is the best solution.

Amazon EFS is a managed NFS file system service that provides shared access to files across multiple Linux-based instances, which makes it suitable for this use case.

Amazon S3 is not ideal for this scenario since it is an object storage service and not a file system, and it requires additional tools or libraries to mount the S3 bucket as a file system.

Amazon CloudFront can be used to improve content delivery performance but is not necessary for this requirement.

Additionally, Amazon EBS volumes can only be mounted to one instance at a time, so it is not suitable for sharing files across multiple instances.
upvoted 2 times

 **Karlos99** 9 months ago

But what about aws ebs multi attach?

upvoted 2 times

 **elearningtakai** 8 months ago

Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple instances. EBS General Purpose SSD (gp3) doesn't support Multi-Attach

upvoted 1 times

A company has an AWS Lambda function that needs read access to an Amazon S3 bucket that is located in the same AWS account.

Which solution will meet these requirements in the MOST secure manner?

- A. Apply an S3 bucket policy that grants read access to the S3 bucket.
- B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket.
- C. Embed an access key and a secret key in the Lambda function's code to grant the required IAM permissions for read access to the S3 bucket.
- D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets in the account.

Correct Answer: D

Community vote distribution

B (100%)

✉  **TMabs** 1 month, 2 weeks ago

Answer=B

upvoted 1 times

✉  **antropaws** 6 months, 1 week ago

Selected Answer: B

B is correct.

upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: B

This solution satisfies the needs in the most secure manner:

- An IAM role provides temporary credentials to the Lambda function to access AWS resources. The function does not have persistent credentials.
- The IAM policy grants least privilege access by specifying read access only to the specific S3 bucket needed. Access is not granted to all S3 buckets.
- If the Lambda function is compromised, the attacker would only gain access to the one specified S3 bucket. They would not receive broad access to resources.

upvoted 2 times

✉  **kruasan** 7 months ago

The other options are less secure:

- A. A bucket policy grants open access to a resource. It is a less granular way to provide access and grants more privilege than needed.
- C. Embedding access keys in code is extremely insecure and against best practices. The keys provide full access and are at major risk of compromise if the code leaks.
- D. Granting access to all S3 buckets provides far too much privilege if only one bucket needs access. It greatly expands the impact if compromised.

upvoted 1 times

✉  **Dr_Chomp** 7 months, 3 weeks ago

Selected Answer: B

you dont want to grant access to all S3 buckets (which is answer D) - only the one identified (so answer A)

upvoted 1 times

✉  **Steve_4542636** 9 months ago

Selected Answer: B

B is only for one bucket and you want to use Role based security here.

upvoted 1 times

✉  **Ja13** 9 months, 1 week ago

Selected Answer: B

C, it says MOST secure manner, so only to one bucket

upvoted 1 times

✉  **Joxtat** 9 months, 1 week ago

Selected Answer: B

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

upvoted 1 times

✉  **kpato87** 9 months, 1 week ago

Selected Answer: B

This is the most secure and recommended way to provide an AWS Lambda function with access to an S3 bucket. It involves creating an IAM role that the Lambda function assumes, and attaching an IAM policy to the role that grants the necessary permissions to read from the S3 bucket.

upvoted 3 times

 **Joan11edu** 9 months, 2 weeks ago

Selected Answer: B

B. Least of privilege

upvoted 2 times

A company hosts a web application on multiple Amazon EC2 instances. The EC2 instances are in an Auto Scaling group that scales in response to user demand. The company wants to optimize cost savings without making a long-term commitment.

Which EC2 instance purchasing option should a solutions architect recommend to meet these requirements?

- A. Dedicated Instances only
- B. On-Demand Instances only
- C. A mix of On-Demand Instances and Spot Instances
- D. A mix of On-Demand Instances and Reserved Instances

Correct Answer: B

Community vote distribution

C (83%) B (17%)

 **beginnercloud** 1 month ago

Selected Answer: C

It's about COST, not operational efficiency for this question :) C is correct
upvoted 1 times

 **TariqKipkemei** 1 month, 3 weeks ago

Selected Answer: C

A mix of On-Demand Instances to handle baseline workload and Spot Instances to handle excess workload.
upvoted 2 times

 **Kt** 2 months, 1 week ago

Exam topic is not free anymore. Anyone has free access ?
upvoted 1 times

 **soewailin** 1 month, 3 weeks ago

for now though, I have still access.
upvoted 1 times

 **Damdom** 3 months, 2 weeks ago

Selected Answer: C

By combining On-Demand Instances for steady-state workloads or critical components and Spot Instances for less critical or burstable workloads, you can achieve a balance between cost savings and performance. This strategy allows you to optimize costs without making a long-term commitment, as Spot Instances provide cost savings without the need for upfront payments or long-term contracts.
upvoted 2 times

 **Abrar2022** 6 months ago

Selected Answer: C

It's about COST, not operational efficiency for this question.
upvoted 2 times

 **kraken21** 8 months ago

Selected Answer: C

Autoscaling with ALB / scale up on demand using on demand and spot instance combination makes sense. Reserved will not fit the no-long term commitment clause.
upvoted 1 times

 **Whericanstart** 8 months, 1 week ago

Selected Answer: C

Without commitment....Spot instances
upvoted 1 times

 **cegama543** 8 months, 2 weeks ago

Selected Answer: B

If the company wants to optimize cost savings without making a long-term commitment, then using only On-Demand Instances may not be the most cost-effective option. Spot Instances can be significantly cheaper than On-Demand Instances, but they come with the risk of being interrupted if the Spot price increases above your bid price. If the company is willing to accept this risk, a mix of On-Demand Instances and Spot Instances may be the best option to optimize cost savings while maintaining the desired level of scalability.

However, if the company wants the most predictable pricing and does not want to risk instance interruption, then using only On-Demand Instances is a good choice. It ultimately depends on the company's priorities and risk tolerance.

upvoted 3 times

✉  **Steve_4542636** 9 months ago

Selected Answer: C

It's about COST, not operational efficiency for this question.

upvoted 1 times

✉  **Samuel03** 9 months, 1 week ago

Selected Answer: C

Should be C

upvoted 1 times

✉  **bdp123** 9 months, 1 week ago

Selected Answer: C

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-mixed-instances-groups.html>

upvoted 1 times

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

Selected Answer: C

C - WEB apps , mostly Stateless , and ASG support OnDemand and Spot mix , in fact , you can prioritize to have Ondemand , before it uses Spot > <https://docs.aws.amazon.com/autoscaling/ec2/userguide/launch-template-spot-instances.html>

upvoted 1 times

✉  **designmood22** 9 months, 1 week ago

Selected Answer: C

Answer : C. A mix of On-Demand Instances and Spot Instances

upvoted 1 times

✉  **LuckyAro** 9 months, 1 week ago

Selected Answer: C

To optimize cost savings without making a long-term commitment, a mix of On-Demand Instances and Spot Instances would be the best EC2 instance purchasing option to recommend.

By combining On-Demand and Spot Instances, the company can take advantage of the cost savings offered by Spot Instances during periods of low demand while maintaining the reliability and stability of On-Demand Instances during periods of high demand. This provides a cost-effective solution that can scale with user demand without making a long-term commitment.

upvoted 1 times

✉  **NolaHolla** 9 months, 1 week ago

In this scenario, a mix of On-Demand Instances and Spot Instances is the most cost-effective option, as it can provide significant cost savings while maintaining application availability. The Auto Scaling group can be configured to launch Spot Instances when the demand is high and On-Demand Instances when demand is low or when Spot Instances are not available. This approach provides a balance between cost savings and reliability.

upvoted 3 times

✉  **minglu** 9 months, 1 week ago

In my opinion, it is C, on demand instances and spot instances can be in a single auto scaling group.

upvoted 3 times

A media company uses Amazon CloudFront for its publicly available streaming video content. The company wants to secure the video content that is hosted in Amazon S3 by controlling who has access. Some of the company's users are using a custom HTTP client that does not support cookies. Some of the company's users are unable to change the hardcoded URLs that they are using for access.

Which services or methods will meet these requirements with the LEAST impact to the users? (Choose two.)

- A. Signed cookies
- B. Signed URLs
- C. AWS AppSync
- D. JSON Web Token (JWT)
- E. AWS Secrets Manager

Correct Answer: CE

Community vote distribution

AB (81%)

Other

✉  **leoatff** Highly Voted 9 months, 1 week ago

Selected Answer: AB

I thought that option A was totally wrong, because the question mentions "HTTP client does not support cookies". However it is right, along with option B. Check the link below, first paragraph.

<https://aws.amazon.com/blogs/media/secure-content-using-cloudfront-functions/>

upvoted 15 times

✉  **Steve_4542636** 9 months ago

Thanks for this! What a tricky question. If the client doesn't support cookies, THEN they use the signed S3 URLs.

upvoted 6 times

✉  **AAAWrekng** 1 month, 1 week ago

LOL, like the old question, in my hand I have 2 coins, and they equal 15 cents, one of them is not a nickel. What are the coins
upvoted 1 times

✉  **johnmcclane78** Highly Voted 8 months, 4 weeks ago

B. Signed URLs - This method allows the media company to control who can access the video content by creating a time-limited URL with a cryptographic signature. This URL can be distributed to the users who are unable to change the hardcoded URLs they are using for access, and they can access the content without needing to support cookies.

D. JSON Web Token (JWT) - This method allows the media company to control who can access the video content by creating a secure token that contains user authentication and authorization information. This token can be distributed to the users who are using a custom HTTP client that does not support cookies. The users can include this token in their requests to access the content without needing to support cookies.

Therefore, options B and D are the correct answers.

Option A (Signed cookies) would not work for users who are using a custom HTTP client that does not support cookies. Option C (AWS AppSync) is not relevant to the requirement of securing video content. Option E (AWS Secrets Manager) is a service used for storing and retrieving secrets, which is not relevant to the requirement of securing video content.

upvoted 14 times

✉  **ONS_KH** 1 month, 1 week ago

This is the response of chatgpt isn't it ? Pay attention ! it doesn't always give the right answer

upvoted 3 times

✉  **prabhjot** Most Recent 1 month, 3 weeks ago

B & E - B. Signed URLs: This allows you to generate time-limited URLs with a signature that grants temporary access to specific resources in your S3 bucket. It doesn't rely on cookies and can be generated for users without requiring any changes to their HTTP client or hardcoded URLs. This method provides fine-grained control over access to your content.

E. AWS Secrets Manager: While AWS Secrets Manager can be useful for managing and rotating secrets, it is not directly related to securing S3 content in the context of the question. It's not one of the primary methods for securing access to S3 objects.

upvoted 1 times

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

Selected Answer: AB

To secure streaming video content from Amazon CloudFront, two methods are available: signed cookies or signed URLs. Customers can choose to use either one or both, depending on the use case.

upvoted 2 times

 **tabbyDolly** 2 months, 1 week ago

AB - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: BD

B and D are the correct options for meeting the requirements with the least impact to users.

Signed URLs allow access to individual objects in Amazon S3 for a specified time period without requiring cookies. This allows the custom HTTP client users to access content.

JSON Web Tokens (JWT) allow users to get temporary access tokens that can be passed in requests. This allows users with hardcoded URLs to access content without updating URLs.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

No good

Signed cookies require client support and may impact users.

AWS AppSync and Secrets Manager do not help address the specific access requirements.

Good

So Signed URLs and JWTs allow securing access to S3 content with minimal impact to users, meeting the requirements.

upvoted 1 times

 **riccardoto** 3 months, 3 weeks ago

Selected Answer: BD

I understand why many users here are voting AB, but in my opinion BD is more correct.

Using JWT or signed urls will work both for users that cannot use cookies or cannot change the url.

upvoted 1 times

 **katetel** 4 months, 1 week ago

Selected Answer: AB

it's correct

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: CE

These are the right answers!

upvoted 2 times

 **DrWatson** 5 months, 4 weeks ago

Selected Answer: AB

"Some of the company's users" does not support cookies, then they'll use Signed URLs.

"Some of the company's users" are unable to change the hardcoded URLs, then they'll use Signed cookies.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: AB

Signed cookies would allow the media company to authorize access to related content (like HLS video segments) with a single signature, minimizing implementation overhead. This works for users that can support cookies.

Signed URLs would allow the media company to sign each URL individually to control access, supporting users that cannot use cookies. By embedding the signature in the URL, existing hardcoded URLs would not need to change.

upvoted 2 times

 **kruasan** 7 months ago

C. AWS AppSync - This is for building data-driven apps with real-time and offline capabilities. It does not directly help with securing streaming content.

D. JSON Web Token (JWT) - Although JWTs can be used for authorization, they would require the client to get a token and validate/check access on the server for each request. This does not work for hardcoded URLs and minimizes impact.

E. AWS Secrets Manager - This service is for managing secrets, not for controlling access to resources. It would not meet the requirements.

upvoted 1 times

 **Shrestwt** 7 months, 2 weeks ago

A. Signed cookies: CloudFront signed cookies allow you to control who can access your content when you don't want to change your current URLs. <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html>

B. Signed URLs: This method allows the media company to control who can access the video content by creating a time-limited URL with a cryptographic signature.

upvoted 1 times

 **ahilan26** 7 months, 3 weeks ago

Selected Answer: AB

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html>
upvoted 2 times

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

Some of the company's users are using a custom HTTP client that does not support cookies.
**Signed URLs

Some of the company's users are unable to change the hardcoded URLs that they are using for access. **Signed cookies
upvoted 5 times

✉ **TungPham** 9 months ago

Selected Answer: BD

<https://aws.amazon.com/vi/blogs/media/awse-protecting-your-media-assets-with-token-authentication/>
JSON Web Token (JWT) need using with Lambda@Edge

upvoted 3 times

✉ **HaineHess** 9 months ago

Selected Answer: BD

b d seems good
upvoted 1 times

✉ **bdp123** 9 months, 1 week ago

Selected Answer: AB

It says some use a custom HTTP client that does not support cookies - those will use signed URLs which has precedence over cookies
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html>
upvoted 1 times

✉ **FF0** 7 months, 2 weeks ago

AB is wrong, your point that cookies are disabled eliminates the use of signed cookies. The hard coding eliminates the use of signed URLs. so AB totally eliminated. read the article further not just the first few lines, the read up signed URLs

upvoted 1 times

A company is preparing a new data platform that will ingest real-time streaming data from multiple sources. The company needs to transform the data before writing the data to Amazon S3. The company needs the ability to use SQL to query the transformed data.

Which solutions will meet these requirements? (Choose two.)

- A. Use Amazon Kinesis Data Streams to stream the data. Use Amazon Kinesis Data Analytics to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
- B. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use AWS Glue to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
- C. Use AWS Database Migration Service (AWS DMS) to ingest the data. Use Amazon EMR to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
- D. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use Amazon Kinesis Data Analytics to transform the data and to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.
- E. Use Amazon Kinesis Data Streams to stream the data. Use AWS Glue to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.

Correct Answer: AB

Community vote distribution

AB (87%) 13%

✉  **Steve_4542636**  9 months ago

Selected Answer: AB

OK, for B I did some research, <https://docs.aws.amazon.com/glue/latest/dg/add-job-streaming.html>

"You can create streaming extract, transform, and load (ETL) jobs that run continuously, consume data from streaming sources like Amazon Kinesis Data Streams, Apache Kafka, and Amazon Managed Streaming for Apache Kafka (Amazon MSK). The jobs cleanse and transform the data, and then load the results into Amazon S3 data lakes or JDBC data stores."

upvoted 10 times

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

Selected Answer: AB

options A and B will meet these requirements.

upvoted 1 times

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

Selected Answer: AB

A and B are correct.

A uses Kinesis Data Streams for streaming, Kinesis Data Analytics for transformation, Kinesis Data Firehose for writing to S3, and Athena for SQL queries on S3 data.

B uses Amazon MSK for streaming, AWS Glue for transformation and writing to S3, and Athena for SQL queries on S3 data.

upvoted 1 times

✉  **Diqian** 3 months, 1 week ago

Why E is incorrect?

upvoted 2 times

✉  **MrCloudy** 7 months, 1 week ago

Selected Answer: AE

To transform real-time streaming data from multiple sources, write it to Amazon S3, and query the transformed data using SQL, the company can use the following solutions: Amazon Kinesis Data Streams, Amazon Kinesis Data Analytics, and Amazon Kinesis Data Firehose. The transformed data can be queried using Amazon Athena. Therefore, options A and E are the correct answers.

Option A is correct because it uses Amazon Kinesis Data Streams to stream data from multiple sources, Amazon Kinesis Data Analytics to transform the data, and Amazon Kinesis Data Firehose to write the data to Amazon S3. Amazon Athena can be used to query the transformed data in Amazon S3.

Option E is also correct because it uses Amazon Kinesis Data Streams to stream data from multiple sources, AWS Glue to transform the data, and Amazon Kinesis Data Firehose to write the data to Amazon S3. Amazon Athena can be used to query the transformed data in Amazon S3.

upvoted 3 times

 **sand444** 2 months ago

Amazon Athena is not in option E
upvoted 3 times

 **Paras043** 7 months, 3 weeks ago

But how can you transform data using kinesis data analytics ??
upvoted 2 times

 **luisgu** 6 months, 3 weeks ago

See <https://aws.amazon.com/kinesis/data-analytics/faqs/?nc=sn&loc=6>
upvoted 1 times

 **kraken21** 8 months ago

Selected Answer: AB

DMS can move data from DBs to streaming services and cannot natively handle streaming data. Hence A.B makes sense. Also AWS Glue/ETL can handle MSK streaming <https://docs.aws.amazon.com/glue/latest/dg/add-job-streaming.html>.
upvoted 2 times

 **elearningtakai** 8 months ago

Selected Answer: AB

The solutions that meet the requirements of streaming real-time data, transforming the data before writing to S3, and querying the transformed data using SQL are A and B.

Option C: This option is not ideal for streaming real-time data as AWS DMS is not optimized for real-time data ingestion.

Option D & E: These options are not recommended as the Amazon RDS query editor is not designed for querying data in S3, and it is not efficient for running complex queries.

upvoted 4 times

 **gold4otas** 8 months ago

Selected Answer: AB

The correct answers are options A & B
upvoted 1 times

 **TungPham** 9 months ago

may Amazon RDS query editor to query the transformed data from Amazon S3 ?
i don't think so, plz get link docs to that
upvoted 1 times

 **ManOnTheMoon** 9 months, 1 week ago

Why not A & D?
upvoted 1 times

 **TungPham** 9 months ago

may Amazon RDS query editor to query the transformed data from Amazon S3 ?
i don't think so, plz get link docs to that
upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: AB
A and B
upvoted 1 times

 **designmood22** 9 months, 1 week ago

Answer is : A & B
upvoted 1 times

 **rrharris** 9 months, 1 week ago

Answer is A and B
upvoted 2 times

 **NolaHolla** 9 months, 1 week ago

A and B
upvoted 2 times

A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.

Which solution meets these requirements?

- A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
- B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
- C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.
- D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Correct Answer: D

Community vote distribution

D (100%)

 **Steve_4542636** Highly Voted 9 months ago

Selected Answer: D

The question states, "wants to maintain local access to all the data" This is storage gateway. Cached gateway stores only the frequently accessed data locally which is not what the problem statement asks for.

upvoted 8 times

 **kruasan** Highly Voted 7 months ago

Selected Answer: D

1. The company wants to maintain local access to all the data. Only stored volumes keep the complete dataset on-premises, providing low-latency access. Cached volumes only cache a subset locally.
2. The company wants the data backed up on AWS. With stored volumes, periodic backups (snapshots) of the on-premises data are sent to S3, providing durable and scalable backup storage.
3. The company wants the data transfer to AWS to be automatic and secure. Storage Gateway provides an encrypted connection between the on-premises gateway and AWS storage. Backups to S3 are sent asynchronously and automatically based on the backup schedule configured.

upvoted 6 times

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

Selected Answer: D

The Volume Gateway runs in either a cached or stored mode.

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access. In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

<https://aws.amazon.com/storagegateway/faqs/#:~:text=What%20is%20Volume%20Gateway%3F>

upvoted 3 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: D

@kruasan well explained

upvoted 1 times

 **ChrisG1454** 9 months, 1 week ago

Ans = D

<https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html>

upvoted 3 times

 **Neha999** 9 months, 1 week ago

D

<https://www.examtopics.com/discussions/amazon/view/43725-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **bpd123** 9 months, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/storagegateway/faqs/#:~:text=In%20the%20cached%20mode%2C%20your,asynchronously%20backed%20up%20to%20AWS>.

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access. In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

upvoted 2 times

Question #294

Topic 1

An application that is hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Traffic must not traverse the internet.

How should a solutions architect configure access to meet these requirements?

- A. Create a private hosted zone by using Amazon Route 53.
- B. Set up a gateway VPC endpoint for Amazon S3 in the VPC.
- C. Configure the EC2 instances to use a NAT gateway to access the S3 bucket.
- D. Establish an AWS Site-to-Site VPN connection between the VPC and the S3 bucket.

Correct Answer: B

Community vote distribution

B (100%)

 **TariqKipkemei** 1 month, 3 weeks ago

Selected Answer: B

Set up a gateway VPC endpoint for Amazon S3 in the VPC.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

The correct answer is B. Set up a gateway VPC endpoint for Amazon S3 in the VPC.

A gateway VPC endpoint is a private way for Amazon EC2 instances in a VPC to access AWS services, such as Amazon S3, without having to go through the internet. This can help to improve security and performance.

upvoted 2 times

 **Steve_4542636** 9 months ago

Selected Answer: B

S3 and DynamoDB are the only services with Gateway endpoint options

upvoted 2 times

 **ManOnTheMoon** 9 months, 1 week ago

Agree with B

upvoted 1 times

 **jennyka76** 9 months, 1 week ago

ANSWER - B

<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html> B

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

 **skiwili** 9 months, 1 week ago

Selected Answer: B

Bbbbbbbb

upvoted 3 times

An ecommerce company stores terabytes of customer data in the AWS Cloud. The data contains personally identifiable information (PII). The company wants to use the data in three applications. Only one of the applications needs to process the PII. The PII must be removed before the other two applications process the data.

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

- A. Store the data in an Amazon DynamoDB table. Create a proxy application layer to intercept and process the data that each application requests.
- B. Store the data in an Amazon S3 bucket. Process and transform the data by using S3 Object Lambda before returning the data to the requesting application.
- C. Process the data and store the transformed data in three separate Amazon S3 buckets so that each application has its own custom dataset. Point each application to its respective S3 bucket.
- D. Process the data and store the transformed data in three separate Amazon DynamoDB tables so that each application has its own custom dataset. Point each application to its respective DynamoDB table.

Correct Answer: B

Community vote distribution

B (84%) Other

 **fruto123** Highly Voted 9 months, 1 week ago

Selected Answer: B

B is the right answer and the proof is in this link.

<https://aws.amazon.com/blogs/aws/introducing-amazon-s3-object-lambda-use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/>
upvoted 10 times

 **Guru4Cloud** 2 months, 3 weeks ago

This is so wrong
upvoted 1 times

 **Steve_4542636** Highly Voted 9 months ago

Selected Answer: B

Actually this is what Macie is best used for.
upvoted 9 times

 **rvca231** Most Recent 1 month ago

Selected Answer: C

Why would you reprocess the data every time you request it when you can just filter it once and be done?
Because of this I think A and B are highly inefficient, leaving us with C and D as options.
Since S3 is better suited for Data Lakes, I think C is the answer.
upvoted 2 times

 **Abrar2022** 6 months ago

Selected Answer: B

Store the data in an Amazon S3 bucket and using S3 Object Lambda to process and transform the data before returning it to the requesting application. This approach allows the PII to be removed in real-time and without the need to create separate datasets or tables for each application.
upvoted 1 times

 **antropaws** 6 months, 1 week ago

Selected Answer: A

@fruto123 and everyone that upvoted:

Is it plausible that S3 Object Lambda can process terabytes of data in 60 seconds? The same link you shared states that the maximum duration for a Lambda function used by S3 Object Lambda is 60 seconds.

Answer is A.
upvoted 2 times

 **antropaws** 6 months, 1 week ago

Chat GPT:

Isn't just 60 seconds the maximum duration for a Lambda function used by S3 Object Lambda? How can it process terabytes of data in 60 seconds?

You are correct that the maximum duration for a Lambda function used by S3 Object Lambda is 60 seconds.

Given the time constraint, it is not feasible to process terabytes of data within a single Lambda function execution.

S3 Object Lambda is designed for lightweight and real-time transformations rather than extensive processing of large datasets.

To handle terabytes of data, you would typically need to implement a distributed processing solution using services like Amazon EMR, AWS Glue, or AWS Batch. These services are specifically designed to handle big data workloads and provide scalability and distributed processing capabilities.

So, while S3 Object Lambda can be useful for lightweight processing tasks, it is not the appropriate tool for processing terabytes of data within the execution time limits of a Lambda function.

upvoted 2 times

 **Kp88** 4 months ago

Terabyte is just the storage. Lambda only need to process which application request. Think like removing/scratching off your social security number before sharing your doc to a third party.

upvoted 2 times

 **kruasan** 7 months ago

Selected Answer: B

- Storing the raw data in S3 provides a durable, scalable data lake. S3 requires little ongoing management overhead.
- S3 Object Lambda can be used to filter and process the data on retrieval transparently. This minimizes operational overhead by avoiding the need to preprocess and store multiple transformed copies of the data.
- Only one copy of the data needs to be stored and maintained in S3. S3 Object Lambda will transform the data on read based on the requesting application.
- No additional applications or proxies need to be developed and managed to handle the data transformation. S3 Object Lambda provides this functionality.

upvoted 2 times

 **kruasan** 7 months ago

Option A requires developing and managing a proxy app layer to handle data transformation, adding overhead.

Options C and D require preprocessing and storing multiple copies of the transformed data, adding storage and management overhead.

Option B using S3 Object Lambda minimizes operational overhead by handling data transformation on read transparently using the native S3 functionality. Only one raw data copy is stored in S3, with no additional applications required.

upvoted 1 times

 **pagom** 9 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/ko/blogs/korea/introducing-amazon-s3-object-lambda-use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/>

upvoted 4 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: B

B is the correct answer.

Amazon S3 Object Lambda allows you to add custom code to S3 GET requests, which means that you can modify the data before it is returned to the requesting application. In this case, you can use S3 Object Lambda to remove the PII before the data is returned to the two applications that do not need to process PII. This approach has the least operational overhead because it does not require creating separate datasets or proxy application layers, and it allows you to maintain a single copy of the data in an S3 bucket.

upvoted 4 times

 **NolaHolla** 9 months, 1 week ago

To meet the requirement of removing the PII before processing by two of the applications, it would be most efficient to use option B, which involves storing the data in an Amazon S3 bucket and using S3 Object Lambda to process and transform the data before returning it to the requesting application. This approach allows the PII to be removed in real-time and without the need to create separate datasets or tables for each application. S3 Object Lambda can be configured to automatically remove PII from the data before it is sent to the non-PII processing applications. This solution provides a cost-effective and scalable way to meet the requirement with the least operational overhead.

upvoted 2 times

 **minglu** 9 months, 1 week ago

Selected Answer: B

I think it is B.

upvoted 1 times

 **skiwili** 9 months, 1 week ago

Selected Answer: C

Looks like C is the correct answer

upvoted 2 times

A development team has launched a new application that is hosted on Amazon EC2 instances inside a development VPC. A solutions architect needs to create a new VPC in the same account. The new VPC will be peered with the development VPC. The VPC CIDR block for the development VPC is 192.168.0.0/24. The solutions architect needs to create a CIDR block for the new VPC. The CIDR block must be valid for a VPC peering connection to the development VPC.

What is the SMALLEST CIDR block that meets these requirements?

- A. 10.0.1.0/32
- B. 192.168.0.0/24
- C. 192.168.1.0/32
- D. 10.0.1.0/24

Correct Answer: B

Community vote distribution

D (100%)

 **BrainOBrain**  9 months, 1 week ago

Selected Answer: D

10.0.1.0/32 and 192.168.1.0/32 are too small for VPC, and /32 network is only 1 host
192.168.0.0/24 is overlapping with existing VPC
upvoted 13 times

 **Guru4Cloud**  2 months, 3 weeks ago

Selected Answer: D

10.0.1.0/32 and 192.168.1.0/32 are too small for VPC, and /32 network is only 1 host
192.168.0.0/24 is overlapping with existing VPC
upvoted 1 times

 **Abrar2022** 6 months ago

Definitely D. The only valid VPC CIDR block that does not overlap with the development VPC CIDR block among the options. The other 2 CIDR block options are too small.

upvoted 1 times

 **antropaws** 6 months, 1 week ago

Selected Answer: D

D is correct.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: D

- Option A (10.0.1.0/32) is invalid - a /32 CIDR prefix is a host route, not a VPC range.
- Option B (192.168.0.0/24) overlaps the development VPC and so cannot be used.
- Option C (192.168.1.0/32) is invalid - a /32 CIDR prefix is a host route, not a VPC range.
- Option D (10.0.1.0/24) satisfies the non-overlapping CIDR requirement but is a larger block than needed. Since only two VPCs need to be peered, a /24 block provides more addresses than necessary.

upvoted 3 times

 **channn** 8 months ago

Selected Answer: D

D is the only correct answer

upvoted 1 times

 **r04dB10ck** 8 months, 1 week ago

Selected Answer: D

only one valid with no overlap

upvoted 1 times

 **Steve_4542636** 9 months ago

Selected Answer: D

A process by elimination solution here. a CIDR value is the number of bits that are locked so 10.0.0.0/32 means no range.

upvoted 3 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: D

Answer is D, 10.0.1.0/24.

upvoted 1 times

 **skiwili** 9 months, 1 week ago

Selected Answer: D

Yes D is the answer

upvoted 1 times

 **obatunde** 9 months, 1 week ago

Selected Answer: D

Definitely D. It is the only valid VPC CIDR block that does not overlap with the development VPC CIDR block among the options.

upvoted 1 times

 **bdp123** 9 months, 2 weeks ago

Selected Answer: D

The allowed block size is between a /28 netmask and /16 netmask.

The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.

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

upvoted 4 times

A company deploys an application on five Amazon EC2 instances. An Application Load Balancer (ALB) distributes traffic to the instances by using a target group. The average CPU usage on each of the instances is below 10% most of the time, with occasional surges to 65%.

A solutions architect needs to implement a solution to automate the scalability of the application. The solution must optimize the cost of the architecture and must ensure that the application has enough CPU resources when surges occur.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm that enters the ALARM state when the CPUUtilization metric is less than 20%. Create an AWS Lambda function that the CloudWatch alarm invokes to terminate one of the EC2 instances in the ALB target group.
- B. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set a target tracking scaling policy that is based on the ASGAverageCPUUtilization metric. Set the minimum instances to 2, the desired capacity to 3, the maximum instances to 6, and the target value to 50%. Add the EC2 instances to the Auto Scaling group.
- C. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set the minimum instances to 2, the desired capacity to 3, and the maximum instances to 6. Add the EC2 instances to the Auto Scaling group.
- D. Create two Amazon CloudWatch alarms. Configure the first CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is below 20%. Configure the second CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is above 50%. Configure the alarms to publish to an Amazon Simple Notification Service (Amazon SNS) topic to send an email message. After receiving the message, log in to decrease or increase the number of EC2 instances that are running.

Correct Answer: D

Community vote distribution

B (94%)	6%
---------	----

 **bdp123** Highly Voted 9 months, 2 weeks ago

Selected Answer: B

Just create an auto scaling policy
upvoted 9 times

 **vilagiri** Most Recent 2 months ago

I picked B.. I am not 100% sure..The application is deployed in 5 instances initially. What is the logic behind 2/3/6 ASG. Because utilization is 10%, we can set min 2? I know for sure I am not going to get this ASG question correct in the exam.
upvoted 2 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

The correct answer is B.

This solution will meet the requirements because it will:

Automate the scalability of the application by using EC2 Auto Scaling.

Optimize the cost of the architecture by only scaling the number of EC2 instances up when needed.

Ensure that the application has enough CPU resources when surges occur by setting the target value of the target tracking scaling policy to 50%.
upvoted 1 times

 **ajchi1980** 5 months ago

Wrong answers: Options A, C, and D are not the most appropriate solutions:

Option A suggests creating a CloudWatch alarm to terminate an EC2 instance when CPU utilization is less than 20%. However, this approach does not ensure that the application will have enough CPU resources during surges, as it only terminates instances when CPU utilization is low, which may not meet the requirements.

Option C suggests creating an Auto Scaling group without any specific scaling policies or configurations. This approach does not address the need for automated scaling based on CPU utilization, making it insufficient for the given requirements.

Option D suggests using CloudWatch alarms to send notifications via Amazon SNS and manually adjusting the number of instances based on the received messages. This approach lacks automation and requires manual intervention, which does not optimize cost or meet the requirement of automated scalability.

Therefore, Option B is the most appropriate solution in this case.

upvoted 2 times

 **ajchi1980** 5 months ago

Selected Answer: B

Explanation:

Option B leverages EC2 Auto Scaling, which is designed to automatically adjust the number of instances based on specified metrics. By setting a target tracking scaling policy based on average CPU utilization, the Auto Scaling group can dynamically scale the number of instances to maintain the desired level of CPU resources. The minimum instances of 2 ensure a minimum baseline capacity, while the desired capacity of 3 ensures at least three instances are running even during normal traffic. The maximum instances of 6 cap the upper limit to control costs.

upvoted 2 times

✉️ **RoroJ** 6 months, 1 week ago

Selected Answer: D

Auto Scaling group must have an AMI for it.

upvoted 1 times

✉️ **th3k33n** 6 months, 2 weeks ago

how can we set max to 6 since the company is using 5 ec2 instance

upvoted 1 times

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

In the scenario you provided, you're setting up an Auto Scaling group to manage the instances for you, and the settings (min 2, desired 3, max 6) are for the Auto Scaling group, not for your existing instances. When you integrate the instances into the Auto Scaling group, you are effectively moving from a fixed instance count to a dynamic one that can range from 2 to 6 based on the demand.

The existing 5 instances can be included in the Auto Scaling group, but the group can reduce the number of instances if the load is low (to the minimum specified, which is 2 in this case) and can also add more instances (up to a maximum of 6) if the load increases.

upvoted 1 times

✉️ **kruasan** 7 months ago

Selected Answer: B

Reasons:

- An Auto Scaling group will automatically scale the EC2 instances to match changes in demand. This optimizes cost by only running as many instances as needed.
- A target tracking scaling policy monitors the ASGAverageCPUUtilization metric and scales to keep the average CPU around the 50% target value. This ensures there are enough resources during CPU surges.
- The ALB and target group are reused, so the application architecture does not change. The Auto Scaling group is associated to the existing load balancer setup.
- A minimum of 2 and maximum of 6 instances provides the ability to scale between 3 and 6 instances as needed based on demand.
- Costs are optimized by starting with only 3 instances (the desired capacity) and scaling up as needed. When CPU usage drops, instances are terminated to match the desired capacity.

upvoted 2 times

✉️ **kruasan** 7 months ago

Option A - terminates instances reactively based on low CPU and may not provide enough capacity during surges. Does not optimize cost.
Option C - lacks a scaling policy so will not automatically adjust capacity based on changes in demand. Does not ensure enough resources during surges.

Option D - requires manual intervention to scale capacity. Does not optimize cost or provide an automated solution.

upvoted 1 times

✉️ **darn** 7 months, 1 week ago

as you dig down the question, they get more and more bogus with less and less votes

upvoted 1 times

✉️ **Steve_4542636** 9 months ago

Selected Answer: B

B is my vote

upvoted 1 times

✉️ **KZM** 9 months, 1 week ago

Based on the information given, the best solution is option "B".

Autoscaling group with target tracking scaling policy with min 2 instances, desired capacity to 3, and the maximum instances to 6.

upvoted 1 times

✉️ **Shrestwt** 7 months, 2 weeks ago

But the company is using only 5 EC2 Instances so how can we set maximum instance to 6.

upvoted 2 times

✉️ **LuckyAro** 9 months, 1 week ago

Selected Answer: B

B is the correct solution because it allows for automatic scaling based on the average CPU utilization of the EC2 instances in the target group. With the use of a target tracking scaling policy based on the ASGAverageCPUUtilization metric, the EC2 Auto Scaling group can ensure that the target value of 50% is maintained while scaling the number of instances in the group up or down as needed. This will help ensure that the application has enough CPU resources during surges without overprovisioning, thus optimizing the cost of the architecture.

upvoted 1 times

✉️ **Babba** 9 months, 1 week ago

Selected Answer: B

Should be B

upvoted 1 times

A company is running a critical business application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances run in an Auto Scaling group and access an Amazon RDS DB instance.

The design did not pass an operational review because the EC2 instances and the DB instance are all located in a single Availability Zone. A solutions architect must update the design to use a second Availability Zone.

Which solution will make the application highly available?

- A. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
- B. Provision two subnets that extend across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
- C. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.
- D. Provision a subnet that extends across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.

Correct Answer: D

Community vote distribution

C (100%)

 **bdp123** Highly Voted 9 months, 2 weeks ago

Selected Answer: C

A subnet must reside within a single Availability Zone.

<https://aws.amazon.com/vpc/faqs/#:~:text=Can%20a%20subnet%20span%20Availability,within%20a%20single%20Availability%20Zone>.

upvoted 11 times

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

Selected Answer: C

Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: C

This solution will ensure that the EC2 instances and the DB instance are not located in the same Availability Zone, which will improve the availability of the application.

upvoted 1 times

 **zjcorpuz** 4 months ago

a subnet only resides on a one AZ, it does not span to another AZ.

upvoted 3 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: C

D is completely wrong, because each subnet must reside entirely within one Availability Zone and cannot span zones. By launching AWS resources in separate Availability Zones, you can protect your applications from the failure of a single Availability Zone.

upvoted 1 times

 **Anmol_1010** 5 months, 2 weeks ago

The key word here was extend.

upvoted 1 times

 **GalileoEC2** 8 months, 2 weeks ago

This discards B and D: Subnet basics. Each subnet must reside entirely within one Availability Zone and cannot span zones. By launching AWS resources in separate Availability Zones, you can protect your applications from the failure of a single Availability Zone

upvoted 2 times

 **Steve_4542636** 9 months ago

Selected Answer: C

a subnet is per AZ. a scaling group can span multiple AZs. <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

upvoted 1 times

✉ **KZM** 9 months, 1 week ago

I think D.

Span the single subnet in both Availability Zones can access the DB instances in either zone without going over the public internet.

upvoted 2 times

✉ **KZM** 9 months, 1 week ago

Can span like that?

upvoted 1 times

✉ **leoattf** 9 months, 1 week ago

Nope. The answer is indeed C.

You cannot span like that. Check the link below:

"Each subnet must reside entirely within one Availability Zone and cannot span zones."

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

upvoted 3 times

✉ **KZM** 9 months, 1 week ago

Thanks, Leoattf for the link you shared.

upvoted 2 times

✉ **KZM** 9 months, 1 week ago

Sorry I think C is correct.

upvoted 1 times

✉ **Babba** 9 months, 1 week ago

Selected Answer: C

it's C

upvoted 1 times

A research laboratory needs to process approximately 8 TB of data. The laboratory requires sub-millisecond latencies and a minimum throughput of 6 GBps for the storage subsystem. Hundreds of Amazon EC2 instances that run Amazon Linux will distribute and process the data.

Which solution will meet the performance requirements?

- A. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to ALL. Import the raw data into the file system. Mount the file system on the EC2 instances.
- B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
- C. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent HDD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
- D. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to NONE. Import the raw data into the file system. Mount the file system on the EC2 instances.

Correct Answer: D

Community vote distribution

B (100%)

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

Selected Answer: B

Keyword here is a minimum throughput of 6 GBps. Only the FSx for Lustre with SSD option gives the sub-milli response and throughput of 6 GBps or more.

B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.

References:

<https://aws.amazon.com/fsx/when-to-choose-fsx/>

upvoted 11 times

 **bdp123** Highly Voted 9 months, 2 weeks ago

Selected Answer: B

Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances. Amazon FSx for Lustre uses SSD storage for submillisecond latencies and up to 6 GBps throughput, and can import data from and export data to Amazon S3. Additionally, the option to select persistent SSD storage will ensure that the data is stored on the disk and not lost if the file system is stopped.

upvoted 6 times

 **Guru4Cloud** Most Recent 2 months, 3 weeks ago

Selected Answer: B

Amazon FSx for Lustre with SSD: Amazon FSx for Lustre is designed for high-performance, parallel file processing workloads. Choosing SSD storage ensures fast I/O and meets the sub-millisecond latency requirement.

upvoted 1 times

 **rolervengador** 3 months ago

Voto por la B

upvoted 1 times

 **Gooniegoogoo** 5 months ago

So many of these are wrong, its good we have people that vote so we can get to the right answer!!

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: B

- Amazon FSx for Lustre with SSD storage can provide up to 260 GB/s of aggregate throughput and sub-millisecond latencies needed for this workload.
- Persistent SSD storage ensures data durability in the file system. Data is also exported to S3 for backup storage.
- The file system will import the initial 8 TB of raw data from S3, providing a fast storage tier for processing while retaining the data in S3.
- The file system is mounted to the EC2 compute instances to distribute processing.
- FSx for Lustre is optimized for high-performance computing workloads running on Linux, matching the EC2 environment.

upvoted 1 times

 **kruasan** 7 months ago

Option A - FSx for NetApp ONTAP with ALL tiering policy would not provide fast enough storage tier for sub-millisecond latency. HDD tiers have higher latency.

Option C - FSx for Lustre with HDD storage would not provide the throughput, IOPS or low latency needed.

Option D - FSx for NetApp ONTAP with NONE tiering policy would require much more expensive SSD storage to meet requirements, increasing cost.

upvoted 1 times

 **Steve_4542636** 9 months ago

Selected Answer: B

I vote B

upvoted 1 times

 **AlmeroSenior** 9 months, 1 week ago

Selected Answer: B

FSX Lustre is 1000mbps per TB provisioned and we have 8TBs so gives us 8GBs . The netapp FSX appears a hard limit of 4gbps .

<https://aws.amazon.com/fsx/lustre/faqs/?nc=sn&loc=5>

<https://aws.amazon.com/fsx/netapp-ontap/faqs/>

upvoted 4 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: B

B is the best choice as it utilizes Amazon S3 for data storage, which is cost-effective and durable, and Amazon FSx for Lustre for high-performance file storage, which provides the required sub-millisecond latencies and minimum throughput of 6 GBps. Additionally, the option to import and export data to and from Amazon S3 makes it easier to manage and move data between the two services.

B is the best option as it meets the performance requirements for sub-millisecond latencies and a minimum throughput of 6 GBps.

upvoted 1 times

 **everfly** 9 months, 1 week ago

Selected Answer: B

Amazon FSx for Lustre provides fully managed shared storage with the scalability and performance of the popular Lustre file system. It can deliver sub-millisecond latencies and hundreds of gigabytes per second of throughput.

upvoted 3 times

A company needs to migrate a legacy application from an on-premises data center to the AWS Cloud because of hardware capacity constraints. The application runs 24 hours a day, 7 days a week. The application's database storage continues to grow over time.

What should a solutions architect do to meet these requirements MOST cost-effectively?

- A. Migrate the application layer to Amazon EC2 Spot Instances. Migrate the data storage layer to Amazon S3.
- B. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon RDS On-Demand Instances.
- C. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon Aurora Reserved Instances.
- D. Migrate the application layer to Amazon EC2 On-Demand Instances. Migrate the data storage layer to Amazon RDS Reserved Instances.

Correct Answer: C

Community vote distribution

C (83%)

B (17%)

✉  **LuckyAro**  9 months, 1 week ago

Selected Answer: C

Amazon EC2 Reserved Instances allow for significant cost savings compared to On-Demand instances for long-running, steady-state workloads like this one. Reserved Instances provide a capacity reservation, so the instances are guaranteed to be available for the duration of the reservation period.

Amazon Aurora is a highly scalable, cloud-native relational database service that is designed to be compatible with MySQL and PostgreSQL. It can automatically scale up to meet growing storage requirements, so it can accommodate the application's database storage needs over time. By using Reserved Instances for Aurora, the cost savings will be significant over the long term.

upvoted 12 times

✉  **NolaHola**  9 months, 1 week ago

Option B based on the fact that the DB storage will continue to grow, so on-demand will be a more suitable solution
upvoted 10 times

✉  **NolaHola** 9 months, 1 week ago

Since the application's database storage is continuously growing over time, it may be difficult to estimate the appropriate size of the Aurora cluster in advance, which is required when reserving Aurora.

In this case, it may be more cost-effective to use Amazon RDS On-Demand Instances for the data storage layer. With RDS On-Demand Instances, you pay only for the capacity you use and you can easily scale up or down the storage as needed.

upvoted 5 times

✉  **hristni0** 6 months ago

Answer is C. From Aurora Reserved Instances documentation:

If you have a DB instance, and you need to scale it to larger capacity, your reserved DB instance is automatically applied to your scaled DB instance. That is, your reserved DB instances are automatically applied across all DB instance class sizes. Size-flexible reserved DB instances are available for DB instances with the same AWS Region and database engine.

upvoted 1 times

✉  **Joxtat** 9 months, 1 week ago

The Answer is C.

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

upvoted 1 times

✉  **cciesam**  3 weeks, 3 days ago

Selected Answer: B

I hope it should be B considering Database growth

upvoted 1 times

✉  **Wayne23Fang** 2 months, 1 week ago

My research concludes that From pure price point of view Aurora Reserved might/ usually be slightly more expensive than On-demand RDS. But RDS has less Operation overhead. For the 24x7 nature, I would vote C. But for pure cost-effective, B is less costly.

upvoted 1 times

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

Selected Answer: C

This option involves migrating the application layer to Amazon EC2 Reserved Instances and migrating the data storage layer to Amazon Aurora Reserved Instances. Amazon EC2 Reserved Instances provide a significant discount (up to 75%) compared to On-Demand Instance pricing, making them a cost-effective choice for applications that have steady state or predictable usage. Similarly, Amazon Aurora Reserved Instances provide a significant discount (up to 69%) compared to On-Demand Instance pricing.

upvoted 1 times

ajchi1980 5 months ago

Selected Answer: C

To meet the requirements of migrating a legacy application from an on-premises data center to the AWS Cloud in a cost-effective manner, the most suitable option would be:

C. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon Aurora Reserved Instances.

Explanation:

Migrating the application layer to Amazon EC2 Reserved Instances allows you to reserve EC2 capacity in advance, providing cost savings compared to On-Demand Instances. This is especially beneficial if the application runs 24/7.

Migrating the data storage layer to Amazon Aurora Reserved Instances provides cost optimization for the growing database storage needs. Amazon Aurora is a fully managed relational database service that offers high performance, scalability, and cost efficiency.

upvoted 1 times

copen 6 months ago

nnascncnscnknkckl

upvoted 1 times

TariqKipkemei 7 months, 2 weeks ago

Answer is C

upvoted 1 times

QuangPham810 7 months, 2 weeks ago

Answer is C. Refer https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_WorkingWithReservedDBInstances.html => Size-flexible reserved DB instances

upvoted 1 times

Abhineet9148232 8 months, 3 weeks ago

Selected Answer: C

C: With Aurora Serverless v2, each writer and reader has its own current capacity value, measured in ACUs. Aurora Serverless v2 scales a writer or reader up to a higher capacity when its current capacity is too low to handle the load. It scales the writer or reader down to a lower capacity when its current capacity is higher than needed.

This is sufficient to accommodate the growing data changes.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html#aurora-serverless-v2.how-it-works.scaling>

upvoted 1 times

Steve_4542636 9 months ago

Selected Answer: C

Typically Amazon RDS cost less than Aurora. But here, it's Aurora reserved.

upvoted 1 times

ACasper 9 months ago

Answer C

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_WorkingWithReservedDBInstances.html
Discounts for reserved DB instances are tied to instance type and AWS Region.

upvoted 1 times

AlmeroSenior 9 months, 1 week ago

Selected Answer: C

Both RDS and RDS aurora support Storage Auto scale .

Aurora is more expensive than base RDS , But between B and C , the Aurora is reserved instance and base RDS is on demand . Also it states the DB strorage will grow , so no concern about a bigger DB instance (server) , only the actual storage

upvoted 1 times

Joxtat 9 months, 1 week ago

Selected Answer: C

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

upvoted 1 times

Samuel03 9 months, 1 week ago

Selected Answer: B

I also think it is B. Otherewise there is no point in mentionig about growing storage requirements.

upvoted 2 times

Americo32 9 months, 1 week ago

Selected Answer: B

A opção B com base no fato de que o armazenamento de banco de dados continuará a crescer, portanto, sob demanda será uma solução mais adequada

upvoted 1 times

✉ **Americo32** 9 months, 1 week ago

Mudando para opção C, Observações importantes sobre compras

Os preços de instâncias reservadas cobrem apenas os custos da instância. O armazenamento e a E/S ainda são faturados separadamente.

upvoted 1 times

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

Why not B?

upvoted 3 times

A university research laboratory needs to migrate 30 TB of data from an on-premises Windows file server to Amazon FSx for Windows File Server. The laboratory has a 1 Gbps network link that many other departments in the university share.

The laboratory wants to implement a data migration service that will maximize the performance of the data transfer. However, the laboratory needs to be able to control the amount of bandwidth that the service uses to minimize the impact on other departments. The data migration must take place within the next 5 days.

Which AWS solution will meet these requirements?

- A. AWS Snowcone
- B. Amazon FSx File Gateway
- C. AWS DataSync
- D. AWS Transfer Family

Correct Answer: C

Community vote distribution

C (100%)

✉  **kruasan**  7 months ago

Selected Answer: C

AWS DataSync is a data transfer service that can copy large amounts of data between on-premises storage and Amazon FSx for Windows File Server at high speeds. It allows you to control the amount of bandwidth used during data transfer.

- DataSync uses agents at the source and destination to automatically copy files and file metadata over the network. This optimizes the data transfer and minimizes the impact on your network bandwidth.
- DataSync allows you to schedule data transfers and configure transfer rates to suit your needs. You can transfer 30 TB within 5 days while controlling bandwidth usage.
- DataSync can resume interrupted transfers and validate data to ensure integrity. It provides detailed monitoring and reporting on the progress and performance of data transfers.

upvoted 7 times

✉  **kruasan** 7 months ago

Option A - AWS Snowcone is more suitable for physically transporting data when network bandwidth is limited. It would not complete the transfer within 5 days.

Option B - Amazon FSx File Gateway only provides access to files stored in Amazon FSx and does not perform the actual data migration from on-premises to FSx.

Option D - AWS Transfer Family is for transferring files over FTP, FTPS and SFTP. It may require scripting to transfer 30 TB and monitor progress, and lacks bandwidth controls.

upvoted 7 times

✉  **Michal_L_95**  8 months, 3 weeks ago

Selected Answer: C

As read a little bit, I assume that B (FSx File Gateway) requires a little bit more configuration rather than C (DataSync). From Stephane Maarek course explanation about DataSync:

An online data transfer service that simplifies, automates, and accelerates copying large amounts of data between on-premises storage systems and AWS Storage services, as well as between AWS Storage services.

You can use AWS DataSync to migrate data located on-premises, at the edge, or in other clouds to Amazon S3, Amazon EFS, Amazon FSx for Windows File Server, Amazon FSx for Lustre, Amazon FSx for OpenZFS, and Amazon FSx for NetApp ONTAP.

upvoted 7 times

✉  **AZ_Master**  6 days, 16 hours ago

Selected Answer: C

Bandwidth control = Data Sync

<https://docs.aws.amazon.com/datasync/latest/userguide/configure-bandwidth.html>

upvoted 1 times

✉  **Ruffyit** 2 weeks ago

Bandwidth Optimization and Control

Transferring hot or cold data should not impede your business. DataSync is equipped with granular controls to optimize bandwidth consumptions. Throttle transfer speeds up to 10 Gbps during off hours and set limits when network availability is needed elsewhere

upvoted 1 times

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

Selected Answer: C

C. AWS DataSync
upvoted 1 times

 **Nikki013** 3 months ago

Selected Answer: C

<https://aws.amazon.com/datasync/features/>
upvoted 1 times

 **Yousuf_Ibrahim** 1 month, 2 weeks ago

Bandwidth Optimization and Control

Transferring hot or cold data should not impede your business. DataSync is equipped with granular controls to optimize bandwidth consumptions. Throttle transfer speeds up to 10 Gbps during off hours and set limits when network availability is needed elsewhere.
upvoted 1 times

 **jayce5** 5 months, 2 weeks ago

Selected Answer: C

"Amazon FSx File Gateway" is for storing data, not for migrating. So the answer should be C.
upvoted 2 times

 **ACloud_Guru15** 3 weeks, 1 day ago

Thanks for the explanation
upvoted 1 times

 **shanwford** 7 months, 3 weeks ago

Selected Answer: C

Snowcone is small and delivery time is long. With DataSync you can set bandwidth limits - so this is a fine solution.
upvoted 3 times

 **MaxMa** 8 months ago

Why not B?
upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Transferring will be much longer term rather than 5 days as required.
upvoted 1 times

 **AlessandraSAA** 8 months, 3 weeks ago

A is not possible because Snowcone is just 8TB and it takes 4-6 business days to deliver
B why cannot be <https://aws.amazon.com/storagegateway/file/fsx/>?
C I don't really get this
D cannot be because not compatible - <https://aws.amazon.com/aws-transfer-family/>
upvoted 1 times

 **Steve_4542636** 9 months ago

Selected Answer: C

Voting C
upvoted 1 times

 **Bhawesh** 9 months, 1 week ago

Selected Answer: C

C. - DataSync is correct.
A. Snowcone is incorrect. The question says data migration must take place within the next 5 days. AWS says: If you order, you will receive the Snowcone device in approximately 4-6 days.
upvoted 2 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: C

DataSync can be used to migrate data between on-premises Windows file servers and Amazon FSx for Windows File Server with its compatibility for Windows file systems.

The laboratory needs to migrate a large amount of data (30 TB) within a relatively short timeframe (5 days) and limit the impact on other departments' network traffic. Therefore, AWS DataSync can meet these requirements by providing fast and efficient data transfer with network throttling capability to control bandwidth usage.

upvoted 3 times

 **cloudbusting** 9 months, 1 week ago

<https://docs.aws.amazon.com/datasync/latest/userguide/configure-bandwidth.html>
upvoted 2 times

 **bdp123** 9 months, 2 weeks ago

Selected Answer: C

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

upvoted 2 times

A company wants to create a mobile app that allows users to stream slow-motion video clips on their mobile devices. Currently, the app captures video clips and uploads the video clips in raw format into an Amazon S3 bucket. The app retrieves these video clips directly from the S3 bucket. However, the videos are large in their raw format.

Users are experiencing issues with buffering and playback on mobile devices. The company wants to implement solutions to maximize the performance and scalability of the app while minimizing operational overhead.

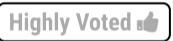
Which combination of solutions will meet these requirements? (Choose two.)

- A. Deploy Amazon CloudFront for content delivery and caching.
- B. Use AWS DataSync to replicate the video files across AW'S Regions in other S3 buckets.
- C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.
- D. Deploy an Auto Sealing group of Amazon EC2 instances in Local Zones for content delivery and caching.
- E. Deploy an Auto Scaling group of Amazon EC2 instances to convert the video files to more appropriate formats.

Correct Answer: A

Community vote distribution

A (53%) C (47%)

✉  **Bhawesh**  9 months, 2 weeks ago

For Minimum operational overhead, the 2 options A,C should be correct.

- A. Deploy Amazon CloudFront for content delivery and caching.
- C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.

upvoted 12 times

✉  **Ruffyit**  2 weeks ago

For Minimum operational overhead, the 2 options A,C should be correct.

- A. Deploy Amazon CloudFront for content delivery and caching.
- C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.

upvoted 1 times

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

Selected Answer: A

For Minimum operational overhead, the 2 options A,C should be correct.

- A. Deploy Amazon CloudFront for content delivery and caching.
- C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.

upvoted 1 times

✉  **Guru4Cloud** 2 months ago

examtopics team, please fix this question, please allow to select two answer

upvoted 1 times

✉  **jacob_ho** 3 months ago

Elastic Transcoder has been deprecated, and AWS encourage to use AWS Elemental MediaConvert right now:

<https://aws.amazon.com/blogs/media/how-to-migrate-workflows-from-amazon-elastic-transcoder-to-aws-elemental-mediaconvert/>

upvoted 4 times

✉  **enc_0343** 5 months ago

Selected Answer: A

AC is the correct answer

upvoted 1 times

✉  **antropaws** 6 months, 1 week ago

Selected Answer: A

AC, the only possible answers.

upvoted 1 times

✉  **Eden** 6 months, 3 weeks ago

It says choose two so I chose AC

upvoted 1 times

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

Selected Answer: C

A & C are the right answers.

upvoted 2 times

 **kampatra** 8 months, 2 weeks ago

Selected Answer: A

Correct answer: AC

upvoted 2 times

 **Steve_4542636** 9 months ago

Selected Answer: C

A and C. Transcoder does exactly what this needs.

upvoted 2 times

 **Steve_4542636** 9 months ago

Selected Answer: A

A and C. CloudFront has caching for A

upvoted 1 times

 **wawaw3213** 9 months, 1 week ago

Selected Answer: C

a and c

upvoted 2 times

 **bdp123** 9 months, 1 week ago

Selected Answer: C

Both A and C - I was not able to choose both

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

upvoted 2 times

 **Bhrino** 9 months, 1 week ago

Selected Answer: C

A and C bc cloud front would help the performance for content such as this and elastictranscoder makes the process from transferring devices almost seamless

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: A

A & C.

A: Deploy Amazon CloudFront for content delivery and caching: Amazon CloudFront is a content delivery network (CDN) that can help improve the performance and scalability of the app by caching content at edge locations, reducing latency, and improving the delivery of video clips to users. CloudFront can also provide features such as DDoS protection, SSL/TLS encryption, and content compression to optimize the delivery of video clips.

C: Use Amazon Elastic Transcoder to convert the video files to more appropriate formats: Amazon Elastic Transcoder is a service that can help optimize the video format for mobile devices, reducing the size of the video files, and improving the playback performance. Elastic Transcoder can also convert videos into multiple formats to support different devices and platforms.

upvoted 2 times

 **Babba** 9 months, 1 week ago

Selected Answer: A

Clearly A & C

upvoted 1 times

 **jahmad0730** 9 months, 1 week ago

Selected Answer: A

A and C

upvoted 1 times

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

- A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
- B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
- C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
- D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

Correct Answer: D

Community vote distribution

D (100%)

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

Answer is D - Auto-scaling with target tracking
upvoted 8 times

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

Target tracking will scale in/out the ECS cluster to maintain the average CPU utilization to a set value. e.g. <<<50%>>> Scale out when average CPU utilization is above 50% until average CPU utilization is back to 50%. And scale in when average CPU utilization is below 50% until average CPU utilization is back to 50%.
upvoted 2 times

 **TariqKipkemei** 1 month, 3 weeks ago

Answer is D
upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: D

Answer is D - Auto-scaling with target tracking
upvoted 1 times

 **TariqKipkemei** 7 months ago

Answer is D - Application Auto Scaling is a web service for developers and system administrators who need a solution for automatically scaling their scalable resources for individual AWS services beyond Amazon EC2.
upvoted 3 times

 **boxu03** 8 months, 3 weeks ago

Selected Answer: D
should be D
upvoted 1 times

 **Joxtat** 9 months, 1 week ago

Selected Answer: D
<https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html>
upvoted 3 times

 **jahmad0730** 9 months, 1 week ago

Selected Answer: D
Answer is D
upvoted 2 times

 **Neha999** 9 months, 1 week ago

D : auto-scaling with target tracking
upvoted 4 times

A company recently created a disaster recovery site in a different AWS Region. The company needs to transfer large amounts of data back and forth between NFS file systems in the two Regions on a periodic basis.

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

- A. Use AWS DataSync.
- B. Use AWS Snowball devices.
- C. Set up an SFTP server on Amazon EC2.
- D. Use AWS Database Migration Service (AWS DMS).

Correct Answer: A

Community vote distribution

A (100%)

✉️  **LuckyAro** Highly Voted 9 months, 1 week ago

Selected Answer: A

AWS DataSync is a fully managed data transfer service that simplifies moving large amounts of data between on-premises storage systems and AWS services. It can also transfer data between different AWS services, including different AWS Regions. DataSync provides a simple, scalable, and automated solution to transfer data, and it minimizes the operational overhead because it is fully managed by AWS.

upvoted 9 times

✉️  **Ruffyit** Most Recent 1 week, 6 days ago

AWS DataSync is a fully managed data transfer service that simplifies moving large amounts of data between on-premises storage systems and AWS services. It can also transfer data between different AWS services, including different AWS Regions. DataSync provides a simple, scalable, and automated solution to transfer data, and it minimizes the operational overhead because it is fully managed by AWS.

upvoted 1 times

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

Selected Answer: A

Use AWS DataSync

upvoted 1 times

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

Selected Answer: A

Use AWS DataSync.

upvoted 1 times

✉️  **kruasan** 7 months ago

Selected Answer: A

- AWS DataSync is a data transfer service optimized for moving large amounts of data between NFS file systems. It can automatically copy files and metadata between your NFS file systems in different AWS Regions.
- DataSync requires minimal setup and management. You deploy a source and destination agent, provide the source and destination locations, and DataSync handles the actual data transfer efficiently in the background.
- DataSync can schedule and monitor data transfers to keep source and destination in sync with minimal overhead. It resumes interrupted transfers and validates data integrity.
- DataSync optimizes data transfer performance across AWS's network infrastructure. It can achieve high throughput with minimal impact to your operations.

upvoted 2 times

✉️  **kruasan** 7 months ago

Option B - AWS Snowball requires physical devices to transfer data. This incurs overhead to transport devices and manually load/unload data. It is not an online data transfer solution.

Option C - Setting up and managing an SFTP server would require provisioning EC2 instances, handling security groups, and writing scripts to automate the data transfer - all of which demand more overhead than DataSync.

Option D - AWS Database Migration Service is designed for migrating databases, not general file system data. It would require converting your NFS data into a database format, incurring additional overhead.

upvoted 1 times

✉️  **ashu089** 8 months ago

Selected Answer: A

A only

upvoted 1 times

✉️  **skiwili** 9 months, 1 week ago

Selected Answer: A

Aaaaaa

upvoted 1 times

 **NolaHolla** 9 months, 1 week ago

A should be correct

upvoted 1 times

A company is designing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.

Which AWS solution meets these requirements?

- A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
- 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 FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon S3 bucket. Assign an IAM role to the application to grant access to the S3 bucket. Mount the S3 bucket to the application server.

Correct Answer: C

Community vote distribution

C (100%)

✉  **rrharris**  9 months, 1 week ago

Answer is C - SMB = storage gateway or FSx
upvoted 6 times

✉  **Neha999**  9 months, 1 week ago

C L: Amazon FSx for Windows File Server file system
upvoted 5 times

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

Selected Answer: C

SMB = FSx for Windows File Server
upvoted 2 times

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

Selected Answer: C

Answer is C - SMB = storage gateway or FSx
upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: C

- Amazon FSx for Windows File Server provides a fully managed native Windows file system that can be accessed using the industry-standard SMB protocol. This allows Windows clients like the gaming application to directly access file data.
- FSx for Windows File Server handles time-consuming file system administration tasks like provisioning, setup, maintenance, file share management, backups, security, and software patching - reducing operational overhead.
- FSx for Windows File Server supports high file system throughput, IOPS, and consistent low latencies required for performance-sensitive workloads. This makes it suitable for a gaming application.
- The file system can be directly attached to EC2 instances, providing a performant shared storage solution for the gaming servers.

upvoted 4 times

✉  **kruasan** 7 months ago

Option A - DataSync is for data transfer, not providing a shared file system. It cannot be mounted or directly accessed.

Option B - A self-managed EC2 file share would require manually installing, configuring and maintaining a Windows file system and share. This demands significant overhead to operate.

Option D - Amazon S3 is object storage, not a native file system. The data in S3 would need to be converted/formatted to provide file share access, adding complexity. S3 cannot be directly mounted or provide the performance of FSx.

upvoted 2 times

✉  **elearningtakai** 8 months ago

Selected Answer: C

Amazon FSx for Windows File Server
upvoted 1 times

✉  **Steve_4542636** 9 months ago

Selected Answer: C

I vote C since FSx supports SMB

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: C

AWS FSx for Windows File Server is a fully managed native Microsoft Windows file system that is accessible through the SMB protocol. It provides features such as file system backups, integrated with Amazon S3, and Active Directory integration for user authentication and access control. This solution allows for the use of SMB clients to access the data and is fully managed, eliminating the need for the company to manage the underlying infrastructure.

upvoted 2 times

 **Babba** 9 months, 1 week ago

Selected Answer: C

C for me

upvoted 1 times

A company wants to run an in-memory database for a latency-sensitive application that runs on Amazon EC2 instances. The application processes more than 100,000 transactions each minute and requires high network throughput. A solutions architect needs to provide a cost-effective network design that minimizes data transfer charges.

Which solution meets these requirements?

- A. Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances.
- B. Launch all EC2 instances in different Availability Zones within the same AWS Region. Specify a placement group with partition strategy when launching EC2 instances.
- C. Deploy an Auto Scaling group to launch EC2 instances in different Availability Zones based on a network utilization target.
- D. Deploy an Auto Scaling group with a step scaling policy to launch EC2 instances in different Availability Zones.

Correct Answer: A

Community vote distribution

A (100%)

✉  **kruasan**  7 months ago

Selected Answer: A

Reasons:

- Launching instances within a single AZ and using a cluster placement group provides the lowest network latency and highest bandwidth between instances. This maximizes performance for an in-memory database and high-throughput application.
- Communications between instances in the same AZ and placement group are free, minimizing data transfer charges. Inter-AZ and public IP traffic can incur charges.
- A cluster placement group enables the instances to be placed close together within the AZ, allowing the high network throughput required. Partition groups span AZs, reducing bandwidth.
- Auto Scaling across zones could launch instances in AZs that increase data transfer charges. It may reduce network throughput, impacting performance.

upvoted 10 times

✉  **kruasan** 7 months ago

In contrast:

- Option B - A partition placement group spans AZs, reducing network bandwidth between instances and potentially increasing costs.
- Option C - Auto Scaling alone does not guarantee the network throughput and cost controls required for this use case. Launching across AZs could increase data transfer charges.
- Option D - Step scaling policies determine how many instances to launch based on metrics alone. They lack control over network connectivity and costs between instances after launch.

upvoted 6 times

✉  **Ruffyt**  1 week, 6 days ago

- Launching instances within a single AZ and using a cluster placement group provides the lowest network latency and highest bandwidth between instances. This maximizes performance for an in-memory database and high-throughput application.
- Communications between instances in the same AZ and placement group are free, minimizing data transfer charges. Inter-AZ and public IP traffic can incur charges.
- A cluster placement group enables the instances to be placed close together within the AZ, allowing the high network throughput required. Partition groups span AZs, reducing bandwidth.

upvoted 1 times

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

Selected Answer: A

Cluster placement group packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance.

upvoted 3 times

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

Selected Answer: A

Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances

upvoted 1 times

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

Selected Answer: A

Cluster - have low latency if its in same AZ and same region so Answer is "A"

upvoted 2 times

✉ **BeeKayEnn** 8 months ago

Answer would be A - As part of selecting all the EC2 instances in the same availability zone, they all will be within the same DC and logically the latency will be very less as compared to the other Availability Zones..

As all the autoscaling nodes will also be on the same availability zones, (as per Placement groups with Cluster mode), this would provide the low-latency network performance

Reference is below:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

upvoted 2 times

✉ **[Removed]** 8 months ago

Selected Answer: A

A - Low latency, high net throughput

upvoted 1 times

✉ **elearningtakai** 8 months ago

Selected Answer: A

A placement group is a logical grouping of instances within a single Availability Zone, and it provides low-latency network connectivity between instances. By launching all EC2 instances in the same Availability Zone and specifying a placement group with cluster strategy, the application can take advantage of the high network throughput and low latency network connectivity that placement groups provide.

upvoted 1 times

✉ **Steve_4542636** 9 months ago

Selected Answer: A

Cluster placement groups improves throughput between the instances which means less EC2 instances would be needed thus reducing costs.

upvoted 1 times

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

Selected Answer: A

A because Specify a placement group

upvoted 1 times

✉ **KZM** 9 months, 1 week ago

It is option A:

To achieve low latency, high throughput, and cost-effectiveness, the optimal solution is to launch EC2 instances as a placement group with the cluster strategy within the same Availability Zone.

upvoted 2 times

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

Why not C?

upvoted 1 times

✉ **Steve_4542636** 9 months ago

You're thinking operational efficiency. The question asks for cost reduction.

upvoted 3 times

✉ **rrharris** 9 months, 1 week ago

Answer is A - Clustering

upvoted 2 times

✉ **Neha999** 9 months, 1 week ago

A : Cluster placement group

upvoted 4 times

A company that primarily runs its application servers on premises has decided to migrate to AWS. The company wants to minimize its need to scale its Internet Small Computer Systems Interface (iSCSI) storage on premises. The company wants only its recently accessed data to remain stored locally.

Which AWS solution should the company use to meet these requirements?

- A. Amazon S3 File Gateway
- B. AWS Storage Gateway Tape Gateway
- C. AWS Storage Gateway Volume Gateway stored volumes
- D. AWS Storage Gateway Volume Gateway cached volumes

Correct Answer: A

Community vote distribution

D (100%)

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

Selected Answer: D

AWS Storage Gateway Volume Gateway provides two configurations for connecting to iSCSI storage, namely, stored volumes and cached volumes. The stored volume configuration stores the entire data set on-premises and asynchronously backs up the data to AWS. The cached volume configuration stores recently accessed data on-premises, and the remaining data is stored in Amazon S3.

Since the company wants only its recently accessed data to remain stored locally, the cached volume configuration would be the most appropriate. It allows the company to keep frequently accessed data on-premises and reduce the need for scaling its iSCSI storage while still providing access to all data through the AWS cloud. This configuration also provides low-latency access to frequently accessed data and cost-effective off-site backups for less frequently accessed data.

upvoted 26 times

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

Selected Answer: D

https://docs.amazonaws.cn/en_us/storagegateway/latest/vgw/StorageGatewayConcepts.html#storage-gateway-cached-concepts
upvoted 6 times

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

Selected Answer: D

Frequently accessed data = AWS Storage Gateway Volume Gateway cached volumes
upvoted 2 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: D

The best AWS solution to meet the requirements is to use AWS Storage Gateway cached volumes (option D).

The key points:

Company migrating on-prem app servers to AWS
Want to minimize scaling on-prem iSCSI storage

Only recent data should remain on-premises

The AWS Storage Gateway cached volumes allow the company to connect their on-premises iSCSI storage to AWS cloud storage. It stores frequently accessed data locally in the cache for low-latency access, while older data is stored in AWS.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: D

- Volume Gateway cached volumes store entire datasets on S3, while keeping a portion of recently accessed data on your local storage as a cache. This meets the goal of minimizing on-premises storage needs while keeping hot data local.
- The cache provides low-latency access to your frequently accessed data, while long-term retention of the entire dataset is provided durable and cost-effective in S3.
- You get virtually unlimited storage on S3 for your infrequently accessed data, while controlling the amount of local storage used for cache. This simplifies on-premises storage scaling.
- Volume Gateway cached volumes support iSCSI connections from on-premises application servers, allowing a seamless migration experience. Servers access local cache and S3 storage volumes as iSCSI LUNs.

upvoted 5 times

 **kruasan** 7 months ago

In contrast:
Option A - S3 File Gateway only provides file interfaces (NFS/SMB) to data in S3. It does not support block storage or cache recently accessed data locally.
Option B - Tape Gateway is designed for long-term backup and archiving to virtual tape cartridges on S3. It does not provide primary storage volumes or local cache for low-latency access.
Option C - Volume Gateway stored volumes keep entire datasets locally, then asynchronously back them up to S3. This does not meet the goal of minimizing on-premises storage needs.

upvoted 3 times

 **Steve_4542636** 9 months ago

Selected Answer: D

I vote D

upvoted 1 times

 **ManOnTheMoon** 9 months, 1 week ago

Agree with D

upvoted 1 times

 **Babba** 9 months, 1 week ago

Selected Answer: D

recently accessed data to remain stored locally - cached

upvoted 3 times

 **Bhawesh** 9 months, 2 weeks ago

Selected Answer: D

D. AWS Storage Gateway Volume Gateway cached volumes

upvoted 3 times

 **bdp123** 9 months, 2 weeks ago

Selected Answer: D

recently accessed data to remain stored locally - cached

upvoted 3 times

A company has multiple AWS accounts that use consolidated billing. The company runs several active high performance Amazon RDS for Oracle On-Demand DB instances for 90 days. The company's finance team has access to AWS Trusted Advisor in the consolidated billing account and all other AWS accounts.

The finance team needs to use the appropriate AWS account to access the Trusted Advisor check recommendations for RDS. The finance team must review the appropriate Trusted Advisor check to reduce RDS costs.

Which combination of steps should the finance team take to meet these requirements? (Choose two.)

- A. Use the Trusted Advisor recommendations from the account where the RDS instances are running.
- B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time.
- C. Review the Trusted Advisor check for Amazon RDS Reserved Instance Optimization.
- D. Review the Trusted Advisor check for Amazon RDS Idle DB Instances.
- E. Review the Trusted Advisor check for Amazon Redshift Reserved Node Optimization.

Correct Answer: AC

Community vote distribution

BD (75%)

BC (25%)

✉  **Nietzsche82** Highly Voted 9 months, 1 week ago

Selected Answer: BD

B & D

<https://aws.amazon.com/premiumsupport/knowledge-center/trusted-advisor-cost-optimization/>

upvoted 12 times

✉  **AZ_Master** Most Recent 6 days, 15 hours ago

Selected Answer: BD

Answer is B & D because you can view from consolidated billing account and since RDS instances are on-demand for 90 days. There is no reserved instances. So, there is no need to check for RDS Reserved Instance Optimization.

upvoted 1 times

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

Selected Answer: BD

Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time and review the Trusted Advisor check for Amazon RDS Idle DB Instances

upvoted 2 times

✉  **ambermeh** 1 month, 4 weeks ago

B & D is correct answer after research

upvoted 1 times

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

Selected Answer: BD

B&D are correct !

upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: BD

<https://docs.aws.amazon.com/awssupport/latest/user/organizational-view.html>

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html#amazon-rds-idle-dbs-instances>

upvoted 1 times

✉  **ErfanKh** 7 months, 2 weeks ago

Selected Answer: BC

I think BC and ChatGPT as well

upvoted 2 times

✉  **ACloud_Guru15** 3 weeks, 1 day ago

ChatGPT is like as kid, if you say & A&D is the correct answer. Its not 100% accurate info

upvoted 1 times

 kraken21 8 months ago

Selected Answer: BD

B and D

upvoted 1 times

 Russ99 8 months, 1 week ago

Selected Answer: BC

Option A is not necessary, as the Trusted Advisor recommendations can be accessed from the consolidated billing account. Option D is not relevant, as the check for idle DB instances is not specific to RDS instances. Option E is for Amazon Redshift, not RDS, and is therefore not relevant.

upvoted 2 times

 kruasan 7 months ago

it is

Amazon RDS Idle DB Instances

Description

Checks the configuration of your Amazon Relational Database Service (Amazon RDS) for any database (DB) instances that appear to be idle.

If a DB instance has not had a connection for a prolonged period of time, you can delete the instance to reduce costs. A DB instance is considered idle if the instance hasn't had a connection in the past 7 days. If persistent storage is needed for data on the instance, you can use lower-cost options such as taking and retaining a DB snapshot. Manually created DB snapshots are retained until you delete them.

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html#amazon-rds-idle-dbs-instances>

upvoted 2 times

 Steve_4542636 9 months ago

Selected Answer: BD

I got with B and D

upvoted 2 times

 Michal_L_95 9 months ago

Selected Answer: BC

I would go with B and C as the company is running for 90 days and C option is basing on 30 days report which would mean that there is higher potential on cost saving rather than on idle instances

upvoted 3 times

 Steve_4542636 9 months ago

C is stating "Reserved Instances" The question states they are using On Demand Instances. Reserved instances are reserved for less money for 1 or 3 years.

upvoted 7 times

 Lalo 5 months, 3 weeks ago

In the scenario it says for 90 days, therefore the correct answer is D

No C

upvoted 2 times

 Michal_L_95 8 months, 3 weeks ago

Once read the question again, I agree with you.

upvoted 1 times

 bdp123 9 months, 1 week ago

Selected Answer: BD

reduce costs - delete idle instances

<https://aws.amazon.com/premiumsupport/knowledge-center/trusted-advisor-cost-optimization/>

upvoted 3 times

 leoattf 9 months, 1 week ago

This same URL also says that there is an option which recommends the purchase of reserved noes. So I think that C is the option instead of D, because since they already use on-demand DB instances, most probably that there will not have iddle instances. But if we replace them by reserved ones, we indeed can have some costs savings.

What are your thought on it?

upvoted 1 times

 LuckyAro 9 months, 1 week ago

Selected Answer: BC

B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time. This option allows the finance team to see all RDS instance checks across all AWS accounts in one place. Since the company uses consolidated billing, this account will have access to all of the AWS accounts' Trusted Advisor recommendations.

C. Review the Trusted Advisor check for Amazon RDS Reserved Instance Optimization. This check can help identify cost savings opportunities for RDS by identifying instances that can be covered by Reserved Instances. This can result in significant savings on RDS costs.

upvoted 2 times

 leoattf 9 months, 1 week ago

I also think it is B and C. I think that C is the option instead of D, because since they already use on-demand DB instances, most probably there will not have idle instances. But if we replace them by reserved ones, we indeed can have some costs savings.

upvoted 1 times

✉️  **LuckyAro** 9 months, 1 week ago

Option A is not recommended because the finance team may not have access to the AWS account where the RDS instances are running. Even if they have access, it may not be practical to check each individual account for Trusted Advisor recommendations.

Option D is not the best choice because it only addresses the issue of idle instances and may not provide the most effective recommendations to reduce RDS costs.

Option E is not relevant to this scenario since it is related to Amazon Redshift, not RDS.

upvoted 1 times

✉️  **jennyka76** 9 months, 1 week ago

B & D

<https://aws.amazon.com/premiumsupport/knowledge-center/trusted-advisor-cost-optimization/>

upvoted 3 times

✉️  **skiwili** 9 months, 1 week ago

Selected Answer: BD

B and D I believe

upvoted 4 times

A solutions architect needs to optimize storage costs. The solutions architect must identify any Amazon S3 buckets that are no longer being accessed or are rarely accessed.

Which solution will accomplish this goal with the LEAST operational overhead?

- A. Analyze bucket access patterns by using the S3 Storage Lens dashboard for advanced activity metrics.
- B. Analyze bucket access patterns by using the S3 dashboard in the AWS Management Console.
- C. Turn on the Amazon CloudWatch BucketSizeBytes metric for buckets. Analyze bucket access patterns by using the metrics data with Amazon Athena.
- D. Turn on AWS CloudTrail for S3 object monitoring. Analyze bucket access patterns by using CloudTrail logs that are integrated with Amazon CloudWatch Logs.

Correct Answer: D

Community vote distribution

A (93%) 7%

 **kpato87** Highly Voted 9 months, 1 week ago

Selected Answer: A

S3 Storage Lens is a fully managed S3 storage analytics solution that provides a comprehensive view of object storage usage, activity trends, and recommendations to optimize costs. Storage Lens allows you to analyze object access patterns across all of your S3 buckets and generate detailed metrics and reports.

upvoted 13 times

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

S3 Storage Lens is a fully managed S3 storage analytics solution that provides a comprehensive view of object storage usage, activity trends, and recommendations to optimize costs. Storage Lens allows you to analyze object access patterns across all of your S3 buckets and generate detailed metrics and reports.

upvoted 1 times

 **TariqKipkemei** 1 month, 3 weeks ago

Selected Answer: A

Amazon S3 Storage Lens was designed to handle this requirement.

upvoted 1 times

 **Wayne23Fang** 2 months, 3 weeks ago

Selected Answer: D

A missed turning on monitoring. It can also help you learn about your customer base and understand your Amazon S3 bill. By default, Amazon S3 doesn't collect server access logs. When you enable logging, Amazon S3 delivers access logs for a source bucket to a target bucket that you choose.

I could not find that S3 storage Lens examples online showing using Lens to identify idle S3 buckets. Instead I find using S3 Access Logging. Hmm.
upvoted 2 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: A

S3 Storage Lens is a cloud-storage analytics feature that provides you with 29+ usage and activity metrics, including object count, size, age, and access patterns. This data can help you understand how your data is being used and identify areas where you can optimize your storage costs. The S3 Storage Lens dashboard provides an interactive view of your storage usage and activity trends. This makes it easy to identify buckets that are no longer being accessed or are rarely accessed.

The S3 Storage Lens dashboard is a fully managed service, so there is no need to set up or manage any additional infrastructure.

upvoted 1 times

 **BigHammer** 2 months, 3 weeks ago

"S3 Storage Lens" seems to be the popular answer, however, where in Storage Lens can you see if a bucket/object is being USED? I see all kinds of stats, but not that.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

<https://aws.amazon.com/blogs/aws/s3-storage-lens/>

upvoted 2 times

 **kruasan** 7 months ago

Selected Answer: A

The S3 Storage Lens dashboard provides visibility into storage metrics and activity patterns to help optimize storage costs. It shows metrics like objects added, objects deleted, storage consumed, and requests. It can filter by bucket, prefix, and tag to analyze specific subsets of data

upvoted 2 times

 **kruasan** 7 months ago

- B) The standard S3 console dashboard provides basic info but would require manually analyzing metrics for each bucket. This does not scale well and requires significant overhead.
- C) Turning on the BucketSizeBytes metric and analyzing the data in Athena may provide insights but would require enabling metrics, building Athena queries, and analyzing the results. This requires more operational effort than option A.
- D) Enabling CloudTrail logging and monitoring the logs in CloudWatch Logs could provide access pattern data but would require setting up CloudTrail, monitoring the logs, and analyzing the relevant info. This option has the highest operational overhead

upvoted 3 times

 **bdp123** 9 months, 1 week ago

Selected Answer: A

<https://aws.amazon.com/blogs/aws/s3-storage-lens/>

upvoted 4 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: A

S3 Storage Lens provides a dashboard with advanced activity metrics that enable the identification of infrequently accessed and unused buckets. This can help a solutions architect optimize storage costs without incurring additional operational overhead.

upvoted 3 times

 **Babba** 9 months, 1 week ago

Selected Answer: A

it looks like it's A

upvoted 2 times

A company sells datasets to customers who do research in artificial intelligence and machine learning (AI/ML). The datasets are large, formatted files that are stored in an Amazon S3 bucket in the us-east-1 Region. The company hosts a web application that the customers use to purchase access to a given dataset. The web application is deployed on multiple Amazon EC2 instances behind an Application Load Balancer. After a purchase is made, customers receive an S3 signed URL that allows access to the files.

The customers are distributed across North America and Europe. The company wants to reduce the cost that is associated with data transfers and wants to maintain or improve performance.

What should a solutions architect do to meet these requirements?

- A. Configure S3 Transfer Acceleration on the existing S3 bucket. Direct customer requests to the S3 Transfer Acceleration endpoint. Continue to use S3 signed URLs for access control.
- B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL. Switch to CloudFront signed URLs for access control.
- C. Set up a second S3 bucket in the eu-central-1 Region with S3 Cross-Region Replication between the buckets. Direct customer requests to the closest Region. Continue to use S3 signed URLs for access control.
- D. Modify the web application to enable streaming of the datasets to end users. Configure the web application to read the data from the existing S3 bucket. Implement access control directly in the application.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

To reduce the cost associated with data transfers and maintain or improve performance, a solutions architect should use Amazon CloudFront, a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

Deploying a CloudFront distribution with the existing S3 bucket as the origin will allow the company to serve the data to customers from edge locations that are closer to them, reducing data transfer costs and improving performance.

Directing customer requests to the CloudFront URL and switching to CloudFront signed URLs for access control will enable customers to access the data securely and efficiently.

upvoted 9 times

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

To reduce the cost associated with data transfers and maintain or improve performance, a solutions architect should use Amazon CloudFront, a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

upvoted 1 times

 **TariqKipkemei** 1 month, 3 weeks ago

Selected Answer: B

Technically both option B and C will work. But because cost is a factor then Amazon CloudFront should be the preferred option.

upvoted 1 times

 **react97** 1 month, 4 weeks ago

Selected Answer: B

B.

1. Amazon CloudFront caches content at edge locations -- reducing the need for frequent data transfer from S3 bucket -- thus significantly lowering data transfer costs (as compared to directly serving data from S3 bucket to customers in different regions)
2. CloudFront delivers content to users from the nearest edge location -- minimizing latency -- improves performance for customers

A - focus on accelerating uploads to S3 which may not necessarily improve the performance needed for serving datasets to customers
C - helps with redundancy and data availability but does not necessarily offer cost savings for data transfer.

D - complex to implement, does not address data transfer cost

upvoted 4 times

 **bdp123** 9 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

upvoted 3 times

 **Bhawesh** 9 months, 2 weeks ago

Selected Answer: B

B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL. Switch to CloudFront signed URLs for access control.

<https://www.examtopics.com/discussions/amazon/view/68990-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

A company is using AWS to design a web application that will process insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type, must be responded to within 24 hours, and must not get lost. The solution must maximize operational efficiency and must minimize maintenance.

Which solution meets these requirements?

- A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to use the Kinesis Client Library (KCL) to pool messages from its own data stream.
- B. Create an AWS Lambda function and an Amazon Simple Notification Service (Amazon SNS) topic for each quote type. Subscribe the Lambda function to its associated SNS topic. Configure the application to publish requests for quotes to the appropriate SNS topic.
- C. Create a single Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to use its own SQS queue.
- D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon OpenSearch Service cluster. Configure the application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from OpenSearch Service and process them accordingly.

Correct Answer: D

Community vote distribution

C (100%)

✉  **LuckyAro** Highly Voted 9 months, 1 week ago

Selected Answer: C

Quote types need to be separated: SNS message filtering can be used to publish messages to the appropriate SQS queue based on the quote type, ensuring that quotes are separated by type.

Quotes must be responded to within 24 hours and must not get lost: SQS provides reliable and scalable queuing for messages, ensuring that quotes will not get lost and can be processed in a timely manner. Additionally, each backend application server can use its own SQS queue, ensuring that quotes are processed efficiently without any delay.

Operational efficiency and minimizing maintenance: Using a single SNS topic and multiple SQS queues is a scalable and cost-effective approach, which can help to maximize operational efficiency and minimize maintenance. Additionally, SNS and SQS are fully managed services, which means that the company will not need to worry about maintenance tasks such as software updates, hardware upgrades, or scaling the infrastructure.

upvoted 10 times

✉  **Vlad** Highly Voted 9 months, 2 weeks ago

C is the best option

upvoted 7 times

✉  **Ruffyit** Most Recent 2 weeks, 1 day ago

Quote types need to be separated: SNS message filtering can be used to publish messages to the appropriate SQS queue based on the quote type, ensuring that quotes are separated by type.

Quotes must be responded to within 24 hours and must not get lost: SQS provides reliable and scalable queuing for messages, ensuring that quotes will not get lost and can be processed in a timely manner. Additionally, each backend application server can use its own SQS queue, ensuring that quotes are processed efficiently without any delay.

Operational efficiency and minimizing maintenance: Using a single SNS topic and multiple SQS queues is a scalable and cost-effective approach, which can help to maximize operational efficiency and minimize maintenance. Additionally, SNS and SQS are fully managed services, which means that the company will not need to worry about maintenance tasks such as software updates, hardware upgrades, or scaling the

upvoted 1 times

✉  **tekjm** 1 month, 2 weeks ago

Keyword is "...and must not get lost" = SQS

upvoted 1 times

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

Selected Answer: C

Create a single SNS topic

Subscribe separate SQS queues per quote type

Use SNS message filtering to send messages to proper queue

Backend servers poll their respective SQS queue

The key points:

Quote requests must be processed within 24 hrs without loss

Need to maximize efficiency and minimize maintenance
Requests separated by quote type
upvoted 1 times

✉ **lexotan** 7 months, 1 week ago

Selected Answer: C

This wrong answers from examtopic are getting me so frustrated. Which one is the correct answer then?
upvoted 5 times

✉ **Steve_4542636** 9 months ago

Selected Answer: C

This is the SNS fan-out technique where you will have one SNS service to many SQS services
<https://docs.aws.amazon.com/sns/latest/dg/sns-sqs-as-subscriber.html>
upvoted 6 times

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

SNS Fan-out fans message to all subscribers, this uses SNS filtering to publish the message only to the right SQS queue (not all of them).
upvoted 1 times

✉ **Yechi** 9 months, 1 week ago

Selected Answer: C

<https://aws.amazon.com/getting-started/hands-on/filter-messages-published-to-topics/>
upvoted 6 times

A company has an application that runs on several Amazon EC2 instances. Each EC2 instance has multiple Amazon Elastic Block Store (Amazon EBS) data volumes attached to it. The application's EC2 instance configuration and data need to be backed up nightly. The application also needs to be recoverable in a different AWS Region.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Region.
- B. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region. Add the application's EC2 instances as resources.
- C. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region. Add the application's EBS volumes as resources.
- D. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Availability Zone.

Correct Answer: C

Community vote distribution

B (90%)	10%
---------	-----

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

B is answer so the requirement is "The application's EC2 instance configuration and data need to be backed up nightly" so we need "add the application's EC2 instances as resources". This option will backup both EC2 configuration and data
upvoted 12 times

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

Selected Answer: B

<https://aws.amazon.com/vi/blogs/aws/aws-backup-ec2-instances-efs-single-file-restore-and-cross-region-backup/>
When you back up an EC2 instance, AWS Backup will protect all EBS volumes attached to the instance, and it will attach them to an AMI that stores all parameters from the original EC2 instance except for two
upvoted 10 times

 **Ruffyit** Most Recent 2 weeks, 1 day ago

<https://aws.amazon.com/vi/blogs/aws/aws-backup-ec2-instances-efs-single-file-restore-and-cross-region-backup/>
When you back up an EC2 instance, AWS Backup will protect all EBS volumes attached to the instance, and it will attach them to an AMI that stores all parameters from the original EC2 instance except for two
upvoted 1 times

 **TariqKipkemei** 1 month, 3 weeks ago

Selected Answer: B

As part of configuring a backup plan you need to enable (opt-in) resource types that will be protected by the backup plan. For this case EC2.
<https://aws.amazon.com/getting-started/hands-on/amazon-ec2-backup-and-restore-using-aws-backup/#:~:text=the%20services%20used%20with-,AWS%20Backup,-a.%20In%20the%20navigation>
upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

B is the most appropriate solution because it allows you to create a backup plan to automate the backup process of EC2 instances and EBS volumes, and copy backups to another region. Additionally, you can add the application's EC2 instances as resources to ensure their configuration and data are backed up nightly.
upvoted 1 times

 **Geekboii** 8 months ago

i would say B
upvoted 1 times

 **Geekboii** 8 months ago

i would say B
upvoted 1 times

 **AlmeroSenior** 9 months, 1 week ago

Selected Answer: B

AWS KB states if you select the EC2 instance , associated EBS's will be auto covered .

<https://aws.amazon.com/blogs/aws/aws-backup-ec2-instances-efs-single-file-restore-and-cross-region-backup/>
upvoted 2 times

✉ **LuckyAro** 9 months, 1 week ago

Selected Answer: B

B is the most appropriate solution because it allows you to create a backup plan to automate the backup process of EC2 instances and EBS volumes, and copy backups to another region. Additionally, you can add the application's EC2 instances as resources to ensure their configuration and data are backed up nightly.

A and D involve writing custom Lambda functions to automate the snapshot process, which can be complex and require more maintenance effort. Moreover, these options do not provide an integrated solution for managing backups and recovery, and copying snapshots to another region.

Option C involves creating a backup plan with AWS Backup to perform backups for EBS volumes only. This approach would not back up the EC2 instances and their configuration

upvoted 2 times

✉ **Mia2009687** 4 months, 3 weeks ago

The data is stored in the EBS storage volume, EC2 won't hold the data, I think we need "Add the application's EBS volumes as resources."
upvoted 2 times

✉ **everfly** 9 months, 1 week ago

Selected Answer: C

The application's EC2 instance configuration and data are stored on EBS volume right?

upvoted 2 times

✉ **Rehan33** 9 months, 1 week ago

The data is store on EBS volume so why we are not using EBS as a source instead of EC2

upvoted 1 times

✉ **obatunde** 9 months, 1 week ago

Because "The application's EC2 instance configuration and data need to be backed up nightly"
upvoted 3 times

✉ **fulingyu288** 9 months, 1 week ago

Selected Answer: B

Use AWS Backup to create a backup plan that includes the EC2 instances, Amazon EBS snapshots, and any other resources needed for recovery. The backup plan can be configured to run on a nightly schedule.
upvoted 1 times

✉ **zTopic** 9 months, 1 week ago

Selected Answer: B

The application's EC2 instance configuration and data need to be backed up nightly >> B
upvoted 1 times

✉ **NolaHOla** 9 months, 1 week ago

But isn't the data needed to be backed up on the EBS ?
upvoted 1 times

A company is building a mobile app on AWS. The company wants to expand its reach to millions of users. The company needs to build a platform so that authorized users can watch the company's content on their mobile devices.

What should a solutions architect recommend to meet these requirements?

- A. Publish content to a public Amazon S3 bucket. Use AWS Key Management Service (AWS KMS) keys to stream content.
- B. Set up IPsec VPN between the mobile app and the AWS environment to stream content.
- C. Use Amazon CloudFront. Provide signed URLs to stream content.
- D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Steve_4542636** Highly Voted 9 months ago

Selected Answer: C

Enough with CloudFront already.

upvoted 16 times

✉  **TariqKipkemei** 7 months ago

Hahaha..cloudfront too hyped :)

upvoted 1 times

✉  **Ruffyt** Most Recent 2 weeks, 1 day ago

Use Amazon CloudFront. Provide signed URLs to stream content.

upvoted 1 times

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

Selected Answer: C

Use Amazon CloudFront. Provide signed URLs to stream content.

upvoted 1 times

✉  **antropaws** 6 months, 1 week ago

Selected Answer: C

C is correct.

upvoted 1 times

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

Cloudfront is the correct solution.

upvoted 2 times

✉  **datz** 8 months, 1 week ago

Feel your pain :D hahaha

upvoted 2 times

✉  **LuckyAro** 9 months, 1 week ago

Selected Answer: C

Amazon CloudFront is a content delivery network (CDN) that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. CloudFront supports signed URLs that provide authorized access to your content. This feature allows the company to control who can access their content and for how long, providing a secure and scalable solution for millions of users.

upvoted 4 times

✉  **jennyka76** 9 months, 1 week ago

C

<https://www.amazonaws.cn/en/cloudfront/>

upvoted 1 times

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.

Which service should a solutions architect recommend?

- A. Amazon Aurora MySQL
- B. Amazon Aurora Serverless for MySQL
- C. Amazon Redshift Spectrum
- D. Amazon RDS for MySQL

Correct Answer: B

Community vote distribution

B (100%)

 **cloudbusting** Highly Voted  9 months, 1 week ago
"without selecting a particular instance type" = serverless
upvoted 18 times

 **Ruffyit** Most Recent  2 weeks, 1 day ago
without selecting a particular instance type = Amazon Aurora Serverless for MySQL
upvoted 1 times

 **TariqKipkemei** 1 month, 3 weeks ago
Selected Answer: B
without selecting a particular instance type = Amazon Aurora Serverless for MySQL
upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago
Selected Answer: B
B. Amazon Aurora Serverless for MySQL
upvoted 1 times

 **Diqian** 3 months, 1 week ago
What's the difference between A and B. I think Aurora is serverless, isn't it?
upvoted 1 times

 **Valder21** 2 months, 3 weeks ago
seems serverless is an option of amazon aurora. Not a very good naming scheme.
upvoted 1 times

 **elearningtakai** 8 months ago
Selected Answer: B
With Aurora Serverless for MySQL, you don't need to select a particular instance type, as the service automatically scales up or down based on the application's needs.
upvoted 4 times

 **Srikanth0057** 8 months, 3 weeks ago
Selected Answer: B
Bbbbbbb
upvoted 1 times

 **Steve_4542636** 9 months ago
Selected Answer: B
<https://aws.amazon.com/rds/aurora/serverless/>
upvoted 1 times

 **LuckyAro** 9 months, 1 week ago
Selected Answer: B
Amazon Aurora Serverless for MySQL is a fully managed, auto-scaling relational database service that scales up or down automatically based on the application demand. This service provides all the capabilities of Amazon Aurora, such as high availability, durability, and security, without requiring the customer to provision any database instances.

With Amazon Aurora Serverless for MySQL, the sales team can enjoy minimal downtime since the database is designed to automatically scale to accommodate the increased traffic. Additionally, the service allows the customer to pay only for the capacity used, making it cost-effective for infrequent access patterns.

Amazon RDS for MySQL could also be an option, but it requires the customer to select an instance type, and the database administrator would need to monitor and adjust the instance size manually to accommodate the increasing traffic.

upvoted 2 times

 **Drayen25** 9 months, 1 week ago

Minimal downtime points directly to Aurora Serverless

upvoted 2 times

A company experienced a breach that affected several applications in its on-premises data center. The attacker took advantage of vulnerabilities in the custom applications that were running on the servers. The company is now migrating its applications to run on Amazon EC2 instances. The company wants to implement a solution that actively scans for vulnerabilities on the EC2 instances and sends a report that details the findings.

Which solution will meet these requirements?

- A. Deploy AWS Shield to scan the EC2 instances for vulnerabilities. Create an AWS Lambda function to log any findings to AWS CloudTrail.
- B. Deploy Amazon Macie and AWS Lambda functions to scan the EC2 instances for vulnerabilities. Log any findings to AWS CloudTrail.
- C. Turn on Amazon GuardDuty. Deploy the GuardDuty agents to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.
- D. Turn on Amazon Inspector. Deploy the Amazon Inspector agent to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.

Correct Answer: C

Community vote distribution

D (96%)	4%
---------	----

 **siyam008** Highly Voted 8 months, 4 weeks ago

Selected Answer: D

AWS Shield for DDOS
 Amazon Macie for discover and protect sensitive date
 Amazon GuardDuty for intelligent thread discovery to protect AWS account
 Amazon Inspector for automated security assessment. like known Vulnerability
 upvoted 36 times

 **Ruffyit** Most Recent 2 weeks, 1 day ago

AWS Shield for DDOS
 Amazon Macie for discover and protect sensitive date
 Amazon GuardDuty for intelligent thread discovery to protect AWS account
 Amazon Inspector for automated security assessment. like known Vulnerability
 upvoted 1 times

 **TariqKipkemei** 1 month, 3 weeks ago

Selected Answer: D

vulnerabilities = Amazon Inspector
 malicious activity = Amazon GuardDuty
 upvoted 2 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: D

Enable Amazon Inspector
 Deploy Inspector agents to EC2 instances
 Use Lambda to generate and distribute vulnerability reports
 The key points:

Migrate on-prem apps with vulnerabilities to EC2
 Need active scanning of EC2 instances for vulnerabilities
 Require reports on findings
 upvoted 2 times

 **kruasan** 7 months ago

Selected Answer: D

Amazon Inspector:
 • Performs active vulnerability scans of EC2 instances. It looks for software vulnerabilities, unintended network accessibility, and other security issues.
 • Requires installing an agent on EC2 instances to perform scans. The agent must be deployed to each instance.
 • Provides scheduled scan reports detailing any findings of security risks or vulnerabilities. These reports can be used to patch or remediate issues.
 • Is best suited for proactively detecting security weaknesses and misconfigurations in your AWS environment.
 upvoted 3 times

 **kruasan** 7 months ago

Amazon GuardDuty:

- Monitors for malicious activity like unusual API calls, unauthorized infrastructure deployments, or compromised EC2 instances. It uses machine learning and behavioral analysis of logs.

- Does not require installing any agents. It relies on analyzing AWS CloudTrail, VPC Flow Logs, and DNS logs.
 - Alerts you to any detected threats, suspicious activity or policy violations in your AWS accounts. These alerts warrant investigation but may not always require remediation.
 - Is focused on detecting active threats, unauthorized behavior, and signs of a compromise in your AWS environment.
 - Can also detect some vulnerabilities and misconfigurations but coverage is not as broad as a dedicated service like Inspector.
- upvoted 4 times

✉ **datz** 8 months, 1 week ago

Selected Answer: D

Amazon Inspector is a vulnerability scanning tool that you can use to identify potential security issues within your EC2 instances.

It is a kind of automated security assessment service that checks the network exposure of your EC2 or latest security state for applications running into your EC2 instance. It has ability to auto discover your AWS workload and continuously scan for the open loophole or vulnerability.

upvoted 1 times

✉ **shanwfard** 8 months, 1 week ago

Selected Answer: D

Amazon Inspector is a vulnerability scanning tool that you can use to identify potential security issues within your EC2 instances. Guard Duty continuously monitors your entire AWS account via Cloud Trail, Flow Logs, DNS Logs as Input.

upvoted 1 times

✉ **GalileoEC2** 8 months, 1 week ago

Selected Answer: C

:) C is the correct

<https://cloudkatha.com/amazon-guardduty-vs-inspector-which-one-should-you-use/>

upvoted 1 times

✉ **MssP** 8 months ago

Please, read the link you sent: Amazon Inspector is a vulnerability scanning tool that you can use to identify potential security issues within your EC2 instances. GuardDuty is very critical part to identify threats, based on that findings you can setup automated preventive actions or remediation's. So Answer is D.

upvoted 1 times

✉ **GalileoEC2** 8 months, 1 week ago

Selected Answer: C

<https://cloudkatha.com/amazon-guardduty-vs-inspector-which-one-should-you-use/>

upvoted 1 times

✉ **LuckyAro** 9 months, 1 week ago

Selected Answer: D

Amazon Inspector is a security assessment service that helps to identify security vulnerabilities and compliance issues in applications deployed on Amazon EC2 instances. It can be used to assess the security of applications that are deployed on Amazon EC2 instances, including those that are custom-built.

To use Amazon Inspector, the Amazon Inspector agent must be installed on the EC2 instances that need to be assessed. The agent collects data about the instances and sends it to Amazon Inspector for analysis. Amazon Inspector then generates a report that details any security vulnerabilities that were found and provides guidance on how to remediate them.

By configuring an AWS Lambda function, the company can automate the generation and distribution of reports that detail the findings. This means that reports can be generated and distributed as soon as vulnerabilities are detected, allowing the company to take action quickly.

upvoted 1 times

✉ **pbpally** 9 months, 1 week ago

Selected Answer: D

I'm a little confused on how someone came up with C, it is definitely D.

upvoted 1 times

✉ **obatunde** 9 months, 1 week ago

Selected Answer: D

Amazon Inspector

upvoted 2 times

✉ **obatunde** 9 months, 1 week ago

Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure. <https://aws.amazon.com/inspector/features/?nc=sn&loc=2>

upvoted 3 times

✉ **Palanda** 9 months, 1 week ago

Selected Answer: D

I think D

upvoted 1 times

✉ **minglu** 9 months, 1 week ago

Selected Answer: D

Inspector for EC2

upvoted 1 times

 **skiwili** 9 months, 1 week ago

Selected Answer: D

Ddddddd

upvoted 1 times

 **cloudbusting** 9 months, 1 week ago

this is inspector = <https://medium.com/aws-architech/use-case-aws-inspector-vs-guardduty-3662bf80767a>

upvoted 3 times

A company uses an Amazon EC2 instance to run a script to poll for and process messages in an Amazon Simple Queue Service (Amazon SQS) queue. The company wants to reduce operational costs while maintaining its ability to process a growing number of messages that are added to the queue.

What should a solutions architect recommend to meet these requirements?

- A. Increase the size of the EC2 instance to process messages faster.
- B. Use Amazon EventBridge to turn off the EC2 instance when the instance is underutilized.
- C. Migrate the script on the EC2 instance to an AWS Lambda function with the appropriate runtime.
- D. Use AWS Systems Manager Run Command to run the script on demand.

Correct Answer: A

Community vote distribution

C (89%) 11%

 **kpato87** Highly Voted 9 months, 1 week ago

Selected Answer: C

By migrating the script to AWS Lambda, the company can take advantage of the auto-scaling feature of the service. AWS Lambda will automatically scale resources to match the size of the workload. This means that the company will not have to worry about provisioning or managing instances as the number of messages increases, resulting in lower operational costs

upvoted 6 times

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

Selected Answer: C

reduce operational costs = serverless = Lambda functions

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: C

The key points are:

Currently using an EC2 instance to poll SQS and process messages

Want to reduce costs while handling growing message volume

By migrating the polling script to a Lambda function, the company can avoid the cost of running a dedicated EC2 instance. Lambda functions scale automatically to handle message spikes. And Lambda billing is based on actual usage, resulting in cost savings versus provisioned EC2 capacity.

upvoted 3 times

 **Steve_4542636** 9 months ago

Selected Answer: C

Lambda costs money only when it's processing, not when idle

upvoted 2 times

 **ManOnTheMoon** 9 months, 1 week ago

Agree with C

upvoted 1 times

 **khasport** 9 months, 1 week ago

the answer is C. With this option, you can reduce operational cost as the question mentioned

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: C

AWS Lambda is a serverless compute service that allows you to run your code without provisioning or managing servers. By migrating the script to an AWS Lambda function, you can eliminate the need to maintain an EC2 instance, reducing operational costs. Additionally, Lambda automatically scales to handle the increasing number of messages in the SQS queue.

upvoted 1 times

 **zTopic** 9 months, 2 weeks ago

Selected Answer: C

It Should be C.

Lambda allows you to execute code without provisioning or managing servers, so it is ideal for running scripts that poll for and process messages in an Amazon SQS queue. The scaling of the Lambda function is automatic, and you only pay for the actual time it takes to process the messages.

upvoted 3 times

 **Bhawesh** 9 months, 2 weeks ago

Selected Answer: D

To reduce the operational overhead, it should be:

D. Use AWS Systems Manager Run Command to run the script on demand.

upvoted 2 times

 **lucdt4** 6 months, 1 week ago

No, replace EC2 instead by using lambda to reduce costs

upvoted 1 times

A company uses a legacy application to produce data in CSV format. The legacy application stores the output data in Amazon S3. The company is deploying a new commercial off-the-shelf (COTS) application that can perform complex SQL queries to analyze data that is stored in Amazon Redshift and Amazon S3 only. However, the COTS application cannot process the .csv files that the legacy application produces.

The company cannot update the legacy application to produce data in another format. The company needs to implement a solution so that the COTS application can use the data that the legacy application produces.

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

- A. Create an AWS Glue extract, transform, and load (ETL) job that runs on a schedule. Configure the ETL job to process the .csv files and store the processed data in Amazon Redshift.
- B. Develop a Python script that runs on Amazon EC2 instances to convert the .csv files to .sql files. Invoke the Python script on a cron schedule to store the output files in Amazon S3.
- C. Create an AWS Lambda function and an Amazon DynamoDB table. Use an S3 event to invoke the Lambda function. Configure the Lambda function to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in the DynamoDB table.
- D. Use Amazon EventBridge to launch an Amazon EMR cluster on a weekly schedule. Configure the EMR cluster to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in an Amazon Redshift table.

Correct Answer: A

Community vote distribution

A (92%) 8%

 **Ruffyit** 2 weeks, 1 day ago

A-ETL is serverless & best suited with the requirement who primary job is ETL
B-Usage of Ec2 adds operational overhead & incur costs
C-DynamoDB(NoSql) does suit the requirement as company is performing SQL queries
D-EMR adds operational overhead & incur costs
upvoted 1 times

 **ACloud_Guru15** 2 weeks, 6 days ago

Selected Answer: A
A-ETL is serverless & best suited with the requirement who primary job is ETL
B-Usage of Ec2 adds operational overhead & incur costs
C-DynamoDB(NoSql) does suit the requirement as company is performing SQL queries
D-EMR adds operational overhead & incur costs
upvoted 1 times

 **TariqKipkemei** 1 month, 3 weeks ago

Selected Answer: A
Data transformation = AWS Glue
upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: A
Create an AWS Glue ETL job to process the CSV files
Configure the job to run on a schedule
Output the transformed data to Amazon Redshift
The key points:

Legacy app generates CSV files in S3
New app requires data in Redshift or S3
Need to transform CSV to support new app with minimal ops overhead
upvoted 1 times

 **kraken21** 8 months ago

Selected Answer: A
Glue is server less and has less operational head than EMR so A.
upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: A

A, AWS Glue is a fully managed ETL service that can extract data from various sources, transform it into the required format, and load it into a target data store. In this case, the ETL job can be configured to read the CSV files from Amazon S3, transform the data into a format that can be loaded into Amazon Redshift, and load it into an Amazon Redshift table.

B requires the development of a custom script to convert the CSV files to SQL files, which could be time-consuming and introduce additional operational overhead. C, while using serverless technology, requires the additional use of DynamoDB to store the processed data, which may not be necessary if the data is only needed in Amazon Redshift. D, while an option, is not the most efficient solution as it requires the creation of an EMR cluster, which can be costly and complex to manage.

upvoted 4 times

 **dcp** 8 months, 2 weeks ago

Selected Answer: C

To meet the requirement with the least operational overhead, a serverless approach should be used. Among the options provided, option C provides a serverless solution using AWS Lambda, S3, and DynamoDB. Therefore, the solution should be to create an AWS Lambda function and an Amazon DynamoDB table. Use an S3 event to invoke the Lambda function. Configure the Lambda function to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in the DynamoDB table.

Option A is also a valid solution, but it may involve more operational overhead than Option C. With Option A, you would need to set up and manage an AWS Glue job, which would require more setup time than creating an AWS Lambda function. Additionally, AWS Glue jobs have a minimum execution time of 10 minutes, which may not be necessary or desirable for this use case. However, if the data processing is particularly complex or requires a lot of data transformation, AWS Glue may be a more appropriate solution.

upvoted 1 times

 **MssP** 8 months, 1 week ago

Important point: The COTS performs complex SQL queries to analyze data in Amazon Redshift. If you use DynamoDB -> No SQL queries. Option A makes more sense.

upvoted 3 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: A

A would be the best solution as it involves the least operational overhead. With this solution, an AWS Glue ETL job is created to process the .csv files and store the processed data directly in Amazon Redshift. This is a serverless approach that does not require any infrastructure to be provisioned, configured, or maintained. AWS Glue provides a fully managed, pay-as-you-go ETL service that can be easily configured to process data from S3 and load it into Amazon Redshift. This approach allows the legacy application to continue to produce data in the CSV format that it currently uses, while providing the new COTS application with the ability to analyze the data using complex SQL queries.

upvoted 3 times

 **jennyka76** 9 months, 1 week ago

A

<https://docs.aws.amazon.com/glue/latest/dg/aws-glue-programming-etl-format-csv-home.html>

I AGREE AFTER READING LINK

upvoted 1 times

 **cloudbusting** 9 months, 1 week ago

A: <https://docs.aws.amazon.com/glue/latest/dg/aws-glue-programming-etl-format.html>

upvoted 1 times

A company recently migrated its entire IT environment to the AWS Cloud. The company discovers that users are provisioning oversized Amazon EC2 instances and modifying security group rules without using the appropriate change control process. A solutions architect must devise a strategy to track and audit these inventory and configuration changes.

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

- A. Enable AWS CloudTrail and use it for auditing.
- B. Use data lifecycle policies for the Amazon EC2 instances.
- C. Enable AWS Trusted Advisor and reference the security dashboard.
- D. Enable AWS Config and create rules for auditing and compliance purposes.
- E. Restore previous resource configurations with an AWS CloudFormation template.

Correct Answer: AD

Community vote distribution

AD (92%)	8%
----------	----

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

Selected Answer: AD

- A. Enable AWS CloudTrail and use it for auditing. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and APIs. By enabling CloudTrail, the company can track user activity and changes to AWS resources, and monitor compliance with internal policies and external regulations.
- D. Enable AWS Config and create rules for auditing and compliance purposes. AWS Config provides a detailed inventory of the AWS resources in your account, and continuously records changes to the configurations of those resources. By creating rules in AWS Config, the company can automate the evaluation of resource configurations against desired state, and receive alerts when configurations drift from compliance.

Options B, C, and E are not directly relevant to the requirement of tracking and auditing inventory and configuration changes.
upvoted 8 times

 **Ruffyit** Most Recent 2 weeks, 1 day ago

- A. Enable AWS CloudTrail and use it for auditing. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and APIs. By enabling CloudTrail, the company can track user activity and changes to AWS resources, and monitor compliance with internal policies and external regulations.
- D. Enable AWS Config and create rules for auditing and compliance purposes. AWS Config provides a detailed inventory of the AWS resources in your account, and continuously records changes to the configurations of those resources. By creating rules in AWS Config, the company can automate the evaluation of resource configurations against desired state, and receive alerts when configurations drift from compliance.

Options B, C, and E are not directly relevant to the requirement of tracking and auditing inventory and configuration changes.
upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: AD

- A. Enable AWS CloudTrail and use it for auditing. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and APIs. By enabling CloudTrail, the company can track user activity and changes to AWS resources, and monitor compliance with internal policies and external regulations.
- D. Enable AWS Config and create rules for auditing and compliance purposes. AWS Config provides a detailed inventory of the AWS resources in your account, and continuously records changes to the configurations of those resources. By creating rules in AWS Config, the company can automate the evaluation of resource configurations against desired state, and receive alerts when configurations drift from compliance.

upvoted 1 times

 **mrsoa** 4 months ago

Selected Answer: CD

I am gonna go with CD
AWS Cloudtrail is already enabled so no need to enable it and for the auditing we are gonna use AWS config Answer D

C because Trusted advisor checks the security groups
upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: AD

A) Enable AWS CloudTrail and use it for auditing.
AWS CloudTrail provides a record of API calls and can be used to audit changes made to EC2 instances and security groups. By analyzing CloudTrail

logs, the solutions architect can track who provisioned oversized instances or modified security groups without proper approval.

D) Enable AWS Config and create rules for auditing and compliance purposes.

AWS Config can record the configuration changes made to resources like EC2 instances and security groups. The solutions architect can create AWS Config rules to monitor for non-compliant changes, like launching certain instance types or opening security group ports without permission. AWS Config would alert on any violations of these rules.

upvoted 2 times

✉️  **kruasan** 7 months ago

The other options would not fully meet the auditing and change tracking requirements:

B) Data lifecycle policies control when EC2 instances are backed up or deleted but do not audit configuration changes.

C) AWS Trusted Advisor security checks may detect some compliance violations after the fact but do not comprehensively log changes like AWS CloudTrail and AWS Config do.

E) CloudFormation templates enable rollback but do not provide an audit trail of changes. The solutions architect would not know who made unauthorized modifications in the first place.

upvoted 2 times

✉️  **skiwili** 9 months, 1 week ago

Selected Answer: AD

Yes A and D

upvoted 1 times

✉️  **jennyka76** 9 months, 1 week ago

AGREE WITH ANSWER - A & D

CloudTrail and Config

upvoted 1 times

✉️  **Neha999** 9 months, 1 week ago

CloudTrail and Config

upvoted 2 times

A company has hundreds of Amazon EC2 Linux-based instances in the AWS Cloud. Systems administrators have used shared SSH keys to manage the instances. After a recent audit, the company's security team is mandating the removal of all shared keys. A solutions architect must design a solution that provides secure access to the EC2 instances.

Which solution will meet this requirement with the LEAST amount of administrative overhead?

- A. Use AWS Systems Manager Session Manager to connect to the EC2 instances.
- B. Use AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand.
- C. Allow shared SSH access to a set of bastion instances. Configure all other instances to allow only SSH access from the bastion instances.
- D. Use an Amazon Cognito custom authorizer to authenticate users. Invoke an AWS Lambda function to generate a temporary SSH key.

Correct Answer: B

Community vote distribution

A (75%)	13%	13%
---------	-----	-----

✉️ **Ruffyit** 2 weeks, 1 day ago

The key reasons why:

STS can generate short-lived credentials that provide temporary access to the EC2 instances for administering them. The credentials can be generated on-demand each time access is needed, eliminating the risks of using permanent shared SSH keys. No infrastructure like bastion hosts needs to be maintained. The on-premises administrators can use the familiar SSH tools with the temporary keys.

upvoted 1 times

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

Selected Answer: A

Session Manager provides secure and auditable node management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.

upvoted 1 times

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

Selected Answer: B

The key reasons why:

STS can generate short-lived credentials that provide temporary access to the EC2 instances for administering them. The credentials can be generated on-demand each time access is needed, eliminating the risks of using permanent shared SSH keys. No infrastructure like bastion hosts needs to be maintained. The on-premises administrators can use the familiar SSH tools with the temporary keys.

upvoted 1 times

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

Selected Answer: B

Using AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand is a secure and efficient way to provide access to the EC2 instances without the need for shared SSH keys. STS is a fully managed service that can be used to generate temporary security credentials, allowing systems administrators to connect to the EC2 instances without having to share SSH keys. The temporary credentials can be generated on demand, reducing the administrative overhead associated with managing SSH access

upvoted 1 times

✉️ **ofinto** 2 months, 1 week ago

Can you please provide documentation about generating a one-time SSH with STS?

upvoted 1 times

✉️ **kruasan** 7 months ago

Selected Answer: A

AWS Systems Manager Session Manager provides secure shell access to EC2 instances without the need for SSH keys. It meets the security requirement to remove shared SSH keys while minimizing administrative overhead.

upvoted 1 times

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

If the systems administrators need to access the EC2 instances from an on-premises environment, using Session Manager may not be the ideal solution.

upvoted 1 times

✉️ **kruasan** 7 months ago

Session Manager is a fully managed AWS Systems Manager capability. With 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). Session Manager provides secure and auditable node management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager also allows you to comply with corporate policies that require controlled access to managed nodes, strict security practices, and fully auditable logs with node access details, while providing end users with simple one-click cross-platform access to your managed nodes.

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

upvoted 2 times

✉ **kruasan** 7 months ago

Who should use Session Manager?

Any AWS customer who wants to improve their security and audit posture, reduce operational overhead by centralizing access control on managed nodes, and reduce inbound node access.

Information Security experts who want to monitor and track managed node access and activity, close down inbound ports on managed nodes, or allow connections to managed nodes that don't have a public IP address.

Administrators who want to grant and revoke access from a single location, and who want to provide one solution to users for Linux, macOS, and Windows Server managed nodes.

Users who want to connect to a managed node with just one click from the browser or AWS CLI without having to provide SSH keys.

upvoted 2 times

✉ **Stanislav4907** 8 months, 2 weeks ago

Selected Answer: C

You guys seriously don't want to go to SMSM for Avery Single EC2. You have to create solution not used services for one time access. Bastion will give you option to manage 1000s EC2 machines from 1. Plus you can use Ansible from it.

upvoted 2 times

✉ **Zox42** 8 months, 1 week ago

Question:" the company's security team is mandating the removal of all shared keys", answer C can't be right because it says:"Allow shared SSH access to a set of bastion instances".

upvoted 5 times

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

Session Manager is the best practice and recommended way by Amazon to manage your instances.
Bastion hosts require remote access therefore exposing them to the internet.

The most secure way is definitely session manager therefore answer A is correct imho.

upvoted 2 times

✉ **Steve_4542636** 9 months ago

Selected Answer: A

I vote a

upvoted 1 times

✉ **LuckyAro** 9 months, 1 week ago

Selected Answer: A

AWS Systems Manager Session Manager provides secure and auditable instance management without the need for any inbound connections or open ports. It allows you to manage your instances through an interactive one-click browser-based shell or through the AWS CLI. This means that you don't have to manage any SSH keys, and you don't have to worry about securing access to your instances as access is controlled through IAM policies.

upvoted 3 times

✉ **bdp123** 9 months, 1 week ago

Selected Answer: A

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

upvoted 2 times

✉ **jahmad0730** 9 months, 1 week ago

Selected Answer: A

Answer must be A

upvoted 2 times

✉ **jennyka76** 9 months, 1 week ago

ANSWER - A

AWS SESSION MANAGER IS CORRECT LEAST EFFORTS TO ACCESS LINUX SYSTEM IN AWS CONSOLE AND YOUR ARE ALREAADY LOGIN TO AWS.
SO NO NEED FOR THE TOKEN OR OTHER STUFF DONE IN THE BACKGROUND BY AWS. MAKES SENESE.

upvoted 2 times

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

Answer is A

upvoted 3 times

✉ **zTopic** 9 months, 2 weeks ago

Selected Answer: A

Answer is A

upvoted 2 times

 **Vlad** 9 months, 2 weeks ago

Answer is A

Using AWS Systems Manager Session Manager to connect to the EC2 instances is a secure option as it eliminates the need for inbound SSH ports and removes the requirement to manage SSH keys manually. It also provides a complete audit trail of user activity. This solution requires no additional software to be installed on the EC2 instances.

upvoted 4 times

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query ingested data in near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

- A. Publish data to Amazon Kinesis Data Streams, Use Kinesis Data Analytics to query the data.
- B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
- C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
- D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

Correct Answer: A

Community vote distribution

A (88%)	13%
---------	-----

 **LuckyAro**  9 months, 1 week ago

Selected Answer: A

A: is the solution for the company's requirements. Publishing data to Amazon Kinesis Data Streams can support ingestion rates as high as 1 MB/s and provide real-time data processing. Kinesis Data Analytics can query the ingested data in real-time with low latency, and the solution can scale as needed to accommodate increases in ingestion rates or querying needs. This solution also ensures minimal data loss in the event of an EC2 instance reboot since Kinesis Data Streams has a persistent data store for up to 7 days by default.

upvoted 11 times

 **bogobob**  1 week, 6 days ago

Selected Answer: B

The fact they specifically mention "near real-time" twice tells me the correct answer is KDF. On top of which its easier to setup and maintain. KDS is really only needed if you need real-time. Also using redshift will mean permanent data retention. The data in A could be lost after a year. Redshift queries are slow but you're still querying near real-time data

upvoted 1 times

 **practice_makes_perfect** 2 weeks, 1 day ago

Selected Answer: B

A is not correct because Kinesis can only store data up to 1 year. The solution need to support querying ALL data instead of "recent" data.

upvoted 1 times

 **Ruffyit** 2 weeks, 1 day ago

A: is the solution for the company's requirements. Publishing data to Amazon Kinesis Data Streams can support ingestion rates as high as 1 MB/s and provide real-time data processing. Kinesis Data Analytics can query the ingested data in real-time with low latency, and the solution can scale as needed to accommodate increases in ingestion rates or querying needs. This solution also ensures minimal data loss in the event of an EC2 instance reboot since Kinesis Data Streams has a persistent data store for up to 7 days by default.

upvoted 1 times

 **TariqKipkemei** 1 month, 3 weeks ago

Selected Answer: A

Publish data to Amazon Kinesis Data Streams, Use Kinesis Data Analytics to query the data

upvoted 2 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: A

- Provide near-real-time data ingestion into Kinesis Data Streams with the ability to handle the 1 MB/s ingestion rate. Data would be stored redundantly across shards.
- Enable near-real-time querying of the data using Kinesis Data Analytics. SQL queries can be run directly against the Kinesis data stream.
- Minimize data loss since data is replicated across shards. If an EC2 instance is rebooted, the data stream is still accessible.
- Scale seamlessly to handle varying ingestion and query rates.

upvoted 3 times

 **Nikki013** 3 months ago

Selected Answer: A

Answer is A as it will provide a more streamlined solution.

Using B (Firehose + Redshift) will involve sending the data to an S3 bucket first and then copying the data to Redshift which will take more time.
<https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html>

upvoted 2 times

✉  **nublit** 6 months ago

Selected Answer: B

Amazon Kinesis Data Firehose can deliver data in real-time to Amazon Redshift, making it immediately available for queries. Amazon Redshift, on the other hand, is a powerful data analytics service that allows fast and scalable querying of large volumes of data.

upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: A

- Provide near-real-time data ingestion into Kinesis Data Streams with the ability to handle the 1 MB/s ingestion rate. Data would be stored redundantly across shards.
- Enable near-real-time querying of the data using Kinesis Data Analytics. SQL queries can be run directly against the Kinesis data stream.
- Minimize data loss since data is replicated across shards. If an EC2 instance is rebooted, the data stream is still accessible.
- Scale seamlessly to handle varying ingestion and query rates.

upvoted 2 times

✉  **kruasan** 7 months ago

The other options would not fully meet the requirements:

- B) Kinesis Firehose + Redshift would introduce latency since data must be loaded from Firehose into Redshift before querying. Redshift would lack real-time capabilities.
- C) An EC2 instance store and Kinesis Firehose to S3 with Athena querying would risk data loss from instance store if an instance reboots. Athena querying data in S3 also lacks real-time capabilities.
- D) Using EBS storage, Kinesis Firehose to Redis and subscribing to Redis may provide near-real-time ingestion and querying but risks data loss if an EBS volume or EC2 instance fails. Recovery requires re-hydrating data from a backup which impacts real-time needs.

upvoted 4 times

✉  **joechen2023** 5 months, 2 weeks ago

I voted A as well, although not 100% sure why B is not correct. I just selected what seems the most simple solution between A and B.

Reason Kruasan gave "Redshift would lack real-time capabilities." This is not true. Redshift could do real-time. evidence

<https://aws.amazon.com/blogs/big-data/real-time-analytics-with-amazon-redshift-streaming-ingestion/>

upvoted 1 times

✉  **jennyka76** 9 months, 1 week ago

ANSWER - A

<https://docs.aws.amazon.com/kinesisanalytics/latest/dev/what-is.html>

upvoted 1 times

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

near-real-time data querying = Kinesis analytics

upvoted 3 times

✉  **zTopic** 9 months, 2 weeks ago

Selected Answer: A

Answer is A

upvoted 1 times

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

- A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.
- B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.
- C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.
- D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

Correct Answer: D

Community vote distribution

D (100%)

 **bdp123** Highly Voted 9 months, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/#:~:text=Solution%20overview>
upvoted 6 times

 **Grace83** 8 months, 1 week ago

Thank you!

upvoted 1 times

 **Guru4Cloud** Most Recent 2 months, 3 weeks ago

Selected Answer: D

The x-amz-server-side-encryption header is used to specify the encryption method that should be used to encrypt objects uploaded to an Amazon S3 bucket. By updating the bucket policy to deny if the PutObject does not have this header set, the solutions architect can ensure that all objects uploaded to the bucket are encrypted.

upvoted 2 times

 **kruasan** 7 months ago

To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS. The following code example shows a Put request using SSE-S3.

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/>

upvoted 3 times

 **kruasan** 7 months ago

The other options would not enforce encryption:

A) Requiring an s3:x-amz-acl header does not mandate encryption. This header controls access permissions.

B) Requiring an s3:x-amz-acl header set to private also does not enforce encryption. It only enforces private access permissions.

C) Requiring an aws:SecureTransport header ensures uploads use SSL but does not specify that objects must be encrypted. Encryption is not required when using SSL transport.

upvoted 3 times

 **kruasan** 7 months ago

Selected Answer: D

To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS. The following code example shows a Put request using SSE-S3.

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/>

upvoted 1 times

 **Sbbh** 8 months, 1 week ago

Confusing question. It doesn't state clearly if the object needs to be encrypted at-rest or in-transit

upvoted 3 times

 **Guru4Cloud** 2 months, 3 weeks ago

That's true

upvoted 1 times

 **Steve_4542636** 9 months ago

Selected Answer: D

I vote d

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: D

To ensure that all objects uploaded to an Amazon S3 bucket are encrypted, the solutions architect should update the bucket policy to deny any PutObject requests that do not have an x-amz-server-side-encryption header set. This will prevent any objects from being uploaded to the bucket unless they are encrypted using server-side encryption.

upvoted 3 times

 **jennyka76** 9 months, 1 week ago

answer - D

upvoted 1 times

 **zTopic** 9 months, 2 weeks ago

Selected Answer: D

Answer is D

upvoted 1 times

 **Neorem** 9 months, 2 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/amazon-s3-policy-keys.html>

upvoted 1 times

A solutions architect is designing a multi-tier application for a company. The application's users upload images from a mobile device. The application generates a thumbnail of each image and returns a message to the user to confirm that the image was uploaded successfully.

The thumbnail generation can take up to 60 seconds, but the company wants to provide a faster response time to its users to notify them that the original image was received. The solutions architect must design the application to asynchronously dispatch requests to the different application tiers.

What should the solutions architect do to meet these requirements?

- A. Write a custom AWS Lambda function to generate the thumbnail and alert the user. Use the image upload process as an event source to invoke the Lambda function.
- B. Create an AWS Step Functions workflow. Configure Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete.
- C. Create an Amazon Simple Queue Service (Amazon SQS) message queue. As images are uploaded, place a message on the SQS queue for thumbnail generation. Alert the user through an application message that the image was received.
- D. Create Amazon Simple Notification Service (Amazon SNS) notification topics and subscriptions. Use one subscription with the application to generate the thumbnail after the image upload is complete. Use a second subscription to message the user's mobile app by way of a push notification after thumbnail generation is complete.

Correct Answer: C

Community vote distribution

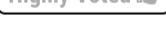
C (89%) 11%

✉  **Steve_4542636**  9 months ago

Selected Answer: C

I've noticed there are a lot of questions about decoupling services and SQS is almost always the answer.

upvoted 14 times

✉  **Neha999**  9 months, 1 week ago

D

SNS fan out

upvoted 11 times

✉  **wsdasdasdqwdaw**  1 month, 1 week ago

... asynchronously dispatch ... => Amazon SQS

upvoted 1 times

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

Selected Answer: C

Asynchronous, Decoupling = Amazon Simple Queue Service

upvoted 1 times

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

Selected Answer: C

SQS is a fully managed message queuing service that can be used to decouple different parts of an application.

upvoted 1 times

✉  **Zox42** 8 months, 1 week ago

Selected Answer: C

Answers B and D alert the user when thumbnail generation is complete. Answer C alerts the user through an application message that the image was received.

upvoted 3 times

✉  **Sbbh** 8 months, 1 week ago

B:

Use cases for Step Functions vary widely, from orchestrating serverless microservices, to building data-processing pipelines, to defining a security-incident response. As mentioned above, Step Functions may be used for synchronous and asynchronous business processes.

upvoted 1 times

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

why not B?

upvoted 4 times

✉ **Wael216** 9 months ago

Selected Answer: C

Creating an Amazon Simple Queue Service (SQS) message queue and placing messages on the queue for thumbnail generation can help separate the image upload and thumbnail generation processes.

upvoted 1 times

✉ **vindahake** 9 months ago

C

The key here is "a faster response time to its users to notify them that the original image was received." i.e user needs to be notified when image was received and not after thumbnail was created.

upvoted 2 times

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

Selected Answer: C

A looks like the best way , but its essentially replacing the mentioned app , that's not the ask

upvoted 1 times

✉ **Mickey321** 9 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/lambda/latest/dg/with-s3-tutorial.html>

upvoted 1 times

✉ **bdp123** 9 months, 1 week ago

Selected Answer: C

C is the only one that makes sense

upvoted 1 times

✉ **LuckyAro** 9 months, 1 week ago

Selected Answer: A

Use a custom AWS Lambda function to generate the thumbnail and alert the user. Lambda functions are well-suited for short-lived, stateless operations like generating thumbnails, and they can be triggered by various events, including image uploads. By using Lambda, the application can quickly confirm that the image was uploaded successfully and then asynchronously generate the thumbnail. When the thumbnail is generated, the Lambda function can send a message to the user to confirm that the thumbnail is ready.

C proposes to use an Amazon Simple Queue Service (Amazon SQS) message queue to process image uploads and generate thumbnails. SQS can help decouple the image upload process from the thumbnail generation process, which is helpful for asynchronous processing. However, it may not be the most suitable option for quickly alerting the user that the image was received, as the user may have to wait until the thumbnail is generated before receiving a notification.

upvoted 2 times

✉ **Bhrino** 9 months, 1 week ago

Selected Answer: A

This is A because SNS and SQS dont work because it can take up to 60 seconds and b is just more complex than a

upvoted 1 times

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

Does Lambda not time out after 15 seconds?

upvoted 1 times

✉ **MssP** 8 months ago

15 min.

upvoted 1 times

✉ **jennyka76** 9 months, 1 week ago

answer - c

upvoted 1 times

✉ **rrharris** 9 months, 1 week ago

Answer is C

upvoted 1 times

A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze.

Which system architecture should the solutions architect recommend?

- A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.
- B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Correct Answer: B

Community vote distribution

B (100%)

✉  **kruasan**  7 months ago

Selected Answer: B

- Option A would not provide high availability. A single EC2 instance is a single point of failure.
- Option B provides a scalable, highly available solution using serverless services. API Gateway and Lambda can scale automatically, and DynamoDB provides a durable data store.
- Option C would expose the Lambda function directly to the public Internet, which is not a recommended architecture. API Gateway provides an abstraction layer and additional features like access control.
- Option D requires configuring a VPN to AWS which adds complexity. It also saves the raw sensor data to S3, rather than processing it and storing the results.

upvoted 8 times

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

Selected Answer: B

Highly available = Serverless

The readers send a message over HTTPS = HTTPS endpoint in Amazon API Gateway

Process these messages from the sensors = AWS Lambda function

upvoted 1 times

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

Selected Answer: B

The correct answer is B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.

Here are the reasons why:

API Gateway is a highly scalable and available service that can be used to create and expose RESTful APIs.

Lambda is a serverless compute service that can be used to process events and data.

DynamoDB is a NoSQL database that can be used to store data in a scalable and highly available way.

upvoted 3 times

✉  **Steve_4542636** 9 months ago

Selected Answer: B

I vote B

upvoted 1 times

✉  **KZM** 9 months, 1 week ago

It is option "B"

Option "B" can provide a system with highly scalable, fault-tolerant, and easy to manage.

upvoted 1 times

✉  **LuckyAro** 9 months, 1 week ago

Selected Answer: B

Deploy Amazon API Gateway as an HTTPS endpoint and AWS Lambda to process and save the messages to an Amazon DynamoDB table. This option provides a highly available and scalable solution that can easily handle large amounts of data. It also integrates with other AWS services, making it easier to analyze and visualize the data for the security team.

upvoted 3 times

 **zTopic** 9 months, 2 weeks ago

Selected Answer: B

B is Correct

upvoted 3 times

A company wants to implement a disaster recovery plan for its primary on-premises file storage volume. The file storage volume is mounted from an Internet Small Computer Systems Interface (iSCSI) device on a local storage server. The file storage volume holds hundreds of terabytes (TB) of data.

The company wants to ensure that end users retain immediate access to all file types from the on-premises systems without experiencing latency.

Which solution will meet these requirements with the LEAST amount of change to the company's existing infrastructure?

- A. Provision an Amazon S3 File Gateway as a virtual machine (VM) that is hosted on premises. Set the local cache to 10 TB. Modify existing applications to access the files through the NFS protocol. To recover from a disaster, provision an Amazon EC2 instance and mount the S3 bucket that contains the files.
- B. Provision an AWS Storage Gateway tape gateway. Use a data backup solution to back up all existing data to a virtual tape library. Configure the data backup solution to run nightly after the initial backup is complete. To recover from a disaster, provision an Amazon EC2 instance and restore the data to an Amazon Elastic Block Store (Amazon EBS) volume from the volumes in the virtual tape library.
- C. Provision an AWS Storage Gateway Volume Gateway cached volume. Set the local cache to 10 TB. Mount the Volume Gateway cached volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.
- D. Provision an AWS Storage Gateway Volume Gateway stored volume with the same amount of disk space as the existing file storage volume. Mount the Volume Gateway stored volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

Correct Answer: C*Community vote distribution*

D (73%)

C (27%)

✉️  Grace83  8 months, 1 week ago

D is the correct answer

Volume Gateway CACHED Vs STORED

Cached = stores a subset of frequently accessed data locally

Stored = Retains the ENTIRE ("all file types") in on prem data centre

upvoted 13 times

✉️  daniel1  1 month, 1 week ago

Selected Answer: C

From chatGPT4

Considering the requirements of minimal infrastructure change, immediate file access, and low-latency, Option C: Provisioning an AWS Storage Gateway Volume Gateway (cached volume) with a 10 TB local cache, seems to be the most fitting solution. This setup aligns with the existing iSCSI setup and provides a local cache for low-latency access, while also configuring scheduled snapshots for disaster recovery. In the event of a disaster, restoring a snapshot to an Amazon EBS volume and attaching it to an Amazon EC2 instance as described in this option would align with the recovery objective.

upvoted 1 times

✉️  TariqKipkemei 1 month, 2 weeks ago

Selected Answer: D

End users retain immediate access to all file types = Volume Gateway stored volume

upvoted 1 times

✉️  netcj 2 months, 2 weeks ago

Selected Answer: D

"users retain immediate access to all file types"

immediate cannot be cached -> D

upvoted 1 times

✉️  Guru4Cloud 2 months, 3 weeks ago

Selected Answer: D

ddddddd

upvoted 2 times

 **alexandercamachop** 6 months ago

Selected Answer: D

Correct answer is Volume Gateway Stored which keeps all data on premises.

To have immediate access to the data. Cached is for frequently accessed data only.

upvoted 1 times

 **omoakin** 6 months ago

CCCCCCCCCC

upvoted 1 times

 **lucdt4** 6 months, 1 week ago

Selected Answer: D

D is the correct answer

Volume Gateway CACHED Vs STORED

Cached = stores a data recently at local

Stored = Retains the ENTIRE ("all file types") in on prem data centre

upvoted 1 times

 **rushi0611** 6 months, 3 weeks ago

Selected Answer: D

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access.

In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

Reference: <https://aws.amazon.com/storagegateway/faqs/>

Good luck.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: D

It is stated the company wants to keep the data locally and have DR plan in cloud. It points directly to the volume gateway

upvoted 1 times

 **UnluckyDucky** 8 months, 2 weeks ago

Selected Answer: D

"The company wants to ensure that end users retain immediate access to all file types from the on-premises systems "

D is the correct answer.

upvoted 2 times

 **CapJackSparrow** 8 months, 2 weeks ago

Selected Answer: C

all file types, NOT all files. Volume mode can not cache 100TBs.

upvoted 2 times

 **eddie5049** 6 months, 3 weeks ago

<https://docs.aws.amazon.com/storagegateway/latest/vgw/StorageGatewayConcepts.html>

Stored volumes can range from 1 GiB to 16 TiB in size and must be rounded to the nearest GiB. Each gateway configured for stored volumes can support up to 32 volumes and a total volume storage of 512 TiB (0.5 PiB).

upvoted 1 times

 **MssP** 8 months, 1 week ago

all file types. Cached only save the most frequently or lastest accesed. If you didn't access any type for a long time, you will not cache it -> No immediate access

upvoted 2 times

 **WhericanIstart** 8 months, 2 weeks ago

Selected Answer: D

"The company wants to ensure that end users retain immediate access to all file types from the on-premises systems "

This points to stored volumes..

upvoted 1 times

 **KAUS2** 8 months, 2 weeks ago

Selected Answer: D

Option D is the right choice for this question . "The company wants to ensure that end users retain immediate access to all file types from the on-premises systems "

- Cached volumes: low latency access to most recent data

- Stored volumes: entire dataset is on premise, scheduled backups to S3

Hence Volume Gateway stored volume is the apt choice.

upvoted 3 times

 **bangfire** 8 months, 3 weeks ago

Answer is C.

Option D is not the best solution because a Volume Gateway stored volume does not provide immediate access to all file types and would require additional steps to retrieve data from Amazon S3, which can result in latency for end-users.

upvoted 2 times

 **UnluckyDucky** 8 months, 3 weeks ago

You're confusing cached mode with stored volume mode.

upvoted 1 times

 **un1x** 8 months, 3 weeks ago

Selected Answer: C

Answer is C.

why?

<https://docs.aws.amazon.com/storagegateway/latest/vgw/StorageGatewayConcepts.html#storage-gateway-stored-volume-concepts>

"Stored volumes can range from 1 GiB to 16 TiB in size and must be rounded to the nearest GiB. Each gateway configured for stored volumes can support up to 32 volumes and a total volume storage of 512 TiB"

Option D states: "Provision an AWS Storage Gateway Volume Gateway stored *volume* with the same amount of disk space as the existing file storage volume."

Notice that it states volume and not volumes, which would be the only way to match the information that the question provides.

Initial question states that on-premise volume is 100s of TB in size.

Therefore, only logical and viable answer can be C.

Feel free to prove me wrong

upvoted 3 times

 **eddie5049** 6 months, 3 weeks ago

Stored volumes can range from 1 GiB to 16 TiB in size and must be rounded to the nearest GiB. Each gateway configured for stored volumes can support up to 32 volumes and a total volume storage of 512 TiB (0.5 PiB).

why not configure multiple gateway to achieve the hundreds of TB?

upvoted 1 times

 **Steve_4542636** 9 months ago

Selected Answer: D

Stored Volume Gateway will retain ALL data locally whereas Cached Volume Gateway retains frequently accessed data locally

upvoted 3 times

A company is hosting a web application from an Amazon S3 bucket. The application uses Amazon Cognito as an identity provider to authenticate users and return a JSON Web Token (JWT) that provides access to protected resources that are stored in another S3 bucket.

Upon deployment of the application, users report errors and are unable to access the protected content. A solutions architect must resolve this issue by providing proper permissions so that users can access the protected content.

Which solution meets these requirements?

- A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.
- B. Update the S3 ACL to allow the application to access the protected content.
- C. Redeploy the application to Amazon S3 to prevent eventually consistent reads in the S3 bucket from affecting the ability of users to access the protected content.
- D. Update the Amazon Cognito pool to use custom attribute mappings within the identity pool and grant users the proper permissions to access the protected content.

Correct Answer: A

Community vote distribution

A (89%)	11%
---------	-----

✉  **alexandercamachop**  6 months ago

Selected Answer: A

To resolve the issue and provide proper permissions for users to access the protected content, the recommended solution is:

- A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.

Explanation:

Amazon Cognito provides authentication and user management services for web and mobile applications.

In this scenario, the application is using Amazon Cognito as an identity provider to authenticate users and obtain JSON Web Tokens (JWTs). The JWTs are used to access protected resources stored in another S3 bucket.

To grant users access to the protected content, the proper IAM role needs to be assumed by the identity pool in Amazon Cognito.

By updating the Amazon Cognito identity pool with the appropriate IAM role, users will be authorized to access the protected content in the S3 bucket.

upvoted 5 times

✉  **alexandercamachop** 6 months ago

Option B is incorrect because updating the S3 ACL (Access Control List) will only affect the permissions of the application, not the users accessing the content.

Option C is incorrect because redeploying the application to Amazon S3 will not resolve the issue related to user access permissions.

Option D is incorrect because updating custom attribute mappings in Amazon Cognito will not directly grant users the proper permissions to access the protected content.

upvoted 4 times

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

Selected Answer: A

- A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.

upvoted 2 times

✉  **Abrar2022** 5 months, 3 weeks ago

Selected Answer: A

Services access other services via IAM Roles. Hence why updating AWS Cognito identity pool to assume proper IAM Role is the right solution.

upvoted 1 times

✉  **shawford** 7 months, 3 weeks ago

Selected Answer: A

Amazon Cognito identity pools assign your authenticated users a set of temporary, limited-privilege credentials to access your AWS resources. The permissions for each user are controlled through IAM roles that you create. <https://docs.aws.amazon.com/cognito/latest/developerguide/role-based-access-control.html>

upvoted 1 times

✉  **Brak** 8 months, 3 weeks ago

Selected Answer: D

A makes no sense - Cognito is not accessing the S3 resource. It just returns the JWT token that will be attached to the S3 request.

D is the right answer, using custom attributes that are added to the JWT and used to grant permissions in S3. See <https://docs.aws.amazon.com/cognito/latest/developerguide/using-attributes-for-access-control-policy-example.html> for an example.

upvoted 2 times

✉ **Abhineet9148232** 8 months, 3 weeks ago

But even D requires setting up the permissions as bucket policy (as show in the shared example) which includes higher overhead than managing permissions attached to specific roles.

upvoted 2 times

✉ **asoli** 8 months, 2 weeks ago

A says "Identity Pool"

According to AWS: "With an identity pool, your users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB."

So, answer is A

upvoted 1 times

✉ **Steve_4542636** 9 months ago

Selected Answer: A

Services access other services via IAM Roles.

upvoted 1 times

✉ **LuckyAro** 9 months, 1 week ago

Selected Answer: A

A is the best solution as it directly addresses the issue of permissions and grants authenticated users the necessary IAM role to access the protected content.

A suggests updating the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content. This is a valid solution, as it would grant authenticated users the necessary permissions to access the protected content.

upvoted 4 times

✉ **jennyka76** 9 months, 1 week ago

ANSWER - A

<https://docs.aws.amazon.com/cognito/latest/developerguide/tutorial-create-identity-pool.html>

You have to create an custom role such as read-only

upvoted 4 times

✉ **zTopic** 9 months, 2 weeks ago

Selected Answer: A

Answer is A

upvoted 2 times

An image hosting company uploads its large assets to Amazon S3 Standard buckets. The company uses multipart upload in parallel by using S3 APIs and overwrites if the same object is uploaded again. For the first 30 days after upload, the objects will be accessed frequently. The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent. The company must optimize its S3 storage costs while maintaining high availability and resiliency of stored assets.

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

- A. Move assets to S3 Intelligent-Tiering after 30 days.
- B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.
- C. Configure an S3 Lifecycle policy to clean up expired object delete markers.
- D. Move assets to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- E. Move assets to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Correct Answer: AB

Community vote distribution

AB (57%)	BD (37%)	7%
----------	----------	----

✉  **Neha999** Highly Voted 9 months, 1 week ago

AB

A : Access Pattern for each object inconsistent, Infrequent Access

B : Deleting Incomplete Multipart Uploads to Lower Amazon S3 Costs
upvoted 14 times

✉  **TungPham** Highly Voted 9 months, 1 week ago

Selected Answer: AB

B because Abort Incomplete Multipart Uploads Using S3 Lifecycle => <https://aws.amazon.com/blogs/aws-cloud-financial-management/discovering-and-deleting-incomplete-multipart-uploads-to-lower-amazon-s3-costs/>

A because The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent => random access => S3 Intelligent-Tiering

upvoted 8 times

✉  **Guru4Cloud** Most Recent 2 months, 3 weeks ago

Selected Answer: AB

A. Move assets to S3 Intelligent-Tiering after 30 days.
B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.

upvoted 1 times

✉  **vini15** 4 months ago

should be A and B

upvoted 1 times

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

Selected Answer: BD

Option A has not been mentioned for resiliency in S3, check the page: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/disaster-recovery-resiliency.html>

Therefore, I am with B & D choices.

upvoted 1 times

✉  **alexandercamachop** 6 months ago

Selected Answer: AB

A. Move assets to S3 Intelligent-Tiering after 30 days.
B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.

Explanation:

A. Moving assets to S3 Intelligent-Tiering after 30 days: This storage class automatically analyzes the access patterns of objects and moves them between frequent access and infrequent access tiers. Since the objects will be accessed frequently for the first 30 days, storing them in the frequent access tier during that period optimizes performance. After 30 days, when the access patterns become inconsistent, S3 Intelligent-Tiering will automatically move the objects to the infrequent access tier, reducing storage costs.

B. Configuring an S3 Lifecycle policy to clean up incomplete multipart uploads: Multipart uploads are used for large objects, and incomplete multipart uploads can consume storage space if not cleaned up. By configuring an S3 Lifecycle policy to clean up incomplete multipart uploads, unnecessary storage costs can be avoided.

upvoted 1 times

✉  **antropaws** 6 months ago

Selected Answer: AD

AD.

B makes no sense because multipart uploads overwrite objects that are already uploaded. The question never says this is a problem.

upvoted 1 times

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

Questions says to optimize cost and if incomplete multipart are not aborted it will still use capacity on S3 Bucket thus increase unnecessary cost.

upvoted 1 times

✉  **klayytech** 8 months ago

Selected Answer: AB

the following two actions to optimize S3 storage costs while maintaining high availability and resiliency of stored assets:

A. Move assets to S3 Intelligent-Tiering after 30 days. This will automatically move objects between two access tiers based on changing access patterns and save costs by reducing the number of objects stored in the expensive tier.

B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads. This will help to reduce storage costs by removing incomplete multipart uploads that are no longer needed.

upvoted 2 times

✉  **datz** 8 months, 1 week ago

Selected Answer: BD

B = Deleting incomplete uploads will lower S3 cost.

and D: as "For the first 30 days after upload, the objects will be accessed frequently"

Intelligent checks and if file haven't been access for 30 consecutive days and send infrequent access. So if somebody accessed the file 20 days after the upload with the intelligent process, file will be moved to Infrequent Access tier after 50 days. Which will reflect against the COST.

"S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the Infrequent Access tier and after 90 days of no access to the Archive Instant Access tier. For data that does not require immediate retrieval, you can set up S3 Intelligent-Tiering to monitor and automatically move objects that aren't accessed for 180 days or more to the Deep Archive Access tier to realize up to 95% in storage cost savings."

https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access

upvoted 4 times

✉  **datz** 8 months, 1 week ago

Apologies D is wrong for sure lol

"S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed." and for the first 30 days data is frequently accessed lol.

So best solution will be A - Amazon S3 Intelligent-Tiering

upvoted 2 times

✉  **datz** 8 months, 1 week ago

sorry remove the above comment, as we are setting solution which will be needed after 30 Days

this should be : Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

upvoted 2 times

✉  **MLCL** 8 months, 2 weeks ago

Selected Answer: BD

Infrequent access is written in the question so it's BD

upvoted 1 times

✉  **MssP** 8 months ago

It is not infrequent... it is LESS frequent. It can be few less or too much less (infrequent) but it is clear that pattern is inconsistent -> A

upvoted 1 times

✉  **asoli** 8 months, 2 weeks ago

Selected Answer: AB

The answer is AB

A: "the access patterns for each object will be inconsistent" so Intelligent-Tiering works well for this assumption (even better than D. It may put it in lower tiers based on access patterns that Standard-IA)

D: incomplete multipart is just a waste of resources

upvoted 2 times

✉  **asoli** 8 months, 2 weeks ago

I meant B: incomplete multipart is just a waste of resources

upvoted 1 times

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

Selected Answer: AB

<https://www.examtopics.com/discussions/amazon/view/84533-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

✉  **cenil** 8 months, 2 weeks ago

AB, Unknown of changing access pattern

<https://aws.amazon.com/s3/storage-classes/>

upvoted 1 times

✉  **houzuun** 8 months, 2 weeks ago

Selected Answer: AB

I think B is obvious, and I chose A because the pattern is unpredictable

upvoted 2 times

✉  **Maximus007** 8 months, 2 weeks ago

B is clear

the choice might be between A and D

I vote for A - S3 Intelligent-Tiering will analyze patterns and decide properly

upvoted 1 times

✉  **taehyeki** 8 months, 3 weeks ago

Selected Answer: BD

i think b , d make more sense

it is no matter where each object is moved,

we only know object is not accessed frequently after 30days

so i go with D

upvoted 2 times

✉  **Abhineet9148232** 8 months, 3 weeks ago

Selected Answer: BD

S3-IA provides same low latency and high throughput performance of S3 Standard. Ideal for infrequent but high throughput access.

https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access

upvoted 1 times

A solutions architect must secure a VPC network that hosts Amazon EC2 instances. The EC2 instances contain highly sensitive data and run in a private subnet. According to company policy, the EC2 instances that run in the VPC can access only approved third-party software repositories on the internet for software product updates that use the third party's URL. Other internet traffic must be blocked.

Which solution meets these requirements?

- A. Update the route table for the private subnet to route the outbound traffic to an AWS Network Firewall firewall. Configure domain list rule groups.
- B. Set up an AWS WAF web ACL. Create a custom set of rules that filter traffic requests based on source and destination IP address range sets.
- C. Implement strict inbound security group rules. Configure an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs.
- D. Configure an Application Load Balancer (ALB) in front of the EC2 instances. Direct all outbound traffic to the ALB. Use a URL-based rule listener in the ALB's target group for outbound access to the internet.

Correct Answer: A

Community vote distribution

A (86%) 14%

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

Selected Answer: A

Correct Answer A. Send the outbound connection from EC2 to Network Firewall. In Network Firewall, create stateful outbound rules to allow certain domains for software patch download and deny all other domains.

<https://docs.aws.amazon.com/network-firewall/latest/developerguide/suricata-examples.html#suricata-example-domain-filtering>
upvoted 9 times

 **Guru4Cloud** 2 months, 3 weeks ago

Option A uses a network firewall which is overkill for instance-level rules.

upvoted 1 times

 **UnluckyDucky** Highly Voted 8 months, 3 weeks ago

Selected Answer: A

Can't use URLs in outbound rule of security groups. URL Filtering screams Firewall.

upvoted 6 times

 **TariqKipkemei** Most Recent 1 month, 2 weeks ago

Selected Answer: A

Just tried on the console to set up an outbound rule, and URLs cannot be used as a destination. I will opt for A.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: C

Implement strict inbound security group rules

Configure an outbound security group rule to allow traffic only to the approved software repository URLs

The key points:

Highly sensitive EC2 instances in private subnet that can access only approved URLs

Other internet access must be blocked

Security groups act as a firewall at the instance level and can control both inbound and outbound traffic.

upvoted 1 times

 **kelvintoy93** 5 months, 2 weeks ago

Isn't private subnet not connectible to internet at all, unless with a NAT gateway?

upvoted 3 times

 **VeseljkoD** 8 months, 3 weeks ago

Selected Answer: A

We can't specify URL in outbound rule of security group. Create free tier AWS account and test it.

upvoted 2 times

 **Leo301** 8 months, 3 weeks ago

Selected Answer: C

CCCCCCCCCC

upvoted 1 times

 **Brak** 8 months, 3 weeks ago

It can't be C. You cannot use URLs in the outbound rules of a security group.

upvoted 3 times

 **johnmcclane78** 8 months, 4 weeks ago

Option C is the best solution to meet the requirements of this scenario. Implementing strict inbound security group rules that only allow traffic from approved sources can help secure the VPC network that hosts Amazon EC2 instances. Additionally, configuring an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs will ensure that only approved third-party software repositories can be accessed from the EC2 instances. This solution does not require any additional AWS services and can be implemented using VPC security groups.

Option A is not the best solution as it involves the use of AWS Network Firewall, which may introduce additional operational overhead. While domain list rule groups can be used to block all internet traffic except for the approved third-party software repositories, this solution is more complex than necessary for this scenario.

upvoted 2 times

 **Steve_4542636** 9 months ago

Selected Answer: C

In the security group, only allow inbound traffic originating from the VPC. Then only allow outbound traffic with a whitelisted IP address. The question asks about blocking EC2 instances, which is best for security groups since those are at the EC2 instance level. A network firewall is at the VPC level, which is not what the question is asking to protect.

upvoted 1 times

 **Theodorz** 8 months, 4 weeks ago

Is Security Group able to allow a specific URL? According to https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html, I cannot find such description.

upvoted 2 times

 **KZM** 9 months, 1 week ago

I am confused that It seems both options A and C are valid solutions.

upvoted 3 times

 **Mia2009687** 4 months, 3 weeks ago

I think C is in private subnet. Even with security group, it could not go public to download the software.

upvoted 1 times

 **ruqui** 6 months ago

C is not valid. Security groups can allow only traffic from specific ports and/or IPs, you can't use an URL. Correct answer is A

upvoted 1 times

 **Zohx** 9 months ago

Same here - why is C not a valid option?

upvoted 2 times

 **Karlos99** 9 months ago

And it is easier to do it at the level

upvoted 1 times

 **Karlos99** 9 months ago

And it is easier to do it at the VPC level

upvoted 1 times

 **Karlos99** 9 months ago

Because in this case, the session is initialized from inside

upvoted 1 times

 **jennyka76** 9 months, 1 week ago

Answer - A

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-al1-al2-update-yum-without-internet/>

upvoted 5 times

 **asoli** 8 months, 2 weeks ago

Although the answer is A, the link you provided here is not related to this question.

The information about "Network Firewall" and how it can help this issue is here:

<https://docs.aws.amazon.com/network-firewall/latest/developerguide/suricata-examples.html#suricata-example-domain-filtering>

(thanks to "@Bhawesh" to provide the link in their answer)

upvoted 3 times

 **Neha999** 9 months, 1 week ago

A as other options are controlling inbound traffic

upvoted 4 times

A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products.

What should a solutions architect recommend to ensure that all the requests are processed successfully?

- A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.
- B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
- C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
- D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

Correct Answer: D

Community vote distribution

D (63%)

B (37%)

✉️  **Steve_4542636**  9 months ago

Selected Answer: B

The auto-scaling would increase the rate at which sales requests are "processed", whereas a SQS will ensure messages don't get lost. If you were at a fast food restaurant with a long line with 3 cash registers, would you want more cash registers or longer ropes to handle longer lines? Same concept here.

upvoted 14 times

✉️  **Chef_couincouin** 3 weeks, 1 day ago

ensure that all the requests are processed successfully? doesn't mean more quickly

upvoted 1 times

✉️  **rushi0611** 6 months, 3 weeks ago

"ensure that all the requests are processed successfully?"

we want to ensure success not the speed, even in the auto-scaling, there is the chance for the failure of the request but not in SQS- if it is failed in sqs it is sent back to the queue again and new consumer will pick the request.

upvoted 7 times

✉️  **joechen2023** 5 months, 2 weeks ago

As an architecture, it is not possible to add more backend workers (it is part of the HR and boss's job, not for architecture design the solution).

So when the demand surge, the only correct choice is to buffer them using SQS so that workers can take their time to process it successfully

upvoted 1 times

✉️  **lizard812** 8 months, 1 week ago

Hell true: I'd rather combine the both options: a SQS + auto-scaled bound to the length of the queue.

upvoted 7 times

✉️  **Abhineet9148232**  6 months, 3 weeks ago

Selected Answer: D

B doesn't fit because Auto Scaling alone does not guarantee that all requests will be processed successfully, which the question clearly asks for.

D ensures that all messages are processed.

upvoted 6 times

✉️  **wsdasdasdqwdaw**  1 month, 1 week ago

Amazon SQS will make sure that the requests are stored and didn't get lost. After that the workers asynchronously will process the requests. I would go for D

upvoted 2 times

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

Technically both option B and D would work. But, there's a need to process requests asynchronously, hence decoupling, hence Amazon SQS. I will settle with option D.

upvoted 1 times

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

Selected Answer: D

D is correct.

upvoted 2 times

✉  **antropaws** 6 months ago

Selected Answer: D

D is correct.

upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: D

An SQS queue acts as a buffer between the frontend (website) and backend (API). Web requests can dump messages into the queue at a high throughput, then the queue handles delivering those messages to the API at a controlled rate that it can sustain. This prevents the API from being overwhelmed.

upvoted 2 times

✉  **kruasan** 7 months ago

Options A and B would help by scaling out more instances, however, this may not scale quickly enough and still risks overwhelming the API. Caching parts of the dynamic content (option C) may help but does not provide the buffering mechanism that a queue does.

upvoted 1 times

✉  **seifshendy99** 7 months, 1 week ago

Selected Answer: D

D make sens

upvoted 1 times

✉  **kraken21** 8 months ago

Selected Answer: D

D makes more sense

upvoted 1 times

✉  **kraken21** 8 months ago

There is no clarity on what the asynchronous process is but D makes more sense if we want to process all requests successfully. The way the question is worded it looks like the msgs->SQS>ELB/Ec2. This ensures that the messages are processed but may be delayed as the load increases.

upvoted 1 times

✉  **channn** 8 months ago

Selected Answer: D

although i agree with B for better performance. but i choose 'D' as question request to ensure that all the requests are processed successfully.

upvoted 2 times

✉  **klaytech** 8 months ago

To ensure that all the requests are processed successfully, I would recommend adding an Amazon CloudFront distribution for the static content and an Amazon CloudFront distribution for the dynamic content. This will help to reduce the load on the API and improve its performance. You can also place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic. This will help to ensure that you have enough capacity to handle the increase in traffic during events for the launch of new products.

upvoted 1 times

✉  **AravindG** 8 months ago

Selected Answer: D

The company is expecting a significant and sudden increase in the number of sales requests and keyword async. So I feel option D suits here.

upvoted 1 times

✉  **MssP** 8 months, 1 week ago

Selected Answer: D

Critical here is "to ensure that all the requests". ALL REQUESTS, so it is only possible with a SQS. ASG can spend time to launch new instances so any request can be lost.

upvoted 4 times

✉  **andyto** 8 months, 1 week ago

Selected Answer: D

I vote for D. "The company is expecting a significant and sudden increase in the number of sales requests". Sudden increase means ASG might not be able to deploy more EC2 instances when requests rocket and some of request will get lost.

upvoted 2 times

✉  **asoli** 8 months, 2 weeks ago

Selected Answer: D

The keyword here about the orders is "asynchronously". Orders are supposed to process asynchronously. So, it can be published in an SQS and processed after that. Also, it ensures in a spike, there is no lost order.

In contrast, if you think the answer is B, the issue is the sudden spike. Maybe the auto-scaling is not acting fast enough and some orders are lost. So, B is not correct.

upvoted 2 times

 **harirkmusa** 8 months, 3 weeks ago

Selected D

upvoted 1 times

A security audit reveals that Amazon EC2 instances are not being patched regularly. A solutions architect needs to provide a solution that will run regular security scans across a large fleet of EC2 instances. The solution should also patch the EC2 instances on a regular schedule and provide a report of each instance's patch status.

Which solution will meet these requirements?

- A. Set up Amazon Macie to scan the EC2 instances for software vulnerabilities. Set up a cron job on each EC2 instance to patch the instance on a regular schedule.
- B. Turn on Amazon GuardDuty in the account. Configure GuardDuty to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Session Manager to patch the EC2 instances on a regular schedule.
- C. Set up Amazon Detective to scan the EC2 instances for software vulnerabilities. Set up an Amazon EventBridge scheduled rule to patch the EC2 instances on a regular schedule.
- D. Turn on Amazon Inspector in the account. Configure Amazon Inspector to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Patch Manager to patch the EC2 instances on a regular schedule.

Correct Answer: D

Community vote distribution

D (100%)

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: D

ddddddddd
upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: D

Amazon Inspector is a security assessment service that automatically assesses applications for vulnerabilities or deviations from best practices. It can be used to scan the EC2 instances for software vulnerabilities. AWS Systems Manager Patch Manager can be used to patch the EC2 instances on a regular schedule. Together, these services can provide a solution that meets the requirements of running regular security scans and patching EC2 instances on a regular schedule. Additionally, Patch Manager can provide a report of each instance's patch status.

upvoted 3 times

 **Steve_4542636** 9 months ago

Selected Answer: D

Inspector is for EC2 instances and network accessibility of those instances
<https://portal.tutorialsdojo.com/forums/discussion/difference-between-security-hub-detective-and-inspector/>
upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: D

Amazon Inspector is a security assessment service that helps improve the security and compliance of applications deployed on Amazon Web Services (AWS). It automatically assesses applications for vulnerabilities or deviations from best practices. Amazon Inspector can be used to identify security issues and recommend fixes for them. It is an ideal solution for running regular security scans across a large fleet of EC2 instances.

AWS Systems Manager Patch Manager is a service that helps you automate the process of patching Windows and Linux instances. It provides a simple, automated way to patch your instances with the latest security patches and updates. Patch Manager helps you maintain compliance with security policies and regulations by providing detailed reports on the patch status of your instances.

upvoted 1 times

 **TungPham** 9 months, 1 week ago

Selected Answer: D

Amazon Inspector for EC2
https://aws.amazon.com/vi/inspector/faqs/?nc1=f_ls
Amazon system manager Patch manager for automates the process of patching managed nodes with both security-related updates and other types of updates.

<http://webcache.googleusercontent.com/search?q=cache:FbFTc6XKycwJ:https://medium.com/aws-architech/use-case-aws-inspector-vs-guardduty-3662bf80767a&hl=vi&gl=kr&strip=1&vwsrc=0>
upvoted 2 times

 **jennyka76** 9 months, 1 week ago

answer - D
<https://aws.amazon.com/inspector/faqs/>

upvoted 2 times

 **Neha999** 9 months, 1 week ago

D as AWS Systems Manager Patch Manager can patch the EC2 instances.

upvoted 1 times

A company is planning to store data on Amazon RDS DB instances. The company must encrypt the data at rest.

What should a solutions architect do to meet this requirement?

- A. Create a key in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances.
- B. Create an encryption key. Store the key in AWS Secrets Manager. Use the key to encrypt the DB instances.
- C. Generate a certificate in AWS Certificate Manager (ACM). Enable SSL/TLS on the DB instances by using the certificate.
- D. Generate a certificate in AWS Identity and Access Management (IAM). Enable SSL/TLS on the DB instances by using the certificate.

Correct Answer: C

Community vote distribution

A (100%)

✉️  **robpalacios1** 1 week ago

Selected Answer: A

KMS only generates and manages encryption keys. That's it. That's all it does. It's a fundamental service that you as well as other AWS Services (like Secrets Manager) use it to encrypt or decrypt.

Key Management Service. Secrets Manager is for database connection strings.

upvoted 3 times

upvoted 1 times

✉️  **antropaws** 6 months ago

OK, but why not B???

upvoted 1 times

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

KMS only generates and manages encryption keys. That's it. That's all it does. It's a fundamental service that you as well as other AWS Services (like Secrets Manager) use it to encrypt or decrypt.

Secrets Manager stores actual secrets like passwords, pass phrases, and anything else you want encrypted. SM uses KMS to encrypt its secrets, it would be circular to get an encryption key from KMS to use SM to encrypt the encryption key.

upvoted 3 times

✉️  **SkyZeroZx** 7 months ago

Selected Answer: A

ANSWER - A

upvoted 1 times

✉️  **datz** 8 months, 1 week ago

Selected Answer: A

A for sure

upvoted 1 times

✉️  **PRASAD180** 8 months, 3 weeks ago

A is 100% Crt

upvoted 1 times

✉️  **Steve_4542636** 9 months ago

Selected Answer: A

Key Management Service. Secrets Manager is for database connection strings.

upvoted 3 times

✉️  **LuckyAro** 9 months, 1 week ago

Selected Answer: A

A is the correct solution to meet the requirement of encrypting the data at rest.

To encrypt data at rest in Amazon RDS, you can use the encryption feature of Amazon RDS, which uses AWS Key Management Service (AWS KMS). With this feature, Amazon RDS encrypts each database instance with a unique key. This key is stored securely by AWS KMS. You can manage your own keys or use the default AWS-managed keys. When you enable encryption for a DB instance, Amazon RDS encrypts the underlying storage, including the automated backups, read replicas, and snapshots.

upvoted 2 times

✉️  **bdp123** 9 months, 1 week ago

Selected Answer: A

AWS Key Management Service (KMS) is used to manage the keys used to encrypt and decrypt the data.
upvoted 1 times

👤 **pbpally** 9 months, 1 week ago

Selected Answer: A

Option A

upvoted 1 times

👤 **NolaHolla** 9 months, 1 week ago

A. Create a key in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances is the correct answer to encrypt the data at rest in Amazon RDS DB instances.

Amazon RDS provides multiple options for encrypting data at rest. AWS Key Management Service (KMS) is used to manage the keys used to encrypt and decrypt the data. Therefore, a solution architect should create a key in AWS KMS and enable encryption for the DB instances to encrypt the data at rest.

upvoted 1 times

👤 **jennyka76** 9 months, 1 week ago

ANSWER - A

<https://docs.aws.amazon.com/whitepapers/latest/efs-encrypted-file-systems/managing-keys.html>

upvoted 1 times

👤 **Bhawesh** 9 months, 2 weeks ago

Selected Answer: A

A. Create a key in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances.

<https://www.examtopics.com/discussions/amazon/view/80753-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization.

What should a solutions architect do to meet these requirements?

- A. Use AWS Snowball.
- B. Use AWS DataSync.
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration.

Correct Answer: A

Community vote distribution

A (84%) B (16%)

✉  **kruasan**  7 months ago

Selected Answer: A

Don't mix up between Mbps and Mbs.
The proper calculation is:

$10 \text{ MB/s} \times 86,400 \text{ seconds per day} \times 30 \text{ days} / 8 = 3,402,000 \text{ MB}$ or approximately 3.4 TB
upvoted 6 times

✉  **wsdasdasdqwdaw**  1 month, 1 week ago

$(15/8) = 1.875 \text{ MB/s}$
 $1.875 \text{ MB/s} \times 0.7 = 1.3125 \text{ (70\% NW utilization) MB/s}$
 $1.3125 \text{ MB/s} \times 3600 = 4725 \text{ MB (MB per 1 hour)}$
 $4725 \times 24 = 113400 \text{ MB per 1 full day (24h)}$
 $113400 \times 30 = 3402000 \text{ MB for 30 days}$
 $3402000 / 1024 = 3322.265625 \text{ GB for 30 days}$
 $3322.265625 / 1024 \sim 3.24 \text{ TB for 30 days} \Rightarrow \text{not enough for NW} \Rightarrow \text{Snowball which is A}$
upvoted 1 times

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

Selected Answer: A

I wont try to think about it, AWS Snowball was designed for this
upvoted 1 times

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

Selected Answer: A

- 15 Mbps bandwidth with 70% max utilization limits the effective bandwidth to 10.5 Mbps or 1.31 MB/s.
- 20 TB of data at 1.31 MB/s would take approximately 193 days to transfer over the network. ◦ This far exceeds the 30 day requirement.
- AWS Snowball provides a physical storage device that can be shipped to the data center. Up to 80 TB can be loaded onto a Snowball device and shipped back to AWS.

This allows the 20 TB of data to be transferred much faster by shipping rather than over the limited network bandwidth.

- Snowball uses tamper-resistant enclosures and 256-bit encryption to keep the data secure during transit.
- The data can be imported into Amazon S3 or Amazon Glacier once the Snowball is received by AWS.

upvoted 2 times

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

Selected Answer: B

$10 \text{ MB/s} \times 86,400 \text{ seconds per day} \times 30 \text{ days} = 25,920,000 \text{ MB}$ or approximately 25.2 TB

That's how much you can transfer with a 10 Mbps link (roughly 70% of the 15 Mbps connection).

With a consistent connection of 8~ Mbps, and 30 days, you can upload 20 TB of data.

My math says B, my brain wants to go with A. Take your pick.

upvoted 3 times

✉  **Zox42** 8 months, 1 week ago

$15 \text{ Mbps} * 0.7 = 1.3125 \text{ MB/s}$ and $1.3125 * 86,400 * 30 = 3,402,000 \text{ MB}$
Answer A is correct.

upvoted 2 times

✉  **hozy_** 4 months, 2 weeks ago

How can 15 * 0.7 be 1.3125 LMAO
upvoted 1 times

✉ **hozy_** 4 months, 2 weeks ago
OMG it was Mbps! Not MBps. You are right! awesome!!!
upvoted 1 times

✉ **Zox42** 8 months, 1 week ago
3,402,000
upvoted 2 times

✉ **Bilalazure** 9 months, 1 week ago
Selected Answer: A
Aws snowball
upvoted 2 times

✉ **PRASAD180** 9 months, 1 week ago
A is 100% Crt
upvoted 1 times

✉ **LuckyAro** 9 months, 1 week ago
Selected Answer: A
AWS Snowball
upvoted 1 times

✉ **pbpally** 9 months, 1 week ago
Selected Answer: A
Option a
upvoted 1 times

✉ **jennyka76** 9 months, 1 week ago
ANSWER - A
<https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html>
upvoted 1 times

✉ **AWSSHA1** 9 months, 2 weeks ago
Selected Answer: A
option A
upvoted 3 times

A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees' devices.

The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.

Which solution will meet these requirements?

- A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
- B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
- C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
- D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS IAM Identity Center (AWS Single Sign-On).

Correct Answer: B

Community vote distribution

B (88%) 13%

 **TariqKipkemei** 1 month, 2 weeks ago

Selected Answer: B

Windows file server = Amazon FSx for Windows File Server file system
Files can be accessed only by authorized users = On-premises Active Directory
upvoted 1 times

 **BrijMohan08** 2 months, 3 weeks ago

Selected Answer: C

Remember: The file server is running out of capacity.
upvoted 1 times

 **SkyZeroZx** 6 months, 3 weeks ago

Selected Answer: B

B is the correct answer
upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: B

This solution addresses the need for secure access to confidential and sensitive files, as well as the increase in remote usage. Migrating the files to Amazon FSx for Windows File Server provides a scalable, fully managed file storage solution in the AWS Cloud that is accessible from on-premises and cloud environments. Integration with the on-premises Active Directory allows for a consistent user experience and centralized access control. AWS Client VPN provides a secure and managed VPN solution that can be used by employees to access the files securely.

upvoted 4 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: B

B is the best solution for the given requirements. It provides a secure way for employees to access confidential and sensitive files from anywhere using AWS Client VPN. The Amazon FSx for Windows File Server file system is designed to provide native support for Windows file system features such as NTFS permissions, Active Directory integration, and Distributed File System (DFS). This means that the company can continue to use their on-premises Active Directory to manage user access to files.

upvoted 1 times

 **Bilalazure** 9 months, 1 week ago

B is the correct answer
upvoted 1 times

 **jennyka76** 9 months, 1 week ago

Answer - B
1- <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>
2- <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-capacity.html>
upvoted 1 times

 **Neha999** 9 months, 1 week ago

B

Amazon FSx for Windows File Server file system

upvoted 2 times

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch runs. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB.
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Correct Answer: C

Community vote distribution

C (100%)

 **TariqKipkemei** 1 month, 2 weeks ago

Selected Answer: C

'On the first day of every month at midnight' = Scheduled scaling policy
upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: C

By configuring a scheduled scaling policy, the EC2 Auto Scaling group can proactively launch additional EC2 instances before the CPU utilization peaks to 100%. This will ensure that the application can handle the workload during the month-end financial calculation batch, and avoid any disruption or downtime.

Configuring a simple scaling policy based on CPU utilization or adding Amazon CloudFront distribution or Amazon ElastiCache will not directly address the issue of handling the monthly peak workload.

upvoted 2 times

 **Steve_4542636** 9 months ago

Selected Answer: C

If the scaling were based on CPU or memory, it requires a certain amount of time above that threshold, 5 minutes for example. That would mean the CPU would be at 100% for five minutes.

upvoted 2 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: C

C: Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule is the best option because it allows for the proactive scaling of the EC2 instances before the monthly batch run begins. This will ensure that the application is able to handle the increased workload without experiencing downtime. The scheduled scaling policy can be configured to increase the number of instances in the Auto Scaling group a few hours before the batch run and then decrease the number of instances after the batch run is complete. This will ensure that the resources are available when needed and not wasted when not needed.

The most appropriate solution to handle the increased workload during the monthly batch run and avoid downtime would be to configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.

upvoted 2 times

 **LuckyAro** 9 months, 1 week ago

Scheduled scaling policies allow you to schedule EC2 instance scaling events in advance based on a specified time and date. You can use this feature to plan for anticipated traffic spikes or seasonal changes in demand. By setting up scheduled scaling policies, you can ensure that you have the right number of instances running at the right time, thereby optimizing performance and reducing costs.

To set up a scheduled scaling policy in EC2 Auto Scaling, you need to specify the following:

Start time and date: The date and time when the scaling event should begin.

Desired capacity: The number of instances that you want to have running after the scaling event.

Recurrence: The frequency with which the scaling event should occur. This can be a one-time event or a recurring event, such as daily or weekly.
upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: C

C is the correct answer as traffic spike is known
upvoted 1 times

 **jennyka76** 9 months, 1 week ago

ANSWER - C
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>
upvoted 2 times

 **Neha999** 9 months, 1 week ago

C as the schedule of traffic spike is known beforehand.
upvoted 1 times

A company wants to give a customer the ability to use on-premises Microsoft Active Directory to download files that are stored in Amazon S3. The customer's application uses an SFTP client to download the files.

Which solution will meet these requirements with the LEAST operational overhead and no changes to the customer's application?

- A. Set up AWS Transfer Family with SFTP for Amazon S3. Configure integrated Active Directory authentication.
- B. Set up AWS Database Migration Service (AWS DMS) to synchronize the on-premises client with Amazon S3. Configure integrated Active Directory authentication.
- C. Set up AWS DataSync to synchronize between the on-premises location and the S3 location by using AWS IAM Identity Center (AWS Single Sign-On).
- D. Set up a Windows Amazon EC2 instance with SFTP to connect the on-premises client with Amazon S3. Integrate AWS Identity and Access Management (IAM).

Correct Answer: B

Community vote distribution

A (100%)

 **Steve_4542636** Highly Voted  9 months ago

Selected Answer: A

SFTP, FTP - think "Transfer" during test time
upvoted 6 times

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

LEAST operational overhead => A, D is much more operational overhead
upvoted 1 times

 **TariqKipkemei** 1 month, 2 weeks ago

Selected Answer: A

SFTP, No changes to the customer's application? = AWS Transfer Family
upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Transfer family is used for SFTP
upvoted 1 times

 **live_reply_developers** 4 months, 1 week ago

SFTP -> transfer family
upvoted 1 times

 **antropaws** 6 months ago

Selected Answer: A

A no doubt. Why the system gives B as the correct answer?
upvoted 1 times

 **Iht** 6 months, 4 weeks ago

Selected Answer: A

just A
upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: A

AWS Transfer Family
upvoted 2 times

 **LuckyAro** 9 months, 1 week ago

AWS Transfer Family is a fully managed service that allows customers to transfer files over SFTP, FTPS, and FTP directly into and out of Amazon S3. It eliminates the need to manage any infrastructure for file transfer, which reduces operational overhead. Additionally, the service can be configured to use an existing Active Directory for authentication, which means that no changes need to be made to the customer's application.
upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: A

Transfer family is used for SFTP

upvoted 1 times

👤 **TungPham** 9 months, 1 week ago

Selected Answer: A

using AWS Batch to LEAST operational overhead
and have SFTP to no changes to the customer's application

<https://aws.amazon.com/vi/blogs/architecture/managed-file-transfer-using-aws-transfer-family-and-amazon-s3/>

upvoted 2 times

👤 **Bhawesh** 9 months, 2 weeks ago

Selected Answer: A

A. Set up AWS Transfer Family with SFTP for Amazon S3. Configure integrated Active Directory authentication.

<https://docs.aws.amazon.com/transfer/latest/userguide/directory-services-users.html>

upvoted 3 times

A company is experiencing sudden increases in demand. The company needs to provision large Amazon EC2 instances from an Amazon Machine Image (AMI). The instances will run in an Auto Scaling group. The company needs a solution that provides minimum initialization latency to meet the demand.

Which solution meets these requirements?

- A. Use the aws ec2 register-image command to create an AMI from a snapshot. Use AWS Step Functions to replace the AMI in the Auto Scaling group.
- B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot. Provision an AMI by using the snapshot. Replace the AMI in the Auto Scaling group with the new AMI.
- C. Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager (Amazon DLM). Create an AWS Lambda function that modifies the AMI in the Auto Scaling group.
- D. Use Amazon EventBridge to invoke AWS Backup lifecycle policies that provision AMIs. Configure Auto Scaling group capacity limits as an event source in EventBridge.

Correct Answer: C

Community vote distribution

B (88%) 12%

✉  **danielklein09** Highly Voted 6 months ago

readed the question 5 times, didn't understand a thing :(
upvoted 23 times

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

Me too
upvoted 2 times

✉  **TariqKipkemei** Most Recent 1 month, 2 weeks ago

Selected Answer: B

Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot. Provision an AMI by using the snapshot. Replace the AMI in the Auto Scaling group with the new AMI
upvoted 1 times

✉  **kambarami** 2 months, 1 week ago

Pleaw3 reword 5he question. Can not understand a thing!
upvoted 1 times

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

Selected Answer: B

Enable EBS fast snapshot restore on a snapshot
Create an AMI from the snapshot
Replace the AMI used by the Auto Scaling group with this new AMI

The key points:

- ° Need to launch large EC2 instances quickly from an AMI in an Auto Scaling group
- ° Looking to minimize instance initialization latency
upvoted 1 times

✉  **antropaws** 6 months ago

Selected Answer: B

B most def
upvoted 1 times

✉  **elearningtakai** 8 months ago

Selected Answer: B

B: "EBS fast snapshot restore": minimizes initialization latency. This is a good choice.
upvoted 2 times

✉  **Zox42** 8 months, 1 week ago

Selected Answer: B

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

upvoted 2 times

 **geekgirl22** 9 months, 1 week ago

Keyword, minimize initialization latency == snapshot. A and B have snapshots in them, but B is the one that makes sense. C has DLP that can create machines from AMI, but that does not talk about latency and snapshots.

upvoted 3 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: B

Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows for rapid restoration of EBS volumes from snapshots. This reduces the time required to create an AMI from a snapshot, which is useful for quickly provisioning large Amazon EC2 instances.

Provisioning an AMI by using the fast snapshot restore feature is a fast and efficient way to create an AMI. Once the AMI is created, it can be replaced in the Auto Scaling group without any downtime or disruption to running instances.

upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: B

Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows you to quickly create a new Amazon Machine Image (AMI) from a snapshot, which can help reduce the initialization latency when provisioning new instances. Once the AMI is provisioned, you can replace the AMI in the Auto Scaling group with the new AMI. This will ensure that new instances are launched from the updated AMI and are able to meet the increased demand quickly.

upvoted 1 times

 **TungPham** 9 months, 1 week ago

Selected Answer: C

Provision an AMI by using the snapshot => not sure because SnapShot only backup a EBS, AMI is backup a cluster . Replace the AMI in the Auto Scaling group with the new AMI. => for what ??

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

Amazon Data Lifecycle Manager helps automate snapshot and AMI management

upvoted 2 times

 **jennyka76** 9 months, 1 week ago

agree with answer - B

upvoted 1 times

 **kpato87** 9 months, 1 week ago

Selected Answer: B

Option B is the most suitable solution for this use case, as it enables Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot, which significantly reduces the time required for creating an AMI from the snapshot. The fast snapshot restore feature enables Amazon EBS to pre-warm the EBS volumes associated with the snapshot, which reduces the time required to initialize the volumes when launching instances from the AMI.

upvoted 2 times

 **Neha999** 9 months, 1 week ago

<https://www.examtopics.com/discussions/amazon/view/82400-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **bdp123** 9 months, 2 weeks ago

Selected Answer: B

Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows you to quickly create a new Amazon Machine Image (AMI) from a snapshot, which can help reduce the initialization latency when provisioning new instances. Once the AMI is provisioned, you can replace the AMI in the Auto Scaling group with the new AMI. This will ensure that new instances are launched from the updated AMI and are able to meet the increased demand quickly.

upvoted 4 times

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.

What should a solutions architect do to meet this requirement with the LEAST operational effort?

- A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.
- B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.
- C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.
- D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials. Download the file to the application regularly to ensure that the correct credentials are used. Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket.

Correct Answer: A

Community vote distribution

A (100%)

 **TariqKipkemei** 1 month, 2 weeks ago

Selected Answer: A

Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: A

Use AWS Secrets Manager to store the Aurora credentials as a secret

Encrypt the secret with a KMS key

Configure 14 day automatic rotation for the secret

Associate the secret with the Aurora DB cluster

The key points:

Aurora MySQL credentials must be encrypted and rotated every 14 days

Want to minimize operational effort

upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: A

AWS Secrets Manager allows you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. With this service, you can automate the rotation of secrets, such as database credentials, on a schedule that you choose. The solution allows you to create a new secret with the appropriate credentials and associate it with the Aurora DB cluster. You can then configure a custom rotation period of 14 days to ensure that the credentials are automatically rotated every two weeks, as required by the IT security guidelines. This approach requires the least amount of operational effort as it allows you to manage secrets centrally without modifying your application code or infrastructure.

upvoted 3 times

 **elearningtakai** 8 months ago

Selected Answer: A

A: AWS Secrets Manager. Simply this supported rotate feature, and secure to store credentials instead of EFS or S3.

upvoted 1 times

 **Steve_4542636** 9 months ago

Selected Answer: A

Voting A

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: A

A proposes to create a new AWS KMS encryption key and use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Then, the secret will be associated with the Aurora DB cluster, and a custom rotation period of 14 days will be configured. AWS Secrets Manager will automate the process of rotating the database credentials, which will reduce the operational effort required to meet the IT security guidelines.

upvoted 1 times

 **jennyka76** 9 months, 1 week ago

Answer is A

To implement password rotation lifecycles, use AWS Secrets Manager. You can rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle using Secrets Manager.

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/>

upvoted 3 times

 **Neha999** 9 months, 1 week ago

A

<https://www.examtopics.com/discussions/amazon/view/59985-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company has deployed a web application on AWS. The company hosts the backend database on Amazon RDS for MySQL with a primary DB instance and five read replicas to support scaling needs. The read replicas must lag no more than 1 second behind the primary DB instance. The database routinely runs scheduled stored procedures.

As traffic on the website increases, the replicas experience additional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutions architect must minimize changes to the application code and must minimize ongoing operational overhead.

Which solution will meet these requirements?

- A. Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora MySQL native functions.
- B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the application to check the cache before the application queries the database. Replace the stored procedures with AWS Lambda functions.
- C. Migrate the database to a MySQL database that runs on Amazon EC2 instances. Choose large, compute optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.
- D. Migrate the database to Amazon DynamoDB. Provision a large number of read capacity units (RCUs) to support the required throughput, and configure on-demand capacity scaling. Replace the stored procedures with DynamoDB streams.

Correct Answer: A

Community vote distribution

A (71%)

B (29%)

✉  **fkie4**  8 months, 3 weeks ago

i hate this kind of question

upvoted 29 times

✉  **warav**  1 month, 2 weeks ago

I was able to approach my Amazon Web Services SAA-C03 exam with confidence thanks to Marks4sure.com's exam dumps. They were comprehensive and helped me identify areas where I needed to improve.

upvoted 1 times

✉  **AAAWrekng** 1 month ago

LOL, "I'm not advertising my own product here, HONEST!!"

upvoted 2 times

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

Selected Answer: A

Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora MySQL native functions

upvoted 1 times

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

Selected Answer: A

Migrate the RDS MySQL database to Amazon Aurora MySQL

Use Aurora Replicas for read scaling instead of RDS read replicas

Configure Aurora Auto Scaling to handle load spikes

Replace stored procedures with Aurora MySQL native functions

upvoted 1 times

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

Selected Answer: A

First, ElastiCache involves heavy change on application code. The question mentioned that "the solutions architect must minimize changes to the application code". Therefore B is not suitable and A is more appropriate for the question requirement.

upvoted 2 times

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

... but migrating their ENTIRE prod database and its replicas to a new platform is not a heavy change?

upvoted 2 times

✉  **KMohsoe** 6 months, 1 week ago

Selected Answer: B

Why not B? Please explain to me.

upvoted 2 times

✉ **Terion** 2 months ago

It wouldn't have the most up to date info since it must no lag in relation to the main DB

upvoted 1 times

✉ **asoli** 8 months, 2 weeks ago

Selected Answer: A

Using Cache required huge changes in the application. Several things need to change to use cache in front of the DB in the application. So, option B is not correct.

Aurora will help to reduce replication lag for read replica

upvoted 4 times

✉ **kaushald** 8 months, 3 weeks ago

Option A is the most appropriate solution for reducing replication lag without significant changes to the application code and minimizing ongoing operational overhead. Migrating the database to Amazon Aurora MySQL allows for improved replication performance and higher scalability compared to Amazon RDS for MySQL. Aurora Replicas provide faster replication, reducing the replication lag, and Aurora Auto Scaling ensures that there are enough Aurora Replicas to handle the incoming traffic. Additionally, Aurora MySQL native functions can replace the stored procedures, reducing the load on the database and improving performance.

Option B is not the best solution since adding an ElastiCache for Redis cluster does not address the replication lag issue, and the cache may not have the most up-to-date information. Additionally, replacing the stored procedures with AWS Lambda functions adds additional complexity and may not improve performance.

upvoted 3 times

✉ **taehyeki** 8 months, 3 weeks ago

Selected Answer: B

a,b are confusing me..

i would like to go with b..

upvoted 1 times

✉ **bangfire** 8 months, 3 weeks ago

Option B is incorrect because it suggests using ElastiCache for Redis as a caching layer in front of the database, but this would not necessarily reduce the replication lag on the read replicas. Additionally, it suggests replacing the stored procedures with AWS Lambda functions, which may require significant changes to the application code.

upvoted 4 times

✉ **lizard812** 8 months, 1 week ago

Yes and moreover Redis requires app refactoring which is a solid operational overhead

upvoted 1 times

✉ **Nel8** 9 months ago

Selected Answer: B

By using ElastiCache you avoid a lot of common issues you might encounter. ElastiCache is a database caching solution. ElastiCache Redis per se, supports failover and Multi-AZ. And Most of all, ElastiCache is well suited to place in front of RDS.

Migrating a database such as option A, requires operational overhead.

upvoted 2 times

✉ **bdp123** 9 months, 1 week ago

Selected Answer: A

Aurora can have up to 15 read replicas - much faster than RDS

<https://aws.amazon.com/rds/aurora/>

upvoted 4 times

✉ **ChrisG1454** 8 months, 4 weeks ago

" As a result, all Aurora Replicas return the same data for query results with minimal replica lag. This lag is usually much less than 100 milliseconds after the primary instance has written an update "

Reference:

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

upvoted 2 times

✉ **ChrisG1454** 8 months, 3 weeks ago

You can invoke an Amazon Lambda function from an Amazon Aurora MySQL-Compatible Edition DB cluster with the "native function"....

https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html

upvoted 1 times

✉ **jennyka76** 9 months, 1 week ago

Answer - A

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PostgreSQL.Replication.ReadReplicas.html

You can scale reads for your Amazon RDS for PostgreSQL DB instance by adding read replicas to the instance. As with other Amazon RDS database

engines, RDS for PostgreSQL uses the native replication mechanisms of PostgreSQL to keep read replicas up to date with changes on the source DB. For general information about read replicas and Amazon RDS, see [Working with read replicas](#).

upvoted 3 times

A solutions architect must create a disaster recovery (DR) plan for a high-volume software as a service (SaaS) platform. All data for the platform is stored in an Amazon Aurora MySQL DB cluster.

The DR plan must replicate data to a secondary AWS Region.

Which solution will meet these requirements MOST cost-effectively?

- A. Use MySQL binary log replication to an Aurora cluster in the secondary Region. Provision one DB instance for the Aurora cluster in the secondary Region.
- B. Set up an Aurora global database for the DB cluster. When setup is complete, remove the DB instance from the secondary Region.
- C. Use AWS Database Migration Service (AWS DMS) to continuously replicate data to an Aurora cluster in the secondary Region. Remove the DB instance from the secondary Region.
- D. Set up an Aurora global database for the DB cluster. Specify a minimum of one DB instance in the secondary Region.

Correct Answer: D

Community vote distribution

D (52%) B (22%) 13% 13%

✉️  **jennyka76** Highly Voted 9 months, 1 week ago

Answer - A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Replication.CrossRegion.html>

Before you begin

Before you can create an Aurora MySQL DB cluster that is a cross-Region read replica, you must turn on binary logging on your source Aurora MySQL DB cluster. Cross-region replication for Aurora MySQL uses MySQL binary replication to replay changes on the cross-Region read replica DB cluster.

upvoted 8 times

✉️  **leoattf** 9 months, 1 week ago

On this same URL you provided, there is a note highlighted, stating the following:

"Replication from the primary DB cluster to all secondaries is handled by the Aurora storage layer rather than by the database engine, so lag time for replicating changes is minimal—typically, less than 1 second. Keeping the database engine out of the replication process means that the database engine is dedicated to processing workloads. It also means that you don't need to configure or manage the Aurora MySQL binlog (binary logging) replication."

So, answer should be A

upvoted 2 times

✉️  **leoattf** 9 months, 1 week ago

Correction: So, answer should be D

upvoted 2 times

✉️  **ChrisG1454** 8 months, 4 weeks ago

The question states " The DR plan must replicate data to a "secondary" AWS Region."

In addition to Aurora Replicas, you have the following options for replication with Aurora MySQL:

Aurora MySQL DB clusters in different AWS Regions.

You can replicate data across multiple Regions by using an Aurora global database. For details, see High availability across AWS Regions with Aurora global databases

You can create an Aurora read replica of an Aurora MySQL DB cluster in a different AWS Region, by using MySQL binary log (binlog) replication. Each cluster can have up to five read replicas created this way, each in a different Region.

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

upvoted 1 times

✉️  **ChrisG1454** 8 months, 3 weeks ago

The question is asking for the most cost-effective solution.

Aurora global databases are more expensive.

<https://aws.amazon.com/rds/aurora/pricing/>

upvoted 1 times

 **luisgu** Highly Voted  6 months, 1 week ago

Selected Answer: B

MOST cost-effective --> B

See section "Creating a headless Aurora DB cluster in a secondary Region" on the link
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

"Although an Aurora global database requires at least one secondary Aurora DB cluster in a different AWS Region than the primary, you can use a headless configuration for the secondary cluster. A headless secondary Aurora DB cluster is one without a DB instance. This type of configuration can lower expenses for an Aurora global database. In an Aurora DB cluster, compute and storage are decoupled. Without the DB instance, you're not charged for compute, only for storage. If it's set up correctly, a headless secondary's storage volume is kept in-sync with the primary Aurora DB cluster."

upvoted 5 times

 **bsbs1234** 2 months ago

upvoted your message, but still think D is correct. Because the question is to design a DR plan. In case of DR, B need to create an instance in DR region manually.

upvoted 1 times

 **minagaboya** Most Recent  2 weeks, 1 day ago

should be D i guess ... Migrating the database to Amazon Aurora MySQL allows for improved replication performance and higher scalability compared to Amazon RDS for MySQL. Aurora Replicas provide faster replication, reducing the replication lag, and Aurora Auto Scaling ensures that there are enough Aurora Replicas to handle the incoming traffic. Additionally, Aurora MySQL native functions can replace the stored procedures, reducing the load on the database and improving performance.

Option B is not the best solution since adding an ElastiCache for Redis cluster does not address the replication lag issue, and the cache may not have the most up-to-date information. Additionally, replacing the stored procedures with AWS Lambda functions adds additional complexity and may not improve performance.

upvoted 2 times

 **TariqKipkemei** 1 month, 2 weeks ago

Selected Answer: D

Set up an Aurora global database for the DB cluster. Specify a minimum of one DB instance in the secondary Region

upvoted 1 times

 **vini15** 4 months ago

should be B for most cost effective solution.

see the link - Achieve cost-effective multi-Region resiliency with Amazon Aurora Global Database headless clusters

<https://aws.amazon.com/blogs/database/achieve-cost-effective-multi-region-resiliency-with-amazon-aurora-global-database-headless-clusters/>

upvoted 1 times

 **Abhineet9148232** 8 months, 3 weeks ago

Selected Answer: D

D: With Amazon Aurora Global Database, you pay for replicated write I/Os between the primary Region and each secondary Region (in this case 1).

Not A because it achieves the same, would be equally costly and adds overhead.

upvoted 3 times

 **[Removed]** 8 months, 4 weeks ago

Selected Answer: C

CCCCCC

upvoted 3 times

 **Steve_4542636** 9 months ago

Selected Answer: D

I think Amazon is looking for D here. I don't think A is intended because that would require knowledge of MySQL, which isn't what they are testing us on. Not option C because the question states large volume. If the volume were low, then DMS would be better. This question is not a good question.

upvoted 3 times

 **fkie4** 8 months, 3 weeks ago

very true. Amazon wanna everyone to use AWS, why do they sell for MySQL?

upvoted 1 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: D

D provides automatic replication

upvoted 3 times

 **LuckyAro** 9 months, 1 week ago

D provides automatic replication to a secondary Region through the Aurora global database feature. This feature provides automatic replication of data across AWS Regions, with the ability to control and configure the replication process. By specifying a minimum of one DB instance in the secondary Region, you can ensure that your secondary database is always available and up-to-date, allowing for quick failover in the event of a disaster.

upvoted 2 times

 **bpd123** 9 months, 1 week ago

Selected Answer: D

Actually I change my answer to 'D' because of following:

An Aurora DB cluster can contain up to 15 Aurora Replicas. The Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans **WITHIN** an AWS Region.

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

You can replicate data across multiple Regions by using an Aurora global database

upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Replication.MySQL.html> Global database is for specific versions - they did not tell us the version

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

upvoted 1 times

 **doodledreads** 9 months, 1 week ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

Checkout the part Recovery from Region-wide outages

upvoted 1 times

 **zTopic** 9 months, 2 weeks ago

Selected Answer: A

Answer is A

upvoted 2 times

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Correct Answer: D

Community vote distribution

C (100%)

✉  **Bhawesh**  9 months, 2 weeks ago

Selected Answer: C

C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.

<https://www.examtopics.com/discussions/amazon/view/46483-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 8 times

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

Parameter Store does not provide automatic credential rotation.
upvoted 8 times

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

Selected Answer: C

Store the RDS credentials in Secrets Manager
Configure the application to retrieve the credentials from Secrets Manager
Use Secrets Manager's built-in rotation to rotate the RDS credentials automatically
upvoted 1 times

✉  **Hades2231** 3 months ago

Selected Answer: C

Secrets Manager can handle the rotation, so no need for Lambda to rotate the keys.
upvoted 1 times

✉  **chen0305_099** 3 months, 1 week ago

WHY NOT B ?
upvoted 1 times

✉  **StacyY** 3 months, 2 weeks ago

B, we need lambda for password rotation, confirmed!
upvoted 2 times

✉  **Nikki013** 3 months ago

It is not needed for certain types RDS, including MySQL as Secrets Manager has built-in rotation capabilities for it:
<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>
upvoted 2 times

✉  **Abrar2022** 5 months, 3 weeks ago

Selected Answer: C

If you need your DB to store credentials then use AWS Secret Manager. System Manager Paramater Store is for CloudFormation (no rotation)
upvoted 1 times

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

why it's not A?

upvoted 4 times

✉️ **MssP** 8 months ago

It is asking for credentials, not for encryption keys.

upvoted 4 times

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

So credentials rotation is secrets manager and key rotation is KMS?

upvoted 1 times

✉️ **bdp123** 9 months, 1 week ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>

upvoted 1 times

✉️ **LuckyAro** 9 months, 1 week ago

Selected Answer: C

C is a valid solution for securing the custom application with the least amount of programming effort. It involves creating credentials on the RDS for MySQL database for the application user and storing them in AWS Secrets Manager. The application can then be configured to load the database credentials from Secrets Manager. Additionally, the solution includes setting up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager, which will automatically rotate the credentials at a specified interval without requiring any programming effort.

upvoted 2 times

✉️ **bdp123** 9 months, 1 week ago

Selected Answer: C

https://docs.aws.amazon.com/secretsmanager/latest/userguide/create_database_secret.html

upvoted 2 times

✉️ **jennyka76** 9 months, 1 week ago

Answer - C

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>

upvoted 3 times

A media company hosts its website on AWS. The website application's architecture includes a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) and a database that is hosted on Amazon Aurora. The company's cybersecurity team reports that the application is vulnerable to SQL injection.

How should the company resolve this issue?

- A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.
- B. Create an ALB listener rule to reply to SQL injections with a fixed response.
- C. Subscribe to AWS Shield Advanced to block all SQL injection attempts automatically.
- D. Set up Amazon Inspector to block all SQL injection attempts automatically.

Correct Answer: C

Community vote distribution

A (100%)

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

Selected Answer: A

A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.

SQL Injection - AWS WAF

DDoS - AWS Shield

upvoted 17 times

 **jennyka76** Highly Voted 9 months, 1 week ago

Answer - A

<https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-common-attacks/#:~:text=To%20protect%20your%20applications%20against,%2C%20query%20string%2C%20or%20URI.>

Protect against SQL injection and cross-site scripting

To protect your applications against SQL injection and cross-site scripting (XSS) attacks, use the built-in SQL injection and cross-site scripting engines. Remember that attacks can be performed on different parts of the HTTP request, such as the HTTP header, query string, or URI. Configure the AWS WAF rules to inspect different parts of the HTTP request against the built-in mitigation engines.

upvoted 6 times

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

AWS WAF - for SQL Injection ---> A

AWS Shield - for DDOS

Amazon Inspector - for automated security assessment, like known vulnerability

upvoted 2 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: A

◦ Use AWS WAF in front of the Application Load Balancer

◦ Configure appropriate WAF web ACLs to detect and block SQL injection patterns

The key points:

◦ Website hosted on EC2 behind an ALB with Aurora database

◦ Application is vulnerable to SQL injection attacks

◦ AWS WAF is designed to detect and block SQL injection and other common web exploits. It can be placed in front of the ALB to inspect all incoming requests. WAF rules can identify malicious SQL patterns and block them.

upvoted 1 times

 **KMohsoe** 6 months, 1 week ago

Selected Answer: A

SQL injection -> WAF

upvoted 1 times

 **lexotan** 7 months, 1 week ago

Selected Answer: A

WAF is the right one

upvoted 1 times

 **akram_akram** 7 months, 3 weeks ago

Selected Answer: A

SQL Injection - AWS WAF

DDoS - AWS Shield

upvoted 1 times

✉️  **movva12** 8 months, 1 week ago

Answer C - Shield Advanced (WAF + Firewall Manager)

upvoted 1 times

✉️  **fkie4** 8 months, 3 weeks ago

Selected Answer: A

It is A. I am happy to see Amazon gives out score like this...

upvoted 2 times

✉️  **LuckyAro** 9 months, 1 week ago

Selected Answer: A

AWS WAF is a managed service that protects web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF enables customers to create custom rules that block common attack patterns, such as SQL injection attacks.

By using AWS WAF in front of the ALB and associating the appropriate web ACLs with AWS WAF, the company can protect its website application from SQL injection attacks. AWS WAF will inspect incoming traffic to the website application and block requests that match the defined SQL injection patterns in the web ACLs. This will help to prevent SQL injection attacks from reaching the application, thereby improving the overall security posture of the application.

upvoted 2 times

✉️  **LuckyAro** 9 months, 1 week ago

B, C, and D are not the best solutions for this issue. Replying to SQL injections with a fixed response

(B) is not a recommended approach as it does not actually fix the vulnerability, but only masks the issue. Subscribing to AWS Shield Advanced

(C) is useful to protect against DDoS attacks but does not protect against SQL injection vulnerabilities. Amazon Inspector

(D) is a vulnerability assessment tool and can identify vulnerabilities but cannot block attacks in real-time.

upvoted 2 times

✉️  **pbpally** 9 months, 1 week ago

Selected Answer: A

Bhawesh answers it perfect so I'm avoiding redundancy but agree on it being A.

upvoted 2 times

A company has an Amazon S3 data lake that is governed by AWS Lake Formation. The company wants to create a visualization in Amazon QuickSight by joining the data in the data lake with operational data that is stored in an Amazon Aurora MySQL database. The company wants to enforce column-level authorization so that the company's marketing team can access only a subset of columns in the database.

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

- A. Use Amazon EMR to ingest the data directly from the database to the QuickSight SPICE engine. Include only the required columns.
- B. Use AWS Glue Studio to ingest the data from the database to the S3 data lake. Attach an IAM policy to the QuickSight users to enforce column-level access control. Use Amazon S3 as the data source in QuickSight.
- C. Use AWS Glue Elastic Views to create a materialized view for the database in Amazon S3. Create an S3 bucket policy to enforce column-level access control for the QuickSight users. Use Amazon S3 as the data source in QuickSight.
- D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

Correct Answer: C

Community vote distribution

D (100%)

✉️  **K0nAn**  9 months, 1 week ago

Selected Answer: D

This solution leverages AWS Lake Formation to ingest data from the Aurora MySQL database into the S3 data lake, while enforcing column-level access control for QuickSight users. Lake Formation can be used to create and manage the data lake's metadata and enforce security and governance policies, including column-level access control. This solution then uses Amazon Athena as the data source in QuickSight to query the data in the S3 data lake. This solution minimizes operational overhead by leveraging AWS services to manage and secure the data, and by using a standard query service (Amazon Athena) to provide a SQL interface to the data.

upvoted 7 times

✉️  **jennyka76**  9 months, 2 weeks ago

Answer - D

<https://aws.amazon.com/blogs/big-data/enforce-column-level-authorization-with-amazon-quicksight-and-aws-lake-formation/>

upvoted 5 times

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

Selected Answer: D

Use a Lake Formation blueprint to ingest data from the Aurora database into the S3 data lake

Leverage Lake Formation to enforce column-level access control for the marketing team

Use Amazon Athena as the data source in QuickSight

The key points:

Need to join S3 data lake data with Aurora MySQL data

Require column-level access controls for marketing team in QuickSight

Minimize operational overhead

upvoted 1 times

✉️  **LuckyAro** 9 months, 1 week ago

Selected Answer: D

Using a Lake Formation blueprint to ingest the data from the database to the S3 data lake, using Lake Formation to enforce column-level access control for the QuickSight users, and using Amazon Athena as the data source in QuickSight. This solution requires the least operational overhead as it utilizes the features provided by AWS Lake Formation to enforce column-level authorization, which simplifies the process and reduces the need for additional configuration and maintenance.

upvoted 3 times

✉️  **Bhawesh** 9 months, 2 weeks ago

Selected Answer: D

D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

<https://www.examtopics.com/discussions/amazon/view/80865-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

A transaction processing company has weekly scripted batch jobs that run on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group. The number of transactions can vary, but the baseline CPU utilization that is noted on each run is at least 60%. The company needs to provision the capacity 30 minutes before the jobs run.

Currently, engineers complete this task by manually modifying the Auto Scaling group parameters. The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. The company needs an automated way to modify the Auto Scaling group's desired capacity.

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

- A. Create a dynamic scaling policy for the Auto Scaling group. Configure the policy to scale based on the CPU utilization metric. Set the target value for the metric to 60%.
- B. Create a scheduled scaling policy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes before the batch jobs run.
- C. Create a predictive scaling policy for the Auto Scaling group. Configure the policy to scale based on forecast. Set the scaling metric to CPU utilization. Set the target value for the metric to 60%. In the policy, set the instances to pre-launch 30 minutes before the jobs run.
- D. Create an Amazon EventBridge event to invoke an AWS Lambda function when the CPU utilization metric value for the Auto Scaling group reaches 60%. Configure the Lambda function to increase the Auto Scaling group's desired capacity and maximum capacity by 20%.

Correct Answer: C

Community vote distribution

C (63%)	B (32%)	5%
---------	---------	----

✉️  **fkie4**  8 months, 3 weeks ago

Selected Answer: C

B is NOT correct. the question said "The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts.".

answer B said "Set the appropriate desired capacity, minimum capacity, and maximum capacity". how can someone set desired capacity if he has no resources to analyze the required capacity.

Read carefully Amigo

upvoted 10 times

✉️  **omoakin** 6 months ago

scheduled scaling....

upvoted 2 times

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

But you can make a vague estimation according to the resources used; you don't need to make machine learning models to do that. You only need common sense.

upvoted 1 times

✉️  **daniel1**  1 month, 1 week ago

Selected Answer: B

From GPT4:

mong the provided options, creating a scheduled scaling policy (Option B) is the most direct and efficient way to ensure that the necessary capacity is provisioned 30 minutes before the weekly batch jobs run, with the least operational overhead. Here's a breakdown of Option B:

B. Create a scheduled scaling policy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes before the batch jobs run.

Scheduled scaling allows you to change the desired capacity of your Auto Scaling group based on a schedule. In this case, setting the recurrence to weekly and adjusting the start time to 30 minutes before the batch jobs run will ensure that the necessary capacity is available when needed, without requiring manual intervention.

upvoted 2 times

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

Selected Answer: C

Predictive scaling: increases the number of EC2 instances in your Auto Scaling group in advance of daily and weekly patterns in traffic flows. If you have regular patterns of traffic increases use predictive scaling, to help you scale faster by launching capacity in advance of forecasted load. You don't have to spend time reviewing your application's load patterns and trying to schedule the right amount of capacity using scheduled scaling. Predictive scaling uses machine learning to predict capacity requirements based on historical data from CloudWatch. The machine learning

algorithm consumes the available historical data and calculates capacity that best fits the historical load pattern, and then continuously learns based on new data to make future forecasts more accurate.

upvoted 1 times

✉  **bsbs1234** 2 months ago

should be C. Question does not say how long the job will run. don't know when to set the end time in the schedule policy.

upvoted 1 times

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

Selected Answer: C

C is correct!

upvoted 1 times

✉  **Abrar2022** 5 months, 3 weeks ago

Selected Answer: C

if the baseline CPU utilization is 60%, then that's enough information needed to determine you to predict some aspect of the usage in the future. So key word "predictive" judging by past usage.

upvoted 1 times

✉  **omoakin** 6 months ago

BBBBBBBBBBBBBBB

upvoted 1 times

✉  **ealpuche** 6 months, 3 weeks ago

Selected Answer: B

B.

you can make a vague estimation according to the resources used; you don't need to make machine-learning models to do that. You only need common sense.

upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: C

Use predictive scaling to increase the number of EC2 instances in your Auto Scaling group in advance of daily and weekly patterns in traffic flows.

Predictive scaling is well suited for situations where you have:

Cyclical traffic, such as high use of resources during regular business hours and low use of resources during evenings and weekends

Recurring on-and-off workload patterns, such as batch processing, testing, or periodic data analysis

Applications that take a long time to initialize, causing a noticeable latency impact on application performance during scale-out events
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

upvoted 1 times

✉  **neverdie** 8 months, 1 week ago

Selected Answer: B

A scheduled scaling policy allows you to set up specific times for your Auto Scaling group to scale out or scale in. By creating a scheduled scaling policy for the Auto Scaling group, you can set the appropriate desired capacity, minimum capacity, and maximum capacity, and set the recurrence to weekly. You can then set the start time to 30 minutes before the batch jobs run, ensuring that the required capacity is provisioned before the jobs run.

Option C, creating a predictive scaling policy for the Auto Scaling group, is not necessary in this scenario since the company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. This would require analyzing the required capacity trends for the Auto Scaling group counts to determine the appropriate scaling policy.

upvoted 3 times

✉  **[Removed]** 8 months ago

(typo above) C is correct..

upvoted 1 times

✉  **[Removed]** 8 months ago

B is correct. "Predictive scaling uses machine learning to predict capacity requirements based on historical data from CloudWatch.", meaning the company does not have to analyze the capacity trends themselves. <https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

upvoted 1 times

✉  **MssP** 8 months, 1 week ago

Look at fkie4 comment... no way to know desired capacity!!! -> B not correct

upvoted 1 times

✉  **Lalo** 5 months, 3 weeks ago

the text says

1.-"A transaction processing company has weekly scripted batch jobs", there is a Schedule

2.-" The company does not have the resources to analyze the required capacity trends for the Auto Scaling " Do not use the answer is B

upvoted 1 times

 **MLCL** 8 months, 2 weeks ago

Selected Answer: C

The second part of the question invalidates option B, they don't know how to procure requirements and need something to do it for them, therefore C.

upvoted 1 times

 **asoli** 8 months, 2 weeks ago

Selected Answer: C

In general, if you have regular patterns of traffic increases and applications that take a long time to initialize, you should consider using predictive scaling. Predictive scaling can help you scale faster by launching capacity in advance of forecasted load, compared to using only dynamic scaling, which is reactive in nature.

upvoted 2 times

 **Whericanstart** 8 months, 2 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

upvoted 3 times

 **UnluckyDucky** 8 months, 3 weeks ago

Selected Answer: B

"The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts"

Using predictive schedule seems appropriate here, however the question says the company doesn't have the resources to analyze this, even though forecast does it for you using ML.

The job runs weekly therefore the easiest way to achieve this with the LEAST operational overhead, seems to be scheduled scaling.

Both solutions achieve the goal, B imho does it better, considering the limitations.

Predictive Scaling:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

Scheduled Scaling:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>

upvoted 2 times

 **samcloudaws** 8 months, 3 weeks ago

Selected Answer: B

Scheduled scaling seems mostly simplest way to solve this

upvoted 4 times

 **Steve_4542636** 9 months ago

Selected Answer: C

"The company needs to provision the capacity 30 minutes before the jobs run." This means the ASG group needs to scale BEFORE the CPU utilization hits 60%. Dynamic scaling only responds to a scaling metric setup such as average CPU utilization at 60% for 5 minutes. The forecasting option is automatic, however, it does require some time for it to be effective since it needs the EC2 utilization in the past to predict the future.

upvoted 2 times

 **nder** 9 months ago

Selected Answer: A

Dynamic Scaling policy is the least operational overhead.

upvoted 1 times

A solutions architect is designing a company's disaster recovery (DR) architecture. The company has a MySQL database that runs on an Amazon EC2 instance in a private subnet with scheduled backup. The DR design needs to include multiple AWS Regions.

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

- A. Migrate the MySQL database to multiple EC2 instances. Configure a standby EC2 instance in the DR Region. Turn on replication.
- B. Migrate the MySQL database to Amazon RDS. Use a Multi-AZ deployment. Turn on read replication for the primary DB instance in the different Availability Zones.
- C. Migrate the MySQL database to an Amazon Aurora global database. Host the primary DB cluster in the primary Region. Host the secondary DB cluster in the DR Region.
- D. Store the scheduled backup of the MySQL database in an Amazon S3 bucket that is configured for S3 Cross-Region Replication (CRR). Use the data backup to restore the database in the DR Region.

Correct Answer: B

Community vote distribution

C (100%)

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

Selected Answer: C

LEAST operational overhead = Serverless = Amazon Aurora global database
upvoted 1 times

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

Selected Answer: C

Amazon Aurora global database can span and replicate DB Servers between multiple AWS Regions. And also compatible with MySQL.
upvoted 1 times

✉️  **GalileoEC2** 8 months, 1 week ago

C, Why B? B is multi zone in one region, C is multi region as it was requested
upvoted 1 times

✉️  **lucdt4** 6 months, 1 week ago

" The DR design needs to include multiple AWS Regions."
with the requirement "DR SITE multiple AWS region" -> B is wrong, because it deploy multy AZ (this is not multi region)
upvoted 1 times

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

Selected Answer: C

A. Multiple EC2 instances to be configured and updated manually in case of DR.
B. Amazon RDS=Multi-AZ while it asks to be multi-region
C. correct, see comment from LuckyAro
D. Manual process to start the DR, therefore same limitation as answer A
upvoted 4 times

✉️  **KZM** 9 months ago

Amazon Aurora global database can span and replicate DB Servers between multiple AWS Regions. And also compatible with MySQL.
upvoted 3 times

✉️  **LuckyAro** 9 months, 1 week ago

C: Migrate MySQL database to an Amazon Aurora global database is the best solution because it requires minimal operational overhead. Aurora is a managed service that provides automatic failover, so standby instances do not need to be manually configured. The primary DB cluster can be hosted in the primary Region, and the secondary DB cluster can be hosted in the DR Region. This approach ensures that the data is always available and up-to-date in multiple Regions, without requiring significant manual intervention.

upvoted 3 times

✉️  **LuckyAro** 9 months, 1 week ago

With dynamic scaling, the Auto Scaling group will automatically adjust the number of instances based on the actual workload. The target value for the CPU utilization metric is set to 60%, which is the baseline CPU utilization that is noted on each run, indicating that this is a reasonable level of utilization for the workload. This solution does not require any scheduling or forecasting, reducing the operational overhead.

upvoted 1 times

✉️  **LuckyAro** 9 months, 1 week ago

Sorry, Posted right answer to the wrong question, mistakenly clicked the next question, sorry.

upvoted 4 times

✉  **geekgirl22** 9 months, 1 week ago

C is the answer as RDS is only multi-zone not multi region.

upvoted 1 times

✉  **bdp123** 9 months, 1 week ago

Selected Answer: C

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

upvoted 1 times

✉  **SMAZ** 9 months, 1 week ago

C

option A has operation overhead whereas option C not.

upvoted 1 times

✉  **alexman** 9 months, 1 week ago

Selected Answer: C

C mentions multiple regions. Option B is within the same region

upvoted 3 times

✉  **jennyka76** 9 months, 1 week ago

ANSWER - B ?? NOT SURE

upvoted 1 times

A company has a Java application that uses Amazon Simple Queue Service (Amazon SQS) to parse messages. The application cannot parse messages that are larger than 256 KB in 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 SQS 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 Amazon SQS.
- 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.

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

A. Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.

Amazon SQS has a limit of 256 KB for the size of messages. To handle messages larger than 256 KB, the Amazon SQS Extended Client Library for Java can be used. This library allows messages larger than 256 KB to be stored in Amazon S3 and provides a way to retrieve and process them. Using this solution, the application code can remain largely unchanged while still being able to process messages up to 50 MB in size.

upvoted 7 times

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

Selected Answer: A

The Amazon SQS Extended Client Library for Java enables you to manage Amazon SQS message payloads with Amazon S3. This is especially useful for storing and retrieving messages with a message payload size greater than the current SQS limit of 256 KB, up to a maximum of 2 GB.

upvoted 1 times

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

Selected Answer: A

The SQS Extended Client Library enables storing large payloads in S3 while referenced via SQS. The application code can stay almost entirely unchanged - it sends/receives SQS messages normally. The library handles transparently routing the large payloads to S3 behind the scenes

upvoted 1 times

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

Selected Answer: A

Quote "The Amazon SQS Extended Client Library for Java enables you to manage Amazon SQS message payloads with Amazon S3." and "An extension to the Amazon SQS client that enables sending and receiving messages up to 2GB via Amazon S3." at <https://github.com/awslabs/amazon-sqs-java-extended-client-lib>

upvoted 1 times

✉️  **Abrar2022** 5 months, 3 weeks ago

Selected Answer: A

Amazon SQS has a limit of 256 KB for the size of messages.

To handle messages larger than 256 KB, the Amazon SQS Extended Client Library for Java can be used.

upvoted 1 times

✉️  **gold4otas** 8 months ago

The Amazon SQS Extended Client Library for Java enables you to publish messages that are greater than the current SQS limit of 256 KB, up to a maximum of 2 GB.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-s3-messages.html>

upvoted 1 times

✉️  **bdp123** 9 months, 1 week ago

Selected Answer: A

<https://github.com/awslabs/amazon-sqs-java-extended-client-lib>

upvoted 3 times

 **Arathore** 9 months, 1 week ago

Selected Answer: A

To send messages larger than 256 KiB, you can use the Amazon SQS Extended Client Library for Java. This library allows you to send an Amazon SQS message that contains a reference to a message payload in Amazon S3. The maximum payload size is 2 GB.

upvoted 4 times

 **Neha999** 9 months, 1 week ago

A

For messages > 256 KB, use Amazon SQS Extended Client Library for Java

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/quotas-messages.html>

upvoted 4 times

A company wants to restrict access to the content of one of its main web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture and an authentication solution for fewer than 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as the company's user base grows while providing the lowest login latency possible.

Which solution will meet these requirements MOST cost-effectively?

- A. Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally.
- B. Use AWS Directory Service for Microsoft Active Directory for authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.
- C. Use Amazon Cognito for authentication. Use AWS Lambda for authorization. Use Amazon S3 Transfer Acceleration to serve the web application globally.
- D. Use AWS Directory Service for Microsoft Active Directory for authentication. Use Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

CloudFront=globally
Lambda@edge = Authorization/ Latency
Cognito=Authentication for Web apps
upvoted 8 times

 **TariqKipkemei** Most Recent 1 month, 2 weeks ago

Selected Answer: A

Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally
upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: A

Amazon Cognito is a serverless authentication service that can be used to easily add user sign-up and authentication to web and mobile apps. It is a good choice for this scenario because it is scalable and can handle a small number of users without any additional costs.

Lambda@Edge is a serverless compute service that can be used to run code at the edge of the AWS network. It is a good choice for this scenario because it can be used to perform authorization checks at the edge, which can improve the login latency.

Amazon CloudFront is a content delivery network (CDN) that can be used to serve web content globally. It is a good choice for this scenario because it can cache web content closer to users, which can improve the performance of the web application.

upvoted 1 times

 **antropaws** 6 months ago

Selected Answer: A

A is perfect.
upvoted 1 times

 **kraken21** 8 months ago

Selected Answer: A

Lambda@Edge for authorization
<https://aws.amazon.com/blogs/networking-and-content-delivery/adding-http-security-headers-using-lambdaedge-and-amazon-cloudfront/>
upvoted 2 times

 **LuckyAro** 9 months, 1 week ago

Selected Answer: A

Amazon CloudFront is a global content delivery network (CDN) service that can securely deliver web content, videos, and APIs at scale. It integrates with Cognito for authentication and with Lambda@Edge for authorization, making it an ideal choice for serving web content globally.

Lambda@Edge is a service that lets you run AWS Lambda functions globally closer to users, providing lower latency and faster response times. It

can also handle authorization logic at the edge to secure content in CloudFront. For this scenario, Lambda@Edge can provide authorization for the web application while leveraging the low-latency benefit of running at the edge.

upvoted 2 times

 **bdp123** 9 months, 1 week ago

Selected Answer: A
CloudFront to serve globally
upvoted 1 times

 **SMAZ** 9 months, 1 week ago

A
Amazon Cognito for authentication and Lambda@Edge for authorization, Amazon CloudFront to serve the web application globally provides low-latency content delivery
upvoted 3 times

A company has an aging network-attached storage (NAS) array in its data center. The NAS array presents SMB shares and NFS shares to client workstations. The company does not want to purchase a new NAS array. The company also does not want to incur the cost of renewing the NAS array's support contract. Some of the data is accessed frequently, but much of the data is inactive.

A solutions architect needs to implement a solution that migrates the data to Amazon S3, uses S3 Lifecycle policies, and maintains the same look and feel for the client workstations. The solutions architect has identified AWS Storage Gateway as part of the solution.

Which type of storage gateway should the solutions architect provision to meet these requirements?

- A. Volume Gateway
- B. Tape Gateway
- C. Amazon FSx File Gateway
- D. Amazon S3 File Gateway

Correct Answer: C

Community vote distribution

D (100%)

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

Selected Answer: D

Amazon S3 File Gateway provides on-premises applications with access to virtually unlimited cloud storage using NFS and SMB file interfaces. It seamlessly moves frequently accessed data to a low-latency cache while storing colder data in Amazon S3, using S3 Lifecycle policies to transition data between storage classes over time.

In this case, the company's aging NAS array can be replaced with an Amazon S3 File Gateway that presents the same NFS and SMB shares to the client workstations. The data can then be migrated to Amazon S3 and managed using S3 Lifecycle policies

upvoted 7 times

 **TariqKipkemei** Most Recent 1 month, 2 weeks ago

Selected Answer: D

The Amazon S3 File Gateway enables you to store and retrieve objects in Amazon Simple Storage Service (S3) using file protocols such as Network File System (NFS) and Server Message Block (SMB).

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: D

It provides an easy way to lift-and-shift file data from the existing NAS to Amazon S3. The S3 File Gateway presents SMB and NFS file shares that client workstations can access just like the NAS shares.

Behind the scenes, it moves the file data to S3 storage, storing it durably and cost-effectively.

S3 Lifecycle policies can be used to transition less frequently accessed data to lower-cost S3 storage tiers like S3 Glacier.

From the client workstation perspective, access to files feels seamless and unchanged after migration to S3. The S3 File Gateway handles the underlying data transfers.

It is a simple, low-cost gateway option tailored for basic file share migration use cases.

upvoted 1 times

 **james2033** 4 months, 2 weeks ago

Selected Answer: D

- Volume Gateway: <https://aws.amazon.com/storagegateway/volume/> (Remove A, related iSCSI)

- Tape Gateway <https://aws.amazon.com/storagegateway/vtl/> (Remove B)

- Amazon FSx File Gateway <https://aws.amazon.com/storagegateway/file/fsx/> (C)

- Why not choose C? Because need working with Amazon S3. (Answer D, and it is correct answer) <https://aws.amazon.com/storagegateway/file/s3/>

upvoted 2 times

 **siyam008** 8 months, 4 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/storage/how-to-create-smb-file-shares-with-aws-storage-gateway-using-hyper-v/>

upvoted 2 times

 **bdp123** 9 months, 1 week ago

Selected Answer: D

<https://aws.amazon.com/about-aws/whats-new/2018/06/aws-storage-gateway-adds-smb-support-to-store-objects-in-amazon-s3/>
upvoted 2 times

 **everfly** 9 months, 1 week ago

Selected Answer: D

Amazon S3 File Gateway provides a file interface to objects stored in S3. It can be used for a file-based interface with S3, which allows the company to migrate their NAS array data to S3 while maintaining the same look and feel for client workstations. Amazon S3 File Gateway supports SMB and NFS protocols, which will allow clients to continue to access the data using these protocols. Additionally, Amazon S3 Lifecycle policies can be used to automate the movement of data to lower-cost storage tiers, reducing the storage cost of inactive data.

upvoted 3 times

A company has an application that is running on Amazon EC2 instances. A solutions architect has standardized the company on a particular instance family and various instance sizes based on the current needs of the company.

The company wants to maximize cost savings for the application over the next 3 years. The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage.

Which solution will meet these requirements MOST cost-effectively?

- A. Compute Savings Plan
- B. EC2 Instance Savings Plan
- C. Zonal Reserved Instances
- D. Standard Reserved Instances

Correct Answer: D

Community vote distribution

A (67%)	B (31%)
---------	---------

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

Selected Answer: A

Read Carefully guys , They need to be able to change FAMILY , and although EC2 Savings has a higher discount , its clearly documented as not allowed >

EC2 Instance Savings Plans provide savings up to 72 percent off On-Demand, in exchange for a commitment to a specific instance family in a chosen AWS Region (for example, M5 in Virginia). These plans automatically apply to usage regardless of size (for example, m5.xlarge, m5.2xlarge, etc.), OS (for example, Windows, Linux, etc.), and tenancy (Host, Dedicated, Default) within the specified family in a Region.

upvoted 12 times

 **FFO** 7 months, 1 week ago

Savings Plans are a flexible pricing model that offer low prices on Amazon EC2, AWS Lambda, and AWS Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in \$/hour) for a 1 or 3 year term. When you sign up for a Savings Plan, you will be charged the discounted Savings Plans price for your usage up to your commitment.

The company wants savings over the next 3 years but wants to change the instance type in 6 months. This invalidates A

upvoted 2 times

 **FFO** 7 months, 1 week ago

Disregard! found more information:

We recommend Savings Plans (over Reserved Instances). Like Reserved Instances, Savings Plans offer lower prices (up to 72% savings compared to On-Demand Instance pricing). In addition, Savings Plans offer you the flexibility to change your usage as your needs evolve. For example, with Compute Savings Plans, lower prices will automatically apply when you change from C4 to C6g instances, shift a workload from EU (Ireland) to EU (London), or move a workload from Amazon EC2 to AWS Fargate or AWS Lambda.

<https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/>

upvoted 1 times

 **hungta** Most Recent 1 week, 3 days ago

Selected Answer: B

EC2 Instance Savings Plans is most saving. And it is enough for required flexibility

EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% (just like Standard RIs) in exchange for commitment to usage of individual instance families in a Region (for example, M5 usage in N. Virginia). This automatically reduces your cost on the selected instance family in that region regardless of AZ, size, operating system, or tenancy. EC2 Instance Savings Plans give you the flexibility to change your usage between instances within a family in that Region. For example, you can move from c5.xlarge running Windows to c5.2xlarge running Linux and automatically benefit from the Savings Plans prices.

upvoted 1 times

 **dilaaziz** 1 week, 5 days ago

Selected Answer: A

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-reservation-models/savings-plans.html>

upvoted 1 times

 **EdenWang** 2 weeks, 6 days ago

Selected Answer: B

The most cost-effective solution that meets the company's requirements would be B. EC2 Instance Savings Plan.

EC2 Instance Savings Plans provide significant cost savings, allowing the company to commit to a consistent amount of usage (measured in \$/hour) for a 1- or 3-year term, and in return, receive a discount on the hourly rate for the instances that match the attributes of the plan.

With EC2 Instance Savings Plans, the company can benefit from the flexibility to change the instance family and sizes over the next 3 years, which aligns with their requirement to adjust based on application popularity and usage.

This option provides the best balance of cost savings and flexibility, making it the most suitable choice for the company's needs.

upvoted 2 times

 **TariqKipkemei** 1 month, 2 weeks ago

Selected Answer: A

Change instance family = Compute Savings Plans

upvoted 1 times

 **Wayne23Fang** 2 months, 3 weeks ago

Selected Answer: A

D is not right. D. Standard Reserved Instances. should be Convertible Reserved Instances if you need additional flexibility, such as the ability to use different instance families, operating systems.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

The key factors are:

Need to maximize cost savings over 3 years

Ability to change instance family and sizes in 6 months

Standardized on a particular instance family for now

upvoted 2 times

 **Kiki_Pass** 4 months ago

Why not C? Can do with Convertible Reserved Instance

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-types.html>

upvoted 1 times

 **ITV2021** 4 months, 1 week ago

Selected Answer: A

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 1 times

 **Mia2009687** 4 months, 3 weeks ago

Selected Answer: A

EC2 Instance Savings Plan cannot change the family.

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

upvoted 1 times

 **mattcl** 5 months, 1 week ago

Answer D: You can use Standard Reserved Instances when you know that you need a specific instance type.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: A

Savings Plans offer a flexible pricing model that provides savings on AWS usage. You can save up to 72 percent on your AWS compute workloads. Compute Savings Plans provide lower prices on Amazon EC2 instance usage regardless of instance family, size, OS, tenancy, or AWS Region. This also applies to AWS Fargate and AWS Lambda usage. SageMaker Savings Plans provide you with lower prices for your Amazon SageMaker instance usage, regardless of your instance family, size, component, or AWS Region.

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

upvoted 2 times

 **kruasan** 7 months ago

With an EC2 Instance Savings Plan, you can change your instance size within the instance family (for example, from c5.xlarge to c5.2xlarge) or the operating system (for example, from Windows to Linux), or move from Dedicated tenancy to Default and continue to receive the discounted rate provided by your EC2 Instance Savings Plan.

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

upvoted 1 times

 **kruasan** 7 months ago

The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage. Therefore EC2 Instance Savings Plan prerequisites are not fulfilled

upvoted 1 times

 **SkyZeroZx** 7 months ago

Selected Answer: B

EC2 Instance Savings Plan

upvoted 1 times

 **lexotan** 7 months, 1 week ago

Selected Answer: D

Why not D. you can change instance type and classes
upvoted 1 times

✉  **bdp123** 9 months, 1 week ago

Selected Answer: A

<https://aws.amazon.com/savingsplans/compute-pricing/>
upvoted 3 times

✉  **everfly** 9 months, 1 week ago

Selected Answer: A

Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, Region, OS or tenancy, and also apply to Fargate or Lambda usage.

EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% in exchange for commitment to usage of individual instance families in a Region

<https://aws.amazon.com/savingsplans/compute-pricing/>
upvoted 4 times

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

Selected Answer: A

Compute Savings plans are most flexible - lets you change the instance types vs EC2 Savings plans offer best savings.
upvoted 2 times

A company collects data from a large number of participants who use wearable devices. The company stores the data in an Amazon DynamoDB table and uses applications to analyze the data. The data workload is constant and predictable. The company wants to stay at or below its forecasted budget for DynamoDB.

Which solution will meet these requirements MOST cost-effectively?

- A. Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA). Reserve capacity for the forecasted workload.
- B. Use provisioned mode. Specify the read capacity units (RCUs) and write capacity units (WCUs).
- C. Use on-demand mode. Set the read capacity units (RCUs) and write capacity units (WCUs) high enough to accommodate changes in the workload.
- D. Use on-demand mode. Specify the read capacity units (RCUs) and write capacity units (WCUs) with reserved capacity.

Correct Answer: A

Community vote distribution

B (82%)

A (18%)

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

Selected Answer: B

The data workload is constant and predictable.

upvoted 5 times

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

Selected Answer: B

I think it is not possible to set Read Capacity Units(RCU)/Write Capacity Units(WCU) in on-demand mode.

upvoted 1 times

 **wsdasdasdqwdaw** 1 month, 1 week ago

predictable/constant => provisioned mode. On-demand mode is more suitable for workloads that are unpredictable and can vary widely from minute to minute.

The use case is not for Standard-IA which is described here: <https://aws.amazon.com/dynamodb/standard-ia/>

=> Option B

upvoted 2 times

 **TariqKipkemei** 1 month, 2 weeks ago

Selected Answer: B

I rule out A because of this 'Standard-Infrequent Access ', clearly the company uses applications to analyze the data.

The data workload is constant and predictable making provisioned mode the best option.

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: A

Option B lacks the cost benefits of Standard-IA.

Option C uses more expensive on-demand pricing.

Option D does not actually allow reserving capacity with on-demand mode.

So option A leverages provisioned mode, Standard-IA, and reserved capacity to meet the requirements in a cost-optimal way.

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: A

A is correct!

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Sorry, A will not work, since Reserved Capacity can only be used with DynamoDB Standard table class. So, B is right for this case.

upvoted 1 times

 **UNGMAN** 8 months, 2 weeks ago

Selected Answer: B

예측가능..

upvoted 4 times

✉ **kayodea25** 8 months, 3 weeks ago

Option C is the most cost-effective solution for this scenario. In on-demand mode, DynamoDB automatically scales up or down based on the current workload, so the company only pays for the capacity it uses. By setting the RCU and WCU high enough to accommodate changes in the workload, the company can ensure that it always has the necessary capacity without overprovisioning and incurring unnecessary costs. Since the workload is constant and predictable, using provisioned mode with reserved capacity (Options A and D) may result in paying for unused capacity during periods of low demand. Option B, using provisioned mode without reserved capacity, may result in throttling during periods of high demand if the provisioned capacity is not sufficient to handle the workload.

upvoted 2 times

✉ **Bofi** 8 months, 1 week ago

Kayode olode..lol

upvoted 1 times

✉ **boxu03** 8 months, 2 weeks ago

you forgot "The data workload is constant and predictable", should be B

upvoted 2 times

✉ **Steve_4542636** 9 months ago

"The data workload is constant and predictable."

<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>

"With provisioned capacity you pay for the provision of read and write capacity units for your DynamoDB tables. Whereas with DynamoDB on-demand you pay per request for the data reads and writes that your application performs on your tables."

upvoted 1 times

✉ **Charly0710** 9 months ago

Selected Answer: B

The data workload is constant and predictable, then, isn't on-demand mode.

DynamoDB Standard-IA is not necessary in this context

upvoted 1 times

✉ **Lonojack** 9 months, 1 week ago

Selected Answer: B

The problem with (A) is: "Standard-Infrequent Access". In the question, they say the company has to analyze the Data.

That's why the Correct answer is (B)

upvoted 3 times

✉ **bdp123** 9 months, 1 week ago

Selected Answer: A

workload is constant

upvoted 2 times

✉ **Lonojack** 9 months, 1 week ago

The problem with (A) is: "Standard-Infrequent Access".

In the question, they say the company has to analyze the Data.

Correct answer is (B)

upvoted 2 times

✉ **Samuel03** 9 months, 1 week ago

Selected Answer: B

As the numbers are already known

upvoted 3 times

A company stores confidential data in an Amazon Aurora PostgreSQL database in the ap-southeast-3 Region. The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The company was recently acquired and must securely share a backup of the database with the acquiring company's AWS account in ap-southeast-3.

What should a solutions architect do to meet these requirements?

- A. Create a database snapshot. Copy the snapshot to a new unencrypted snapshot. Share the new snapshot with the acquiring company's AWS account.
- B. Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.
- C. Create a database snapshot that uses a different AWS managed KMS key. Add the acquiring company's AWS account to the KMS key alias. Share the snapshot with the acquiring company's AWS account.
- D. Create a database snapshot. Download the database snapshot. Upload the database snapshot to an Amazon S3 bucket. Update the S3 bucket policy to allow access from the acquiring company's AWS account.

Correct Answer: B

Community vote distribution

B (100%)

 **TariqKipkemei** 1 month, 2 weeks ago

Selected Answer: B

Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.

upvoted 1 times

 **Vuuu** 4 months ago

Selected Answer: B

B. Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account. Most Voted

upvoted 1 times

 **Abrar2022** 5 months, 3 weeks ago

Create a database snapshot of the encrypted. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.

upvoted 1 times

 **Abrar2022** 5 months, 3 weeks ago

Selected Answer: B

A. - "So let me get this straight, with the current company the data is protected and encrypted. However, for the acquiring company the data is unencrypted? How is that fair?"

C - Wouldn't recommended this option because using a different AWS managed KMS key will not allow the acquiring company's AWS account to access the encrypted data.

D. - Don't risk it for a biscuit and get fired!!!! - by downloading the database snapshot and uploading it to an Amazon S3 bucket. This will increase the risk of data leakage or loss of confidentiality during the transfer process.

B - CORRECT

upvoted 3 times

 **SkyZeroZx** 6 months, 4 weeks ago

Selected Answer: B

To securely share a backup of the database with the acquiring company's AWS account in the same Region, a solutions architect should create a database snapshot, add the acquiring company's AWS account to the AWS KMS key policy, and share the snapshot with the acquiring company's AWS account.

Option A, creating an unencrypted snapshot, is not recommended as it will compromise the confidentiality of the data. Option C, creating a snapshot that uses a different AWS managed KMS key, does not provide any additional security and will unnecessarily complicate the solution. Option D, downloading the database snapshot and uploading it to an S3 bucket, is not secure as it can expose the data during transit.

Therefore, the correct option is B: Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.

upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: B

Option B is the correct answer.

Option A is not recommended because copying the snapshot to a new unencrypted snapshot will compromise the confidentiality of the data.

Option C is not recommended because using a different AWS managed KMS key will not allow the acquiring company's AWS account to access the encrypted data.

Option D is not recommended because downloading the database snapshot and uploading it to an Amazon S3 bucket will increase the risk of data leakage or loss of confidentiality during the transfer process.

upvoted 1 times

 **Steve_4542636** 9 months ago

Selected Answer: B

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html>

upvoted 1 times

 **geekgirl122** 9 months, 1 week ago

It is C, you have to create a new key. Read below

You can't share a snapshot that's encrypted with the default AWS KMS key. You must create a custom AWS KMS key instead. To share an encrypted Aurora DB cluster snapshot:

Create a custom AWS KMS key.

Add the target account to the custom AWS KMS key.

Create a copy of the DB cluster snapshot using the custom AWS KMS key. Then, share the newly copied snapshot with the target account.

Copy the shared DB cluster snapshot from the target account

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

upvoted 1 times

 **KZM** 9 months, 1 week ago

Yes, as per the given information "The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key", it may not be the default AWS KMS key.

upvoted 1 times

 **KZM** 9 months, 1 week ago

Yes, can't share a snapshot that's encrypted with the default AWS KMS key.

But as per the given information "The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key", it may not be the default AWS KMS key.

upvoted 3 times

 **enzomv** 8 months, 3 weeks ago

I agree with KZM.

It is B.

There's no need to create another custom AWS KMS key.

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

Give target account access to the custom AWS KMS key within the source account

1. Log in to the source account, and go to the AWS KMS console in the same Region as the DB cluster snapshot.

2. Select Customer-managed keys from the navigation pane.

3. Select your custom AWS KMS key (ALREADY CREATED)

4. From the Other AWS accounts section, select Add another AWS account, and then enter the AWS account number of your target account.

Then:

Copy and share the DB cluster snapshot

upvoted 2 times

 **leoattf** 9 months, 1 week ago

I also thought straight away that it could be C, however, the questions mentions that the database is encrypted with an AWS KMS custom key already. So maybe the letter B could be right, since it already has a custom key, not the default KMS Key.

What do you think?

upvoted 3 times

 **enzomv** 8 months, 3 weeks ago

It is B.

There's no need to create another custom AWS KMS key.

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

Give target account access to the custom AWS KMS key within the source account

1. Log in to the source account, and go to the AWS KMS console in the same Region as the DB cluster snapshot.

2. Select Customer-managed keys from the navigation pane.

3. Select your custom AWS KMS key (ALREADY CREATED)

4. From the Other AWS accounts section, select Add another AWS account, and then enter the AWS account number of your target account.

Then:

Copy and share the DB cluster snapshot

upvoted 2 times

 **nyx12345** 9 months, 1 week ago

Is it bad that in answer B the acquiring company is using the same KMS key? Should a new KMS key not be used?

upvoted 2 times

 **geekgirl22** 9 months, 1 week ago

Yes, you are right, read my comment above.
upvoted 1 times

 **bsbs1234** 2 months ago

I think I would agree with you if option C say using a new "customer managed key" instead of AWS managed key
upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>
upvoted 2 times

 **jennyka76** 9 months, 1 week ago

ANSWER - B
upvoted 1 times

A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east-1 Region to store customer transactions. The company needs high availability and automatic recovery for the DB instance.

The company must also run reports on the RDS database several times a year. The report process causes transactions to take longer than usual to post to the customers' accounts. The company needs a solution that will improve the performance of the report process.

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

- A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.
- B. Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.
- C. Create a read replica of the DB instance in a different Availability Zone. Point all requests for reports to the read replica.
- D. Migrate the database to RDS Custom.
- E. Use RDS Proxy to limit reporting requests to the maintenance window.

Correct Answer: AC

Community vote distribution

AC (100%)

 **elearningtakai** Highly Voted 8 months ago

A and C are the correct choices.
B. It will not help improve the performance of the report process.
D. Migrating to RDS Custom does not address the issue of high availability and automatic recovery.
E. RDS Proxy can help with scalability and high availability but it does not address the issue of performance for the report process. Limiting the reporting requests to the maintenance window will not provide the required availability and recovery for the DB instance.

upvoted 5 times

 **TariqKipkemei** Most Recent 1 month, 2 weeks ago

Selected Answer: AC

Create a Multi-AZ deployment, create a read replica of the DB instance in the second Availability Zone, point all requests for reports to the read replica

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: AC

The correct answers are A and C.

A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment. This will provide high availability and automatic recovery for the DB instance. If the primary DB instance fails, the standby DB instance will automatically become the primary DB instance. This will ensure that the database is always available.

C. Create a read replica of the DB instance in a different Availability Zone. Point all requests for reports to the read replica. This will improve the performance of the report process by offloading the read traffic from the primary DB instance to the read replica. The read replica is a fully synchronized copy of the primary DB instance, so the reports will be accurate.

upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: AC

A and C.

upvoted 2 times

 **WhericanIstart** 8 months, 2 weeks ago

Selected Answer: AC

Options A & C...

upvoted 3 times

 **KZM** 9 months, 1 week ago

Options A+C

upvoted 2 times

 **bdp123** 9 months, 1 week ago

Selected Answer: AC

<https://medium.com/awesome-cloud/aws-difference-between-multi-az-and-read-replicas-in-amazon-rds-60fe848ef53a>

upvoted 2 times

 **jennyka76** 9 months, 1 week ago

ANSWER - A & C

upvoted 3 times

A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to be more distributed and to use serverless concepts while performing the different aspects of the workflow. The company also wants to minimize operational overhead.

Which solution will meet these requirements?

- A. Build out the workflow in AWS Glue. Use AWS Glue to invoke AWS Lambda functions to process the workflow steps.
- B. Build out the workflow in AWS Step Functions. Deploy the application on Amazon EC2 instances. Use Step Functions to invoke the workflow steps on the EC2 instances.
- C. Build out the workflow in Amazon EventBridge. Use EventBridge to invoke AWS Lambda functions on a schedule to process the workflow steps.
- D. Build out the workflow in AWS Step Functions. Use Step Functions to create a state machine. Use the state machine to invoke AWS Lambda functions to process the workflow steps.

Correct Answer: D

Community vote distribution

D (84%)

C (16%)

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

Selected Answer: D

This is why I'm voting D.....QUESTION ASKED FOR IT TO: use serverless concepts while performing the different aspects of the workflow. Is option D utilizing Serverless concepts?

upvoted 8 times

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

Selected Answer: D

One of the use cases for step functions is to Automate extract, transform, and load (ETL) processes.

<https://aws.amazon.com/step-functions/#:~:text=for%20modern%20applications.-,Use%20cases,-Automate%20extract%2C%20transform>

upvoted 1 times

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

Selected Answer: D

AWS Step functions is serverless Visual workflows for distributed applications

<https://aws.amazon.com/step-functions/>

upvoted 1 times

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

Selected Answer: D

Step Functions is based on state machines and tasks. A state machine is a workflow. A task is a state in a workflow that represents a single unit of work that another AWS service performs. Each step in a workflow is a state.

Depending on your use case, you can have Step Functions call AWS services, such as Lambda, to perform tasks.

<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html>

upvoted 2 times

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

Answer is D.

Step Functions is based on state machines and tasks. A state machine is a workflow. A task is a state in a workflow that represents a single unit of work that another AWS service performs. Each step in a workflow is a state.

Depending on your use case, you can have Step Functions call AWS services, such as Lambda, to perform tasks.

<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html>

upvoted 1 times

✉️  **Karlos99** 8 months, 4 weeks ago

Selected Answer: C

There are two main types of routers used in event-driven architectures: event buses and event topics. At AWS, we offer Amazon EventBridge to build event buses and Amazon Simple Notification Service (SNS) to build event topics. <https://aws.amazon.com/event-driven-architecture/>

upvoted 1 times

✉️  **TungPham** 9 months ago

Selected Answer: D

Step 3: Create a State Machine

Use the Step Functions console to create a state machine that invokes the Lambda function that you created earlier in Step 1.

<https://docs.aws.amazon.com/step-functions/latest/dg/tutorial-creating-lambda-state-machine.html>

In Step Functions, a workflow is called a state machine, which is a series of event-driven steps. Each step in a workflow is called a state.

upvoted 2 times

✉ **Bilalazure** 9 months, 1 week ago

Selected Answer: D

Distrubuted****

upvoted 1 times

✉ **geekgirl22** 9 months, 1 week ago

It is D. Cannot be C because C is "scheduled"

upvoted 4 times

✉ **Americo32** 9 months, 1 week ago

Selected Answer: C

Vou de C, orientada a eventos

upvoted 2 times

✉ **MssP** 8 months ago

It is true that an Event-driven is made with EventBridge but with a Lambda on schedule??? It is a mismatch, isn't it?

upvoted 2 times

✉ **kraken21** 8 months ago

Tricky question huh!

upvoted 2 times

✉ **bdp123** 9 months, 1 week ago

Selected Answer: D

AWS Step functions is serverless Visual workflows for distributed applications

<https://aws.amazon.com/step-functions/>

upvoted 1 times

✉ **leoattf** 9 months ago

Besides, "Visualize and develop resilient workflows for EVENT-DRIVEN architectures."

upvoted 1 times

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

Could it be a C because it's event-driven architecture?

upvoted 3 times

✉ **SMAZ** 9 months, 1 week ago

Option D..

AWS Step functions are used for distributed applications

upvoted 2 times

A company is designing the network for an online multi-player game. The game uses the UDP networking protocol and will be deployed in eight AWS Regions. The network architecture needs to minimize latency and packet loss to give end users a high-quality gaming experience.

Which solution will meet these requirements?

- A. Setup a transit gateway in each Region. Create inter-Region peering attachments between each transit gateway.
- B. Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.
- C. Set up Amazon CloudFront with UDP turned on. Configure an origin in each Region.
- D. Set up a VPC peering mesh between each Region. Turn on UDP for each VPC.

Correct Answer: B

Community vote distribution

B (100%)

✉  **lucdt4**  6 months, 1 week ago

Selected Answer: B

AWS Global Accelerator = TCP/UDP minimize latency
upvoted 7 times

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

Selected Answer: B

Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.
upvoted 1 times

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

Selected Answer: B

Connect to up to 10 regions within the AWS global network using the AWS Global Accelerator.
upvoted 1 times

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

UDP = Global Accelerator
upvoted 1 times

✉  **OAdeku**le 7 months ago

General

Q: What is AWS Global Accelerator?

A: AWS Global Accelerator is a networking service that helps you improve the availability and performance of the applications that you offer to your global users. AWS Global Accelerator is easy to set up, configure, and manage. It provides static IP addresses that provide a fixed entry point to your applications and eliminate the complexity of managing specific IP addresses for different AWS Regions and Availability Zones. AWS Global Accelerator always routes user traffic to the optimal endpoint based on performance, reacting instantly to changes in application health, your user's location, and policies that you configure. You can test the performance benefits from your location with a speed comparison tool. Like other AWS services, AWS Global Accelerator is a self-service, pay-per-use offering, requiring no long term commitments or minimum fees.

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

upvoted 4 times

✉  **elearningtakai** 8 months ago

Selected Answer: B

Global Accelerator supports the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), making it an excellent choice for an online multi-player game using UDP networking protocol. By setting up Global Accelerator with UDP listeners and endpoint groups in each Region, the network architecture can minimize latency and packet loss, giving end users a high-quality gaming experience.

upvoted 4 times

✉  **Bofi** 9 months ago

Selected Answer: B

AWS Global Accelerator is a service that improves the availability and performance of applications with local or global users. 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 1 times

✉  **KOnAn** 9 months ago

Selected Answer: B

Global Accelerator for UDP and TCP traffic
upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: B
Global Accelerator
upvoted 1 times

 **Neha999** 9 months, 1 week ago

B
Global Accelerator for UDP traffic
upvoted 1 times

A company hosts a three-tier web application on Amazon EC2 instances in a single Availability Zone. The web application uses a self-managed MySQL database that is hosted on an EC2 instance to store data in an Amazon Elastic Block Store (Amazon EBS) volume. The MySQL database currently uses a 1 TB Provisioned IOPS SSD (io2) EBS volume. The company expects traffic of 1,000 IOPS for both reads and writes at peak traffic.

The company wants to minimize any disruptions, stabilize performance, and reduce costs while retaining the capacity for double the IOPS. The company wants to move the database tier to a fully managed solution that is highly available and fault tolerant.

Which solution will meet these requirements MOST cost-effectively?

- A. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with an io2 Block Express EBS volume.
- B. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume.
- C. Use Amazon S3 Intelligent-Tiering access tiers.
- D. Use two large EC2 instances to host the database in active-passive mode.

Correct Answer: B

Community vote distribution

B (85%) A (15%)

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

Selected Answer: B

RDS does not support IO2 or IO2express . GP2 can do the required IOPS

RDS supported Storage >

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

GP2 max IOPS >

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose.html#gp2-performance>

upvoted 12 times

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

Selected Answer: B

RDS does not support IO2 or IO2express . GP2 can do the required IOPS

upvoted 1 times

✉  **Gooniegoogoo** 5 months ago

The Options is A only because it is sufficient.. Provisioned IOPS are available but overkill.. just want to make sure we understand why its A for the right reason

upvoted 1 times

✉  **Abrar2022** 5 months, 3 weeks ago

Simplified by Almero - thanks.

RDS does not support IO2 or IO2express . GP2 can do the required IOPS

upvoted 1 times

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

Selected Answer: B

I tried on the portal and only gp3 and i01 are supported.

This is 11 May 2023.

upvoted 3 times

✉  **ruqui** 6 months ago

it doesn't matter whether or no io* is supported, using io2 is overkill, you only need 1K IOPS, B is the correct answer

upvoted 1 times

✉  **SimiTik** 7 months, 1 week ago

A

Amazon RDS supports the use of Amazon EBS Provisioned IOPS (io2) volumes. When creating a new DB instance or modifying an existing one, you can select the io2 volume type and specify the amount of IOPS and storage capacity required. RDS also supports the newer io2 Block Express volumes, which can deliver even higher performance for mission-critical database workloads.

upvoted 2 times

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

Impossible. I just tried on the portal and only io1 and gp3 are supported.

upvoted 1 times

✉ **klayytech** 8 months, 1 week ago

Selected Answer: B

The most cost-effective solution that meets the requirements is to use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume. This solution will provide high availability and fault tolerance while minimizing disruptions and stabilizing performance. The gp2 EBS volume can handle up to 16,000 IOPS. You can also scale up to 64 TiB of storage.

Amazon RDS for MySQL provides automated backups, software patching, and automatic host replacement. It also provides Multi-AZ deployments that automatically replicate data to a standby instance in another Availability Zone. This ensures that data is always available even in the event of a failure.

upvoted 1 times

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

Selected Answer: B

RDS does not support io2 !!!

upvoted 1 times

✉ **Maximus007** 8 months, 2 weeks ago

B: gp3 would be the better option, but considering we have only gp2 option and such storage volume - gp2 will be the right choice

upvoted 2 times

✉ **Nel8** 8 months, 2 weeks ago

Selected Answer: B

I thought the answer here is A. But when I found the link from Amazon website; as per AWS:

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1), and magnetic (also known as standard). They differ in performance characteristics and price, which means that you can tailor your storage performance and cost to the needs of your database workload. You can create MySQL, MariaDB, Oracle, and PostgreSQL RDS DB instances with up to 64 tebibytes (TiB) of storage. You can create SQL Server RDS DB instances with up to 16 TiB of storage. For this amount of storage, use the Provisioned IOPS SSD and General Purpose SSD storage types.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

✉ **Steve_4542636** 9 months ago

Selected Answer: B

for DB instances between 1 TiB and 4 TiB, storage is striped across four Amazon EBS volumes providing burst performance of up to 12,000 IOPS.

from "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html"

upvoted 1 times

✉ **TungPham** 9 months ago

Selected Answer: B

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1), and magnetic (also known as standard)

B - MOST cost-effectively

upvoted 2 times

✉ **KZM** 9 months ago

The baseline IOPS performance of gp2 volumes is 3 IOPS per GB, which means that a 1 TB gp2 volume will have a baseline performance of 3,000 IOPS. However, the volume can also burst up to 16,000 IOPS for short periods, but this burst performance is limited and may not be sustained for long durations.

So, I am more prefer option A.

upvoted 1 times

✉ **KZM** 9 months ago

If a 1 TB gp3 EBS volume is used, the maximum available IOPS according to calculations is 3000. This means that the storage can support a requirement of 1000 IOPS, and even 2000 IOPS if the requirement is doubled.

I am confusing between choosing A or B.

upvoted 1 times

✉ **mark16dc** 9 months, 1 week ago

Selected Answer: A

Option A is the correct answer. A Multi-AZ deployment provides high availability and fault tolerance by automatically replicating data to a standby instance in a different Availability Zone. This allows for seamless failover in the event of a primary instance failure. Using an io2 Block Express EBS volume provides the needed IOPS performance and capacity for the database. It is also designed for low latency and high durability, which makes it a good choice for a database tier.

upvoted 1 times

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

How will you select io2 when RDS only offers io1....magic?

upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: B

Correction - hit wrong answer button - meant 'B'

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1)

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: A

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1)

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

 **everfly** 9 months, 1 week ago

Selected Answer: A

<https://aws.amazon.com/about-aws/whats-new/2021/07/aws-announces-general-availability-amazon-ebs-block-express-volumes/>

upvoted 2 times

A company hosts a serverless application on AWS. The application uses Amazon API Gateway, AWS Lambda, and an Amazon RDS for PostgreSQL database. The company notices an increase in application errors that result from database connection timeouts during times of peak traffic or unpredictable traffic. The company needs a solution that reduces the application failures with the least amount of change to the code.

What should a solutions architect do to meet these requirements?

- A. Reduce the Lambda concurrency rate.
- B. Enable RDS Proxy on the RDS DB instance.
- C. Resize the RDS DB instance class to accept more connections.
- D. Migrate the database to Amazon DynamoDB with on-demand scaling.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

RDS Proxy is a fully managed, highly available, and scalable proxy for Amazon Relational Database Service (RDS) that makes it easy to connect to your RDS instances from applications running on AWS Lambda. RDS Proxy offloads the management of connections to the database, which can help to improve performance and reliability.

upvoted 1 times

 **TariqKipkemei** 6 months, 3 weeks 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. With RDS Proxy, failover times for Aurora and RDS databases are reduced by up to 66%.

<https://aws.amazon.com/rds/proxy/>

upvoted 3 times

 **elearningtakai** 8 months ago

Selected Answer: B

To reduce application failures resulting from database connection timeouts, the best solution is to enable RDS Proxy on the RDS DB instance

upvoted 1 times

 **Wheretostart** 8 months, 2 weeks ago

Selected Answer: B

RDS Proxy

upvoted 3 times

 **nder** 9 months, 1 week ago

Selected Answer: B

RDS Proxy will pool connections, no code changes need to be made

upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: B

RDS proxy

upvoted 1 times

 **Neha999** 9 months, 1 week ago

B RDS Proxy

<https://aws.amazon.com/rds/proxy/>

upvoted 2 times

A company is migrating an old application to AWS. The application runs a batch job every hour and is CPU intensive. The batch job takes 15 minutes on average with an on-premises server. The server has 64 virtual CPU (vCPU) and 512 GiB of memory.

Which solution will run the batch job within 15 minutes with the LEAST operational overhead?

- A. Use AWS Lambda with functional scaling.
- B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.
- C. Use Amazon Lightsail with AWS Auto Scaling.
- D. Use AWS Batch on Amazon EC2.

Correct Answer: A

Community vote distribution

D (95%)	5%
---------	----

✉  **NolaHolla** Highly Voted 9 months, 1 week ago

The amount of CPU and memory resources required by the batch job exceeds the capabilities of AWS Lambda and Amazon Lightsail with AWS Auto Scaling, which offer limited compute resources. AWS Fargate offers containerized application orchestration and scalable infrastructure, but may require additional operational overhead to configure and manage the environment. AWS Batch is a fully managed service that automatically provisions the required infrastructure for batch jobs, with options to use different instance types and launch modes.

Therefore, the solution that will run the batch job within 15 minutes with the LEAST operational overhead is D. Use AWS Batch on Amazon EC2. AWS Batch can handle all the operational aspects of job scheduling, instance management, and scaling while using Amazon EC2 instances with the right amount of CPU and memory resources to meet the job's requirements.

upvoted 13 times

✉  **everfly** Highly Voted 9 months, 1 week ago

Selected Answer: D

AWS Batch is a fully-managed service that can launch and manage the compute resources needed to execute batch jobs. It can scale the compute environment based on the size and timing of the batch jobs.

upvoted 8 times

✉  **Ramdi1** Most Recent 1 month, 3 weeks ago

Selected Answer: D

The question needs to be phrased differently. I assume at first it was Lambda, because it says 15 minutes in the question which can be done. Yes it also does say CPU intensive however they go on with a full stop and then give you the server specs. It does not say it uses that much of the specs so they need to really rephrase the questions.

upvoted 1 times

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

Selected Answer: D

The main reasons are:

AWS Batch can easily schedule and run batch jobs on EC2 instances. It can scale up to the required vCPUs and memory to match the on-premises server.

Using EC2 provides full control over the instance type to meet the resource needs.

No servers or clusters to manage like with ECS/Fargate or Lightsail. AWS Batch handles this automatically.

More cost effective and operationally simple compared to Lambda which is not ideal for long running batch jobs.

upvoted 2 times

✉  **BrijMohan08** 2 months, 3 weeks ago

Selected Answer: A

On-Prem was avg 15 min, but target state architecture is expected to finish within 15 min

upvoted 1 times

✉  **jayce5** 4 months ago

Selected Answer: D

Not Lambda, "average 15 minutes" means there are jobs with running more and less than 15 minutes. Lambda max is 15 minutes.

upvoted 1 times

✉  **Gooniegoogoo** 5 months ago

This is for certain a tough one. I do see that they have thrown a curve ball in making it Lambda Functional scaling, however what we don't know is if this application has many requests or one large one.. looks like Lambda can scale and use the same lambda env.. seems intensive tho so will go with D

upvoted 2 times

 **TariqKipkemei** 6 months, 3 weeks ago

Selected Answer: D

AWS Batch

upvoted 1 times

 **JLII** 8 months, 3 weeks ago

Selected Answer: D

Not A because: "AWS Lambda now supports up to 10 GB of memory and 6 vCPU cores for Lambda Functions." <https://aws.amazon.com/about-aws/whats-new/2020/12/aws-lambda-supports-10gb-memory-6-vcpu-cores-lambda-functions/> vs. "The server has 64 virtual CPU (vCPU) and 512 GiB of memory" in the question.

upvoted 5 times

 **geekgirl22** 9 months, 1 week ago

A is the answer. Lambda is known that has a limit of 15 minutes. So for as long as it says "within 15 minutes" that should be a clear indication it is Lambda

upvoted 1 times

 **nder** 9 months, 1 week ago

Wrong, the job takes "On average 15 minutes" and requires more cpu and ram than lambda can deal with. AWS Batch is correct in this scenario

upvoted 3 times

 **geekgirl22** 9 months, 1 week ago

read the rest of the question which gives the answer:

"Which solution will run the batch job within 15 minutes with the LEAST operational overhead?"

Keyword "Within 15 minutes"

upvoted 2 times

 **Lonojack** 9 months, 1 week ago

What happens if it EXCEEDS the 15 min AVERAGE?

Average = possibly can be more than 15min.

The safer bet would be option D: AWS Batch on EC2

upvoted 6 times

 **Terion** 2 months ago

I think what he means is that it takes on average 15 min on prem only

upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: D

AWS batch on EC2

upvoted 1 times

A company stores its data objects in Amazon S3 Standard storage. A solutions architect has found that 75% of the data is rarely accessed after 30 days. The company needs all the data to remain immediately accessible with the same high availability and resiliency, but the company wants to minimize storage costs.

Which storage solution will meet these requirements?

- A. Move the data objects to S3 Glacier Deep Archive after 30 days.
- B. Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- C. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately.

Correct Answer: B

Community vote distribution

B (100%)

 **TariqKipkemei** 1 month, 2 weeks ago

Selected Answer: B

high availability, resiliency = multi AZ

75% of the data is rarely accessed but remain immediately accessible = Standard-Infrequent Access

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

The correct answer is B.

S3 Standard-IA is a storage class that is designed for infrequently accessed data. It offers lower storage costs than S3 Standard, but it has a retrieval latency of 1-5 minutes.

upvoted 1 times

 **Piccalo** 8 months ago

Highly available so One Zone IA is out the question

Glacier Deep archive isn't immediately accessible 12-48 hours

B is the answer.

upvoted 3 times

 **elearningtakai** 8 months ago

Selected Answer: B

S3 Glacier Deep Archive is intended for data that is rarely accessed and can tolerate retrieval times measured in hours. Moving data to S3 One Zone-IA immediately would not meet the requirement of immediate accessibility with the same high availability and resiliency.

upvoted 1 times

 **KS2020** 8 months, 2 weeks ago

The answer should be C.

S3 One Zone-IA is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA.

<https://aws.amazon.com/s3/storage-classes/#:~:text=S3%20One%20Zone%2DIA%20is,less%20than%20S3%20Standard%2DIA>.

upvoted 1 times

 **shanwfrod** 8 months, 1 week ago

The Question emphasises to keep same high availability class - S3 One Zone-IA doesn't support multiple Availability Zone data resilience model like S3 Standard-Infrequent Access.

upvoted 2 times

 **Lonojack** 9 months, 1 week ago

Selected Answer: B

Needs immediate accessibility after 30 days, IF they need to be accessed.

upvoted 4 times

 **bpd123** 9 months, 1 week ago

Selected Answer: B

S3 Standard-Infrequent Access after 30 days

upvoted 2 times

 **NolaHolla** 9 months, 1 week ago

B

Option B - Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days - will meet the requirements of keeping the data immediately accessible with high availability and resiliency, while minimizing storage costs. S3 Standard-IA is designed for infrequently accessed data, and it provides a lower storage cost than S3 Standard, while still offering the same low latency, high throughput, and high durability as S3 Standard.

upvoted 4 times

A gaming company is moving its public scoreboard from a data center to the AWS Cloud. The company uses Amazon EC2 Windows Server instances behind an Application Load Balancer to host its dynamic application. The company needs a highly available storage solution for the application. The application consists of static files and dynamic server-side code.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge.
- B. Store the static files on Amazon S3. Use Amazon ElastiCache to cache objects at the edge.
- C. Store the server-side code on Amazon Elastic File System (Amazon EFS). Mount the EFS volume on each EC2 instance to share the files.
- D. Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.
- E. Store the server-side code on a General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on each EC2 instance to share the files.

Correct Answer: AD

Community vote distribution

AD (100%)

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: AD

The reasons are:

Storing static files in S3 with CloudFront provides durability, high availability, and low latency by caching at edge locations. FSx for Windows File Server provides a fully managed Windows native file system that can be accessed from the Windows EC2 instances to share server-side code. It is designed for high availability and scales up to 10s of GBPS throughput. EFS and EBS volumes can be attached to a single AZ. FSx and S3 are replicated across AZs for high availability.

upvoted 2 times

 **Whericanstart** 8 months, 2 weeks ago

Selected Answer: AD

A & D for sure

upvoted 4 times

 **Steve_4542636** 9 months ago

Selected Answer: AD

A because ElastiCache, despite being ideal for leaderboards per Amazon, doesn't cache at edge locations. D because FSx has higher performance for low latency needs.

<https://www.techtarget.com/searchaws/tip/Amazon-FSx-vs-EFS-Compare-the-AWS-file-services>

"FSx is built for high performance and submillisecond latency using solid-state drive storage volumes. This design enables users to select storage capacity and latency independently. Thus, even a subterabyte file system can have 256 Mbps or higher throughput and support volumes up to 64 TB."

upvoted 3 times

 **baba365** 2 months, 1 week ago

Why not EFS?

upvoted 1 times

 **Nel8** 8 months, 2 weeks ago

Just to add, ElastiCache is used in front of AWS database.

upvoted 2 times

 **KZM** 9 months ago

It is obvious that A and D.

upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: AD

both A and D seem correct

upvoted 1 times

 **NolaHolla** 9 months, 1 week ago

A and D seems correct

upvoted 1 times

A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients.

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

- A. Install an external image management library on an EC2 instance. Use the image management library to process the images.
- B. Create a CloudFront origin request policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.
- C. Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.
- D. Create a CloudFront response headers policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

Correct Answer: D

Community vote distribution

C (89%)	11%
---------	-----

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

Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.

Using a Lambda@Edge function with an external image management library is the best solution to resize the images dynamically and serve appropriate formats to clients. Lambda@Edge is a serverless computing service that allows running custom code in response to CloudFront events, such as viewer requests and origin requests. By using a Lambda@Edge function, it's possible to process images on the fly and modify the CloudFront response before it's sent back to the client. Additionally, Lambda@Edge has built-in support for external libraries that can be used to process images. This approach will reduce operational overhead and scale automatically with traffic.

upvoted 12 times

 **TariqKipkemei** Most Recent 1 month, 2 weeks ago

Selected Answer: C

The moment there is a need to implement some logic at the CDN think Lambda@Edge.

upvoted 2 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: C

The correct answer is C.

A Lambda@Edge function is a serverless function that runs at the edge of the CloudFront network. This means that the function is executed close to the user, which can improve performance.

An external image management library can be used to resize images and to serve the appropriate format.

Associating the Lambda@Edge function with the CloudFront behaviors that serve the images ensures that the function is executed for all requests that are served by those behaviors.

upvoted 1 times

 **BrijMohan08** 2 months, 3 weeks ago

Selected Answer: B

If the user asks for the most optimized image format (JPEG, WebP, or AVIF) using the directive format=auto, CloudFront Function will select the best format based on the Accept header present in the request.

Latest documentation: <https://aws.amazon.com/blogs/networking-and-content-delivery/image-optimization-using-amazon-cloudfront-and-aws-lambda/>

upvoted 1 times

 **bdp123** 9 months, 1 week ago

Selected Answer: C

<https://aws.amazon.com/cn/blogs/networking-and-content-delivery/resizing-images-with-amazon-cloudfront-lambdaedge-aws-cdn-blog/>

upvoted 3 times

 **everfly** 9 months, 1 week ago

Selected Answer: C

<https://aws.amazon.com/cn/blogs/networking-and-content-delivery/resizing-images-with-amazon-cloudfront-lambdaedge-aws-cdn-blog/>

upvoted 2 times

A hospital needs to store patient records in an Amazon S3 bucket. The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest. The compliance team must administer the encryption key for data at rest.

Which solution will meet these requirements?

- A. Create a public SSL/TLS certificate in AWS Certificate Manager (ACM). Associate the certificate with Amazon S3. Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
- B. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with S3 managed encryption keys (SSE-S3). Assign the compliance team to manage the SSE-S3 keys.
- C. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
- D. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Use Amazon Macie to protect the sensitive data that is stored in Amazon S3. Assign the compliance team to manage Macie.

Correct Answer: C

Community vote distribution

C (80%)

D (15%) 5%

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

Option C is correct because it allows the compliance team to manage the KMS keys used for server-side encryption, thereby providing the necessary control over the encryption keys. Additionally, the use of the "aws:SecureTransport" condition on the bucket policy ensures that all connections to the S3 bucket are encrypted in transit.
option B might be misleading but using SSE-S3, the encryption keys are managed by AWS and not by the compliance team
upvoted 14 times

✉  **Lonojack** 9 months, 1 week ago

Perfect explanation. I Agree
upvoted 2 times

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

Selected Answer: C

Macie does not encrypt the data like the question is asking
<https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html>

Also, SSE-S3 encryption is fully managed by AWS so the Compliance Team can't administer this.
upvoted 1 times

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

Selected Answer: C

D - Can't be because - Amazon Macie is a data security service that uses machine learning (ML) and pattern matching to discover and help protect your sensitive data.
Macie discovers sensitive information, can help in protection but can't protect
upvoted 1 times

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

Selected Answer: C

B can work if they do not want control over encryption keys.
upvoted 1 times

✉  **Russ99** 8 months ago

Selected Answer: A

Option A proposes creating a public SSL/TLS certificate in AWS Certificate Manager and associating it with Amazon S3. This step ensures that data is encrypted in transit. Then, the default encryption for each S3 bucket will be configured to use server-side encryption with AWS KMS keys (SSE-KMS), which will provide encryption at rest for the data stored in S3. In this solution, the compliance team will manage the KMS keys, ensuring that they control the encryption keys for data at rest.
upvoted 1 times

✉  **Shrestwt** 7 months, 2 weeks ago

ACM cannot be integrated with Amazon S3 bucket directly.

upvoted 1 times

✉ **Bofi** 8 months, 1 week ago

Selected Answer: C

Option C seems to be the correct answer, option A is also close but ACM cannot be integrated with Amazon S3 bucket directly, hence, u can not attached TLS to S3. You can only attached TLS certificate to ALB, API Gateway and CloudFront and maybe Global Accelerator but definitely NOT EC2 instance and S3 bucket

upvoted 1 times

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

Selected Answer: C

D makes no sense.

upvoted 2 times

✉ **Dody** 8 months, 3 weeks ago

Selected Answer: C

Correct Answer is "C"

"D" is not correct because Amazon Macie securely stores your data at rest using AWS encryption solutions. Macie encrypts data, such as findings, using an AWS managed key from AWS Key Management Service (AWS KMS). However, in the question there is a requirement that the compliance team must administer the encryption key for data at rest.

<https://docs.aws.amazon.com/macie/latest/user/data-protection.html>

upvoted 2 times

✉ **cegama543** 8 months, 3 weeks ago

Selected Answer: C

Option C will meet the requirements.

Explanation:

The compliance team needs to administer the encryption key for data at rest in order to ensure that protected health information (PHI) is encrypted in transit and at rest. Therefore, we need to use server-side encryption with AWS KMS keys (SSE-KMS). The default encryption for each S3 bucket can be configured to use SSE-KMS to ensure that all new objects in the bucket are encrypted with KMS keys.

Additionally, we can configure the S3 bucket policies to allow only encrypted connections over HTTPS (TLS) using the aws:SecureTransport condition. This ensures that the data is encrypted in transit.

upvoted 1 times

✉ **Karlos99** 8 months, 4 weeks ago

Selected Answer: C

We must provide encrypted in transit and at rest. Macie is needed to discover and recognize any PII or Protected Health Information. We already know that the hospital is working with the sensitive data) so protect them with KMS and SSL. Answer D is unnecessary

upvoted 1 times

✉ **Steve_4542636** 9 months ago

Selected Answer: C

Macie does not encrypt the data like the question is asking

<https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html>

Also, SSE-S3 encryption is fully managed by AWS so the Compliance Team can't administer this.

upvoted 2 times

✉ **Abhineet9148232** 9 months ago

Selected Answer: C

C [Correct]: Ensures Https only traffic (encrypted transit), Enables compliance team to govern encryption key.

D [Incorrect]: Misleading; PHI is required to be encrypted not discovered. Macie is a discovery service. (<https://aws.amazon.com/macie/>)

upvoted 4 times

✉ **Nel8** 9 months ago

Selected Answer: D

Correct answer should be D. "Use Amazon Macie to protect the sensitive data..."

As requirement says "The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest."

Macie protects personal record such as PHI. Macie provides you with an inventory of your S3 buckets, and automatically evaluates and monitors the buckets for security and access control. If Macie detects a potential issue with the security or privacy of your data, such as a bucket that becomes publicly accessible, Macie generates a finding for you to review and remediate as necessary.

upvoted 3 times

✉ **Drayen25** 9 months ago

Option C should be

upvoted 2 times

A company uses Amazon API Gateway to run a private gateway with two REST APIs in the same VPC. The BuyStock RESTful web service calls the CheckFunds RESTful web service to ensure that enough funds are available before a stock can be purchased. The company has noticed in the VPC flow logs that the BuyStock RESTful web service calls the CheckFunds RESTful web service over the internet instead of through the VPC. A solutions architect must implement a solution so that the APIs communicate through the VPC.

Which solution will meet these requirements with the FEWEST changes to the code?

- A. Add an X-API-Key header in the HTTP header for authorization.
- B. Use an interface endpoint.
- C. Use a gateway endpoint.
- D. Add an Amazon Simple Queue Service (Amazon SQS) queue between the two REST APIs.

Correct Answer: A

Community vote distribution

B (87%) 13%

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

Selected Answer: B

an interface endpoint is a horizontally scaled, redundant VPC endpoint that provides private connectivity to a service. It is an elastic network interface with a private IP address that serves as an entry point for traffic destined to the AWS service. Interface endpoints are used to connect VPCs with AWS services

upvoted 12 times

 **liux99** Most Recent 2 weeks, 6 days ago

The question here is that the BuyStock RESTful web service calls the CheckFunds RESTful web service through API gateway (internet), not directly. How does API gateway connect the services BuyStock and CheckFunds? It connects the Interface Endpoint of the services through PrivateLink. The interface endpoints provide direct connection between services within the same private subnet. Answer B is correct.

upvoted 1 times

 **youdelin** 1 month, 2 weeks ago

how is it even possible, I mean if it's private and both are in the same VPC then we shouldn't even have such an issue right?

upvoted 1 times

 **Guru4Cloud** 2 months, 3 weeks ago

Selected Answer: B

B. Use an interface endpoint.

upvoted 1 times

 **envest** 6 months ago

Answer B (from abylead)

With API GW, you can create multiple prv REST APIs, only accessible with an interface VPC endpt. To allow/ deny simple or cross acc access to your API from selected VPCs & its endpts, you use resource plcs. In addition, you can also use DX for a connection between onprem network to VPC or your prv API.

API GW to VPC: <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html>

Less correct & incorrect (infeasible & inadequate) answers:

A)X-API-Key in HTTP header for authorization needs auto-process fcts & changes: inadequate.

C)VPC GW endpts for S3 or DynamDB aren't for RESTful svcs: infeasible.

D)SQS que between 2 REST APIs needs endpts & some changes: inadequate.

upvoted 1 times

 **lucdt4** 6 months, 1 week ago

Selected Answer: B

C. Use a gateway endpoint is wrong because gateway endpoints only support for S3 and dynamoDB, so B is correct

upvoted 3 times

 **aqmdla2002** 6 months, 2 weeks ago

Selected Answer: C

I select C because it's the solution with the " FEWEST changes to the code"

upvoted 1 times

 **TariqKipkemei** 6 months, 3 weeks ago

Selected Answer: B

An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service upvoted 1 times

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

Selected Answer: B

BBBBBB

upvoted 1 times

✉ **siyam008** 9 months ago

Selected Answer: C

<https://www.linkedin.com/pulse/aws-interface-endpoint-vs-gateway-alex-chang>

upvoted 1 times

✉ **siyam008** 9 months ago

Correct answer is B. Incorrectly selected C

upvoted 1 times

✉ **DASBOL** 9 months ago

Selected Answer: B

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html>

upvoted 4 times

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

Selected Answer: C

The only time where an Interface Endpoint may be preferable (for S3 or DynamoDB) over a Gateway Endpoint is if you require access from on-premises, for example you want private access from your on-premise data center

upvoted 2 times

✉ **Steve_4542636** 9 months ago

The RESTful services is neither an S3 or DynamDB service, so a VPC Gateway endpoint isn't available here.

upvoted 4 times

✉ **bdp123** 9 months, 1 week ago

Selected Answer: B

fewest changes to code and below link:

<https://gkzz.medium.com/what-is-the-differences-between-vpc-endpoint-gateway-endpoint-ae97bfab97d8>

upvoted 2 times

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

This really helped me understand the difference between the two. Thx

upvoted 1 times

✉ **KAUS2** 9 months, 1 week ago

Agreed B

upvoted 2 times

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

Selected Answer: B

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html> - Interface EP

upvoted 3 times

A company hosts a multiplayer gaming application on AWS. The company wants the application to read data with sub-millisecond latency and run one-time queries on historical data.

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

- A. Use Amazon RDS for data that is frequently accessed. Run a periodic custom script to export the data to an Amazon S3 bucket.
- B. Store the data directly in an Amazon S3 bucket. Implement an S3 Lifecycle policy to move older data to S3 Glacier Deep Archive for long-term storage. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
- C. Use Amazon DynamoDB with DynamoDB Accelerator (DAX) for data that is frequently accessed. Export the data to an Amazon S3 bucket by using DynamoDB table export. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
- D. Use Amazon DynamoDB for data that is frequently accessed. Turn on streaming to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to read the data from Kinesis Data Streams. Store the records in an Amazon S3 bucket.

Correct Answer: B

Community vote distribution

C (100%)

✉  **lexotan** Highly Voted 7 months, 1 week ago

Selected Answer: C

would be nice to have an explanation on why examtopic selects its answers.

upvoted 6 times

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

Selected Answer: C

DAX delivers up to a 10 times performance improvement—from milliseconds to microseconds.

Using DynamoDB export to S3, you can export data from an Amazon DynamoDB table to an Amazon S3 bucket. This feature enables you to perform analytics and complex queries on your data using other AWS services such as Athena, AWS Glue.

upvoted 2 times

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

Selected Answer: C

Amazon DynamoDB with DynamoDB Accelerator (DAX) is a fully managed, in-memory caching solution for DynamoDB. DAX can improve the performance of DynamoDB by up to 10x. This makes it a good choice for data that needs to be accessed with sub-millisecond latency.

DynamoDB table export allows you to export data from DynamoDB to an S3 bucket. This can be useful for running one-time queries on historical data.

Amazon Athena is a serverless, interactive query service that makes it easy to analyze data in Amazon S3. Athena can be used to run one-time queries on the data in the S3 bucket.

upvoted 3 times

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

A NoSQL isn't even mentioned in the question and yet we are supposed to just imagine this fictional customer is using a NoSQL DB

upvoted 1 times

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

C

Amazon DynamoDB with DynamoDB Accelerator (DAX): DynamoDB is a fully managed NoSQL database service provided by AWS. It is designed for low-latency access to frequently accessed data. DynamoDB Accelerator (DAX) is an in-memory cache for DynamoDB that can significantly reduce read latency, making it suitable for achieving sub-millisecond read times.

upvoted 1 times

✉  **lucdt4** 6 months, 1 week ago

Selected Answer: C

C is correct

A don't meets a requirement (LEAST operational overhead) because use script

B: Not regarding to require

D: Kinesis for near-real-time (Not for read)

-> C is correct

upvoted 2 times

✉  **DagsH** 8 months, 1 week ago

Selected Answer: C

Agreed C will be best because of DynamoDB DAX

upvoted 1 times

 **BeeKayEnn** 8 months, 1 week ago

Option C will be the best fit.

As they would like to retrieve the data with sub-millisecond, DynamoDB with DAX is the answer.

DynamoDB supports some of the world's largest scale applications by providing consistent, single-digit millisecond response times at any scale. You can build applications with virtually unlimited throughput and storage.

upvoted 2 times

 **Grace83** 8 months, 1 week ago

C is the correct answer

upvoted 1 times

 **KAUS2** 8 months, 3 weeks ago

Selected Answer: C

Option C is the right one. The questions clearly states "sub-millisecond latency "

upvoted 2 times

 **smgsi** 8 months, 3 weeks ago

Selected Answer: C

https://aws.amazon.com/dynamodb/dax/?nc1=h_ls

upvoted 3 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: C

Ccccccccccc

upvoted 2 times

 **ACasper** 8 months, 3 weeks ago

Answer is C for Submillisecond

upvoted 4 times

A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent. Otherwise, the payments might be processed incorrectly.

Which actions should a solutions architect take to meet this requirement? (Choose two.)

- A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key.
- B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.
- C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key.
- D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue. Set the message attribute to use the payment ID.
- E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

Correct Answer: BD

Community vote distribution

BE (66%)	AE (29%)	5%
----------	----------	----

✉️  **Ashkan_10** Highly Voted 7 months, 4 weeks ago

Selected Answer: BE

Option B is preferred over A because Amazon Kinesis Data Streams inherently maintain the order of records within a shard, which is crucial for the given requirement of preserving the order of messages for a particular payment ID. When you use the payment ID as the partition key, all messages for that payment ID will be sent to the same shard, ensuring that the order of messages is maintained.

On the other hand, Amazon DynamoDB is a NoSQL database service that provides fast and predictable performance with seamless scalability. While it can store data with partition keys, it does not guarantee the order of records within a partition, which is essential for the given use case. Hence, using Kinesis Data Streams is more suitable for this requirement.

As DynamoDB does not keep the order, I think BE is the correct answer here.

upvoted 16 times

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

Selected Answer: BE

Technically both B and E will ensure processing order, but SQS FIFO was specifically built to handle this requirement. There is no ask on how to store the data so A and C are out.

upvoted 1 times

✉️  **Pritam228** 1 month, 3 weeks ago

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.Partitions.html>
upvoted 1 times

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

Selected Answer: DE

options D and E are better because they mimic a real-world queue system and ensure that payments are processed in the correct order, just like customers in a store would be served in the order they arrived. This is crucial for a payment processing system where order matters to avoid mistakes in payment processing.

upvoted 2 times

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

Amazon Kinesis Data Streams Overkill for Ordering

Overkill for Ordering: While Kinesis can maintain order within a partition key, it might be seen as overkill for a scenario where your primary concern is maintaining the order of payments. SQS FIFO queues (option E) are specifically designed for this purpose and provide an easier and more cost-effective solution.

upvoted 1 times

✉️  **omoakin** 6 months ago

AAAAAAA EEEEEEEEEE
upvoted 2 times

✉️  **Konb** 6 months, 1 week ago

Selected Answer: AE

IF the question would be "Choose all the solutions that fulfill these requirements" I would chosen BE.

But it is:

"Which actions should a solutions architect take to meet this requirement? "

For this reason I chose AE, because we don't need both Kinesis AND SQS for this solution. Both choices complement to order processing: order stored in DB, work item goes to the queue.

upvoted 3 times

 **Smart** 3 months, 4 weeks ago

Incorrect, AWS will clarify it by using the phrase - "combination of actions".

upvoted 1 times

 **luisgu** 6 months, 3 weeks ago

Selected Answer: BE

E --> no doubt

B --> see <https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html>

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: BE

1) SQS FIFO queues guarantee that messages are received in the exact order they are sent. Using the payment ID as the message group ensures all messages for a payment ID are received sequentially.

2) Kinesis data streams can also enforce ordering on a per partition key basis. Using the payment ID as the partition key will ensure strict ordering of messages for each payment ID.

upvoted 2 times

 **kruasan** 7 months ago

The other options do not guarantee message ordering. DynamoDB and ElastiCache are not message queues. SQS standard queues deliver messages in approximate order only.

upvoted 2 times

 **mrgeee** 7 months ago

Selected Answer: BE

BE no doubt.

upvoted 1 times

 **nonsense** 7 months, 1 week ago

Selected Answer: BE

Option A, writing the messages to an Amazon DynamoDB table, would not necessarily preserve the order of messages for a particular payment ID

upvoted 1 times

 **MssP** 8 months ago

Selected Answer: BE

I don't understand A, How you can guarantee the order with DynamoDB?? The order is guaranteed with SQS FIFO and Kinesis Data Stream in 1 shard...

upvoted 4 times

 **Grace83** 8 months, 1 week ago

AE is the answer

upvoted 2 times

 **XXXman** 8 months, 2 weeks ago

Selected Answer: BE

dynamodb or kinesis data stream which one is ordered?

upvoted 1 times

 **Karlos99** 8 months, 3 weeks ago

Selected Answer: AE

No doubt)

upvoted 3 times

 **kprakashbehera** 8 months, 3 weeks ago

Selected Answer: AE

Ans - AE

Kinesis and elastic cache are not required in this case.

upvoted 2 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: AE

Araeaeaaaa

upvoted 4 times

A company is building a game system that needs to send unique events to separate leaderboard, matchmaking, and authentication services concurrently. The company needs an AWS event-driven system that guarantees the order of the events.

Which solution will meet these requirements?

- A. Amazon EventBridge event bus
- B. Amazon Simple Notification Service (Amazon SNS) FIFO topics
- C. Amazon Simple Notification Service (Amazon SNS) standard topics
- D. Amazon Simple Queue Service (Amazon SQS) FIFO queues

Correct Answer: B

Community vote distribution

B (59%)	D (31%)	10%
---------	---------	-----

✉  **bella** Highly Voted 6 months, 4 weeks ago

Selected Answer: B

I don't honestly / can't understand why people go to ChatGPT to ask for the answers.... if I recall correctly they only consolidated their DB until 2021...

upvoted 8 times

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

Yup, ChatGPT doesn't //know// anything about AWS services. It only repeats what other people have said about it, which could be nonsense or hyperbole or some combination thereof.

upvoted 2 times

✉  **cra2yk** Highly Voted 8 months, 2 weeks ago

Given B by chatgpt:

The solution that meets the requirements of sending unique events to separate services concurrently and guaranteeing the order of events is option B, Amazon Simple Notification Service (Amazon SNS) FIFO topics.

Amazon SNS FIFO topics ensure that messages are processed in the order in which they are received. This makes them an ideal choice for situations where the order of events is important. Additionally, Amazon SNS allows messages to be sent to multiple endpoints, which meets the requirement of sending events to separate services concurrently.

Amazon EventBridge event bus can also be used for sending events, but it does not guarantee the order of events.

Amazon Simple Notification Service (Amazon SNS) standard topics do not guarantee the order of messages.

Amazon Simple Queue Service (Amazon SQS) FIFO queues ensure that messages are processed in the order in which they are received, but they are designed for message queuing, not publishing.

upvoted 7 times

✉  **omoakin** 6 months ago

Answer is D B is just for a message but not do orderliness.

I went to check Chatgpt she did not choose b i dnt know which one you subscribed to..or maybe its free. LOL her answer is D

upvoted 1 times

✉  **nw47** 8 months, 1 week ago

ChatGPT also give A:

The requirement of maintaining the order of events rules out the use of Amazon SNS standard topics as they do not provide any ordering guarantees.

Amazon SNS FIFO topics offer message ordering but do not support concurrent delivery to multiple subscribers, so this option is also not a suitable choice.

Amazon SQS FIFO queues provide both ordering guarantees and support concurrent delivery to multiple subscribers. However, the use of a queue adds additional latency, and the ordering guarantee may not be required in this scenario.

The best option for this use case is Amazon EventBridge event bus. It allows multiple targets to subscribe to an event bus and receive the same event simultaneously, meeting the requirement of concurrent delivery to multiple subscribers. Additionally, EventBridge provides ordering guarantees within an event bus, ensuring that events are processed in the order they are received.

upvoted 1 times

✉  **sparun1607** Most Recent 4 days, 5 hours ago

My Answer is B

You can use Amazon SNS FIFO (first in, first out) topics with Amazon SQS FIFO queues to provide strict message ordering and message deduplication. The FIFO capabilities of each of these services work together to act as a fully managed service to integrate distributed applications that require data consistency in near-real time. Subscribing Amazon SQS standard queues to Amazon SNS FIFO topics provides best-effort ordering and at least once delivery.

upvoted 1 times

✉️  **LazyTs** 2 months, 3 weeks ago

Selected Answer: B

The answer is B la. SNS FIFO topics queue should be used combined with SQS FIFO queue in this case. The question asked for correct order to different event, so asking for SNS fan out here to send to individual SQS.

<https://docs.aws.amazon.com/sns/latest/dg/fifo-example-use-case.html>

upvoted 4 times

✉️  **Po_chih** 1 month, 3 weeks ago

The best answer!

upvoted 1 times

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

Selected Answer: B

bbbbbbbbbbbbb

upvoted 1 times

✉️  **jaydesai8** 4 months, 3 weeks ago

Selected Answer: D

SQS FIFO maintains the order of the events - Answer is D

upvoted 2 times

✉️  **jayce5** 5 months, 3 weeks ago

Selected Answer: B

It should be the fan-out pattern, and the pattern starts with Amazon SNS FIFO for the orders.

upvoted 2 times

✉️  **danielklein09** 6 months ago

Selected Answer: D

Answer is D. You are so lazy because instead of searching in documentation or your notes, you are asking ChatGPT. Do you really think you will take this exam ? Hint: ask ChatGPT

upvoted 5 times

✉️  **lucdt4** 6 months, 1 week ago

Selected Answer: D

D is correct (SQS FIFO)

Because B can't send event concurrently though it can send in the order of the events

upvoted 1 times

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

Selected Answer: B

Amazon SNS is a highly available and durable publish-subscribe messaging service that allows applications to send messages to multiple subscribers through a topic. SNS FIFO topics are designed to ensure that messages are delivered in the order in which they are sent. This makes them ideal for situations where message order is important, such as in the case of the company's game system.

Option A, Amazon EventBridge event bus, is a serverless event bus service that makes it easy to build event-driven applications. While it supports ordering of events, it does not provide guarantees on the order of delivery.

upvoted 3 times

✉️  **rushi0611** 6 months, 4 weeks ago

Selected Answer: B

Option B:

send unique events to separate leaderboard, matchmaking, and authentication services concurrently. Concurrently= fan out pattern. Only SQS cannot do a fan out SQS will be consumer for SNS FIFO.

upvoted 1 times

✉️  **neosis91** 7 months, 1 week ago

Selected Answer: B

BBBBBBB

upvoted 1 times

✉️  **kels1** 7 months, 1 week ago

Guys, gotta question here... can sqs perform fan out by itself without sns?

Here's what our beloved AI said:

AWS SQS (Simple Queue Service) can perform fan-out by itself using its native functionality, without the need for SNS (Simple Notification Service).

having that answer... would D be an option?

upvoted 2 times

✉ **ErfanKh** 7 months, 2 weeks ago

Selected Answer: D

D for me, and ChatGPT

upvoted 1 times

✉ **udo2020** 7 months, 3 weeks ago

I think it should be D. Because in the question I saw nothing regarding subscribe which leads to SNS.

upvoted 1 times

✉ **jayce5** 7 months, 3 weeks ago

Selected Answer: B

Separate leader boards -> fan out pattern.

upvoted 1 times

✉ **maver144** 7 months, 4 weeks ago

Vague question. Its either SNS FIFO or SQS FIFO. Consider that SNS FIFO can only have SQS FIFO as subscriber. You can't emmit events to other sources like with standard SNS.

upvoted 3 times

A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) in the architecture.

A solutions architect is reviewing the infrastructure design. Data must be encrypted at rest and in transit. Only authorized personnel of the hospital should be able to access the data.

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

- A. Turn on server-side encryption on the SQS components. Update the default key policy to restrict key usage to a set of authorized principals.
- B. Turn on server-side encryption on the SNS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals.
- C. Turn on encryption on the SNS components. Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic policy to allow only encrypted connections over TLS.
- D. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.
- E. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.

Correct Answer: CD

Community vote distribution

BD (64%) CD (23%) 14%

 **fkie4**  8 months, 3 weeks ago

Selected Answer: BD

read this:

<https://docs.aws.amazon.com/sns/latest/dg/sns-server-side-encryption.html>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-server-side-encryption.html>

upvoted 10 times

 **Gooniegoogoo** 5 months ago

good call.. that confirms on that page:

Important

All requests to topics with SSE enabled must use HTTPS and Signature Version 4.

For information about compatibility of other services with encrypted topics, see your service documentation.

Amazon SNS only supports symmetric encryption KMS keys. You cannot use any other type of KMS key to encrypt your service resources. For help determining whether a KMS key is a symmetric encryption key, see Identifying asymmetric KMS keys.

upvoted 2 times

 **TariqKipkemei**  6 months, 2 weeks ago

Selected Answer: CD

Its only options C and D that covers encryption on transit, encryption at rest and a restriction policy.

upvoted 2 times

 **Lalo** 5 months, 3 weeks ago

Answer is BD

SNS: AWS KMS, key policy, SQS: AWS KMS, Key policy

upvoted 3 times

 **luisgu** 6 months, 3 weeks ago

Selected Answer: BD

"IAM policies you can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached"

reference: https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/security_iam_service-with-iam.html

that excludes E

upvoted 1 times

 **imvb88** 7 months, 2 weeks ago

Selected Answer: CD

Encryption at transit = use SSL/TLS -> rule out A,B
Encryption at rest = encryption on components -> keep C, D, E
KMS always need a key policy, IAM is optional -> E out

-> C, D left, one for SNS, one for SQS. TLS: checked, encryption on components: checked
upvoted 3 times

 **Lalo** 5 months, 3 weeks ago

Answer is BD
SNS: AWS KMS, key policy, SQS: AWS KMS, Key policy
upvoted 1 times

 **imvb88** 7 months, 2 weeks ago

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-data-encryption.html>

You can protect data in transit using Secure Sockets Layer (SSL) or client-side encryption. You can protect data at rest by requesting Amazon SQS to encrypt your messages before saving them to disk in its data centers and then decrypt them when the messages are received.

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html>

A key policy is a resource policy for an AWS KMS key. Key policies are the primary way to control access to KMS keys. Every KMS key must have exactly one key policy. The statements in the key policy determine who has permission to use the KMS key and how they can use it. You can also use IAM policies and grants to control access to the KMS key, but every KMS key must have a key policy.

upvoted 1 times

 **MarkGerwich** 8 months, 1 week ago

CD
B does not include encryption in transit.
upvoted 3 times

 **MssP** 8 months, 1 week ago

in transit is included in D. With C, not include encryption at rest.... Server-side will include it.
upvoted 1 times

 **Bofi** 8 months, 1 week ago

That was my objection toward option B. CD cover both encryption at Rest and Server-Side_Encryption
upvoted 1 times

 **Maximus007** 8 months, 2 weeks ago

ChatGPT returned AD as a correct answer)
upvoted 1 times

 **cegama543** 8 months, 2 weeks ago

Selected Answer: BE
B: To encrypt data at rest, we can use a customer-managed key stored in AWS KMS to encrypt the SNS components.

E: To restrict access to the data and allow only authorized personnel to access the data, we can apply an IAM policy to restrict key usage to a set of authorized principals. We can also set a condition in the queue policy to allow only encrypted connections over TLS to encrypt data in transit.
upvoted 2 times

 **Karlos99** 8 months, 3 weeks ago

Selected Answer: BD
For a customer managed KMS key, you must configure the key policy to add permissions for each queue producer and consumer.
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-key-management.html>
upvoted 3 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: BE
bebebe
upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

bdbdbdbd
All KMS keys must have a key policy. IAM policies are optional.
upvoted 5 times

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

- A. Read replicas
- B. Manual snapshots
- C. Automated backups
- D. Multi-AZ deployments

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: C

Automated backups allow you to recover your database to any point in time within your specified retention period, which can be up to 35 days. The recovery process creates a new Amazon RDS instance with a new endpoint, and the process takes time proportional to the size of the database. Automated backups are enabled by default and occur daily during the backup window. This feature provides an easy and convenient way to recover from data loss incidents such as the one described in the scenario.

upvoted 2 times

 **elearningtakai** 8 months ago

Selected Answer: C

Option C, Automated backups, will meet the requirement. Amazon RDS allows you to automatically create backups of your DB instance. Automated backups enable point-in-time recovery (PITR) for your DB instance down to a specific second within the retention period, which can be up to 35 days. By setting the retention period to 30 days, the company can restore the database to its state from up to 5 minutes before any change within the last 30 days.

upvoted 2 times

 **joechen2023** 5 months, 2 weeks ago

I selected C as well, but still don't know how the automatic backup could have a copy 5 minutes before any change. AWS doc states "Automated backups occur daily during the preferred backup window."

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html.

I think the answer maybe A, as read replica will be kept sync and then restore from the read replica. could an expert help?

upvoted 1 times

 **gold4otas** 8 months ago

Selected Answer: C

C: Automated Backups

<https://aws.amazon.com/rds/features/backup/>

upvoted 2 times

 **WhericanIstart** 8 months, 1 week ago

Selected Answer: C

Automated Backups...

upvoted 2 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: C

cccccccccc

upvoted 1 times

A company's web application consists of an Amazon API Gateway API in front of an AWS Lambda function and an Amazon DynamoDB database. The Lambda function handles the business logic, and the DynamoDB table hosts the data. The application uses Amazon Cognito user pools to identify the individual users of the application. A solutions architect needs to update the application so that only users who have a subscription can access premium content.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Enable API caching and throttling on the API Gateway API.
- B. Set up AWS WAF on the API Gateway API. Create a rule to filter users who have a subscription.
- C. Apply fine-grained IAM permissions to the premium content in the DynamoDB table.
- D. Implement API usage plans and API keys to limit the access of users who do not have a subscription.

Correct Answer: C

Community vote distribution

D (94%)	6%
---------	----

 **lipi0035** 4 days, 18 hours ago

In the same document <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html> if you scroll down, it says `Don't use API keys for authentication or authorization to control access to your APIs. If you have multiple APIs in a usage plan, a user with a valid API key for one API in that usage plan can access all APIs in that usage plan. Instead, to control access to your API, use an IAM role, a Lambda authorizer, or an Amazon Cognito user pool.'

In the same document at the bottom, it says "If you're using a developer portal to publish your APIs, note that all APIs in a given usage plan are subscribable, even if you haven't made them visible to your customers."

I go with C

upvoted 1 times

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: D

After you create, test, and deploy your APIs, you can use API Gateway usage plans to make them available as product offerings for your customers. 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. These can be set at the API, or API method level.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html#:~:text=Creating%20and%20using-,usage%20plans,-with%20API%20keys>

upvoted 1 times

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: D

Implementing API usage plans and API keys is a straightforward way to restrict access to specific users or groups based on subscriptions. It allows you to control access at the API level and doesn't require extensive changes to your existing architecture. This solution provides a clear and manageable way to enforce access restrictions without complicating other parts of the application

upvoted 4 times

 **marufxplorer** 5 months, 1 week ago

D

Option D involves implementing API usage plans and API keys. By associating specific API keys with users who have a valid subscription, you can control access to the premium content.

upvoted 1 times

 **kruasan** 7 months ago

Selected Answer: D

A. This would not actually limit access based on subscriptions. It helps optimize and control API usage, but does not address the core requirement.
B. This could work by checking user subscription status in the WAF rule, but would require ongoing management of WAF and increases operational overhead.

C. This is a good approach, using IAM permissions to control DynamoDB access at a granular level based on subscriptions. However, it would require managing IAM permissions which adds some operational overhead.

D. This option uses API Gateway mechanisms to limit API access based on subscription status. It would require the least amount of ongoing management and changes, minimizing operational overhead. API keys could be easily revoked/changed as subscription status changes.

upvoted 3 times

 **imvb88** 7 months, 2 weeks ago

CD both possible but D is more suitable since it mentioned in <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

A,B not relevant.
upvoted 1 times

✉ **elearningtakai** 8 months ago

Selected Answer: D

The solution that will meet the requirement with the least operational overhead is to implement API Gateway usage plans and API keys to limit access to premium content for users who do not have a subscription.
Option A is incorrect because API caching and throttling are not designed for authentication or authorization purposes, and it does not provide access control.
Option B is incorrect because although AWS WAF is a useful tool to protect web applications from common web exploits, it is not designed for authorization purposes, and it might require additional configuration, which increases the operational overhead.
Option C is incorrect because although IAM permissions can restrict access to data stored in a DynamoDB table, it does not provide a mechanism for limiting access to specific content based on the user subscription. Moreover, it might require a significant amount of additional IAM permissions configuration, which increases the operational overhead.

upvoted 3 times

✉ **klayytech** 8 months, 1 week ago

Selected Answer: D

To meet the requirement with the least operational overhead, you can implement API usage plans and API keys to limit the access of users who do not have a subscription. This way, you can control access to your API Gateway APIs by requiring clients to submit valid API keys with requests. You can associate usage plans with API keys to configure throttling and quota limits on individual client accounts.

upvoted 2 times

✉ **techhb** 8 months, 2 weeks ago

answer is D ,if looking for least overhead
<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>
C will achieve it but operational overhead is high.

upvoted 2 times

✉ **quentin17** 8 months, 2 weeks ago

Selected Answer: D

Both C&D are valid solution
According to ChatGPT:
"Applying fine-grained IAM permissions to the premium content in the DynamoDB table is a valid approach, but it requires more effort in managing IAM policies and roles for each user, making it more complex and adding operational overhead."
upvoted 1 times

✉ **Karlos99** 8 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>
upvoted 2 times

✉ **taehyeki** 8 months, 3 weeks ago

Selected Answer: C

CCCCCCCC
upvoted 1 times

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

- A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
- D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

NLBs allow UDP traffic (ALBs don't support UDP)

Global Accelerator uses Anycast IP addresses and its global network to intelligently route users to the optimal endpoint
Using NLBs as Global Accelerator endpoints provides improved availability and DDoS protection.

upvoted 5 times

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

Selected Answer: A

UDP = NLB and Global Accelerator

upvoted 1 times

 **live_reply_developers** 4 months, 3 weeks ago

Selected Answer: A

NLB + GA support UDP/TCP

upvoted 2 times

 **Gooniegoogoo** 5 months ago

good reference <https://blog.cloudcraft.co/alb-vs-nlb-which-aws-load-balancer-fits-your-needs/>

upvoted 1 times

 **lucdt4** 6 months, 1 week ago

Selected Answer: A

C - D: Cloudfront don't support UDP/TCP

B: Global accelerator don't support ALB

A is correct

upvoted 2 times

 **SkyZeroZx** 7 months ago

Selected Answer: A

UDP = NBL

UDP = GLOBAL ACCELERATOR

UPD NOT WORKING WITH CLOUDFRONT

ANS IS A

upvoted 3 times

 **MssP** 8 months, 1 week ago

Selected Answer: A

More discussions at: <https://www.examtopics.com/discussions/amazon/view/51508-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **Grace83** 8 months, 1 week ago

Why is C not correct - does anyone know?

upvoted 2 times

 **Shrestwt** 7 months, 2 weeks ago

Latency based routing is already using in the application, so AWS global network will optimize the path from users to applications.

upvoted 1 times

 **MssP** 8 months, 1 week ago

It could be valid but I think A is better. Uses the AWS global network to optimize the path from users to applications, improving the performance of TCP and UDP traffic

upvoted 1 times

 **FourOfAKind** 8 months, 2 weeks ago

Selected Answer: A

UDP == NLB

Must be hosted on-premises != CloudFront

upvoted 3 times

 **imvb88** 7 months, 2 weeks ago

actually CloudFront's origin can be on-premises. Source:

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

"A custom origin is an HTTP server, for example, a web server. The HTTP server can be an Amazon EC2 instance or an HTTP server that you host somewhere else."

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: A

aaaaaaaaa

upvoted 3 times

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords.

What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account.
- B. Set a password policy for each IAM user in the AWS account.
- C. Use third-party vendor software to set password requirements.
- D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **TariqKipkemei** 1 month, 1 week ago

Selected Answer: A

You can set a custom password policy on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. When you create or change a password policy, most of the password policy settings are enforced the next time your users change their passwords. However, some of the settings are enforced immediately.

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html#:~:text=Setting%20an%20account-,password%20policy,-for%20IAM%20users
upvoted 1 times

✉️  **angel_marquina** 2 months ago

The question is for new users, answer A is not exact for that case.

upvoted 3 times

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

Selected Answer: A

To accomplish this, the solutions architect should set an overall password policy for the entire AWS account. This policy will apply to all IAM users in the account, including new users.

upvoted 3 times

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

Selected Answer: A

Set overall password policy ...

upvoted 1 times

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

Selected Answer: A

A is correct

upvoted 1 times

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

Selected Answer: A

aaaaaaaa

upvoted 4 times

A company has migrated an application to Amazon EC2 Linux instances. One of these EC2 instances runs several 1-hour tasks on a schedule. These tasks were written by different teams and have no common programming language. The company is concerned about performance and scalability while these tasks run on a single instance. A solutions architect needs to implement a solution to resolve these concerns.

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

- A. Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events).
- B. Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs.
- C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events).
- D. Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance.

Correct Answer: A

Community vote distribution

A (65%)	C (22%)	8%
---------	---------	----

✉️  **fkie4** Highly Voted 8 months, 3 weeks ago

Selected Answer: C

question said "These tasks were written by different teams and have no common programming language", and key word "scalable". Only Lambda can fulfil these. Lambda can be done in different programming languages, and it is scalable

upvoted 6 times

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

But the question states "several 1-hour tasks on a schedule", and the maximum runtime for Lambda is 15 minutes, so it can't be A.

upvoted 15 times

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

can't be C

upvoted 4 times

✉️  **wsdasdasdqwdaw** 1 month, 1 week ago

AWS Batch - As a fully managed service, AWS Batch helps you to run batch computing workloads of any scale. AWS Batch automatically provisions compute resources and optimizes the workload distribution based on the quantity and scale of the workloads. With AWS Batch, there's no need to install or manage batch computing software, so you can focus your time on analyzing results and solving problems.
<https://docs.aws.amazon.com/batch/latest/userguide/what-is-batch.html> ---> I am voting for A, C would have been OK if the time was within 15 minutes.

upvoted 2 times

✉️  **smgsi** 8 months, 2 weeks ago

It's not because time limit of lambda is 15 minutes

upvoted 3 times

✉️  **taehyeki** Highly Voted 8 months, 3 weeks ago

Selected Answer: A

aaaaaaaaaa

upvoted 5 times

✉️  **fkie4** 8 months, 3 weeks ago

A my S. show some reasons next time

upvoted 11 times

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

Selected Answer: A

The last working for hour but lambda function timeout is 15 minutes. So vote A.

upvoted 1 times

✉️  **yodelin** 1 month, 2 weeks ago

I know guys are stressed out trying to figure this exam out okay, but no matter what people say, with or without reasoning, at least put your mouth clean. Going like AAA is an issue, but talking shi* on him just because he didn't write down the reasoning is your fault.

upvoted 1 times

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

Selected Answer: A

It can run heterogeneous workloads and tasks without needing to convert them to a common format.
AWS Batch manages the underlying compute resources - no need to manage containers, Lambda functions or Auto Scaling groups.

upvoted 2 times

 **zjcorpuz** 3 months, 4 weeks ago

AWS Lambda function can only be run for 15 mins

upvoted 1 times

 **jaydesai8** 4 months, 3 weeks ago

Selected Answer: A

maximum runtime for Lambda is 15 minutes, hence A

upvoted 1 times

 **antropaws** 6 months ago

Selected Answer: A

I also go with A.

upvoted 1 times

 **omoakin** 6 months ago

C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events)

upvoted 1 times

 **ruqui** 6 months ago

wrong, Lambda maximum runtime is 15 minutes and the tasks run for an hour

upvoted 2 times

 **KMohsoe** 6 months, 1 week ago

Selected Answer: A

B and D out!

A and C let's think!

AWS Lambda functions are time limited.

So, Option A

upvoted 1 times

 **lucdt4** 6 months, 1 week ago

AAAAAAAAAAAAAA

because lambda only run within 15 minutes

upvoted 1 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: A

Answer is A.

Could have been C but AWS Lambda functions can be only configured to run up to 15 minutes per execution. While the task in question need an 1hour to run,

upvoted 1 times

 **luisgu** 6 months, 3 weeks ago

Selected Answer: D

question is asking for the LEAST operational overhead. With batch, you have to create the compute environment, create the job queue, create the job definition and create the jobs --> more operational overhead than creating an ASG

upvoted 1 times

 **WELL_212** 7 months, 1 week ago

Selected Answer: A

A not C

The maximum AWS Lambda function run time is 15 minutes. If a Lambda function runs for longer than 15 minutes, it will be terminated by AWS Lambda. This limit is in place to prevent the Lambda environment from becoming stale and to ensure that resources are available for other functions. If a task requires more than 15 minutes to complete, a different AWS service or architecture may be better suited for the use case.

upvoted 1 times

 **neosis91** 7 months, 1 week ago

Selected Answer: C

CCCCCCCCCC

upvoted 1 times

 **neosis91** 7 months, 1 week ago

Selected Answer: A

AAAAAAA

upvoted 1 times

 **udo2020** 7 months, 2 weeks ago

It must be A!

In general, AWS Lambda can be more cost-effective for smaller, short-lived tasks or for event-driven computing use cases. For long running or computation heavy tasks, AWS Batch can be more cost-effective, as it allows you to provision and manage a more robust computing environment.

upvoted 2 times

A company runs a public three-tier web application in a VPC. The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet. The company needs a managed solution that minimizes operational maintenance.

Which solution meets these requirements?

- A. Provision a NAT instance in a public subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- B. Provision a NAT instance in a private subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- C. Provision a NAT gateway in a public subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.
- D. Provision a NAT gateway in a private subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.

Correct Answer: C

Community vote distribution

C (100%)

 **UnluckyDucky**  8 months, 3 weeks ago

Selected Answer: C

"The company needs a managed solution that minimizes operational maintenance"

Watch out for NAT instances vs NAT Gateways.

As the company needs a managed solution that minimizes operational maintenance - NAT Gateway is a public subnet is the answer.
upvoted 5 times

 **Guru4Cloud**  2 months, 4 weeks ago

Selected Answer: C

This meets the requirements for a managed, low maintenance solution for private subnets to access the internet:

NAT gateway provides automatic scaling, high availability, and fully managed service without admin overhead.
Placing the NAT gateway in a public subnet with proper routes allows private instances to use it for internet access.
Minimal operational maintenance compared to NAT instances.

upvoted 1 times

 **Guru4Cloud** 2 months, 4 weeks ago

No good:

NAT instances (A, B) require more hands-on management.

Placing a NAT gateway in a private subnet (D) would not allow internet access.

upvoted 1 times

 **lucdt4** 6 months, 1 week ago

C

Nat gateway can't deploy in a private subnet.

upvoted 1 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: C

minimizes operational maintenance = NGW

upvoted 1 times

 **WhericanIstart** 8 months, 2 weeks ago

Selected Answer: C

C..provision NGW in Public Subnet

upvoted 1 times

 **cegama543** 8 months, 2 weeks ago

Selected Answer: C

cccccc is the best

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: C

cccccccc

upvoted 2 times

A company needs to create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host a digital media streaming application. The EKS cluster will use a managed node group that is backed by Amazon Elastic Block Store (Amazon EBS) volumes for storage. The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS).

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

- A. Use a Kubernetes plugin that uses the customer managed key to perform data encryption.
- B. After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.
- C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.
- D. Create the EKS cluster. Create an IAM role that has a policy that grants permission to the customer managed key. Associate the role with the EKS cluster.
- E. Store the customer managed key as a Kubernetes secret in the EKS cluster. Use the customer managed key to encrypt the EBS volumes.

Correct Answer: AE

Community vote distribution

CD (56%)	BD (40%)	5%
----------	----------	----

✉  **asoli**  8 months, 2 weeks ago

Selected Answer: CD

<https://docs.aws.amazon.com/eks/latest/userguide/managed-node-groups.html#:~:text=encrypted%20Amazon%20EBS%20volumes%20without%20using%20a%20launch%20template%2C%20encrypt%20all%20new%20Amazon%20EBS%20volumes%20created%20in%20your%20account>.

upvoted 10 times

✉  **imvb88**  7 months, 2 weeks ago

Selected Answer: BD

Quickly rule out A (which plugin? > overhead) and E because of bad practice

Among B,C,D: B and C are functionally similar > choice must be between B or C, D is fixed

Between B and C: C is out since it set default for all EBS volume in the region, which is more than required and even wrong, say what if other EBS volumes of other applications in the region have different requirement?

upvoted 5 times

✉  **maudsha**  4 weeks, 1 day ago

Selected Answer: CD

IF you need to encrypt an unencrypted volume,

- Create an EBS snapshot of the volume
 - Encrypt the EBS snapshot (using copy)
 - Create new EBS volume from the snapshot (the volume will also be encrypted)
- so it has an operational overhead.

So assuming they won't use this account for anything else we can use C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.

upvoted 1 times

✉  **TariqKipkemei** 1 month, 1 week ago

Selected Answer: CD

Option D is required either way.

Technically both option B and C would work, but with B you would have to enable encryption node by node, while with option C provides a one-time action of enabling encryption on all nodes.

The requirement is the option with LEAST operational overhead.

upvoted 1 times

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

Selected Answer: CD

These options allow EBS encryption with the customer managed KMS key with minimal operational overhead:

C) Setting the KMS key as the regional EBS encryption default automatically encrypts new EKS node EBS volumes.

D) The IAM role grants the EKS nodes access to use the key for encryption/decryption operations.

upvoted 1 times

✉  **jaydesai8** 4 months, 3 weeks ago

Selected Answer: CD

C - enable EBS encryption by default in a region -<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

D - Provides key access permission just to the EKS cluster without changing broader IAM permissions

upvoted 1 times

✉  **pedroso** 5 months, 3 weeks ago

Selected Answer: BD

I was in doubt between B and C.

You can't "Enable EBS encryption by default in the AWS Region". Enable EBS encryption by default is only possible at Account level, not Region.

B is the right option once you can enable encryption on the EBS volume with KMS and custom KMS.

upvoted 1 times

✉  **antropaws** 5 months, 1 week ago

Not accurate: "Encryption by default is a Region-specific setting":

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default>

upvoted 2 times

✉  **jayce5** 5 months, 3 weeks ago

Selected Answer: CD

It's C and D. I tried it in my AWS console.

C seems to have fewer operations ahead compared to B.

upvoted 5 times

✉  **nauman001** 6 months, 1 week ago

B and C.

Unless the key policy explicitly allows it, you cannot use IAM policies to allow access to a KMS key. Without permission from the key policy, IAM policies that allow permissions have no effect.

upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: BD

B. Manually enable encryption on the intended EBS volumes after ensuring no default changes. Requires manually enabling encryption on the nodes but ensures minimum impact.

D. Create an IAM role with access to the key to associate with the EKS cluster. This provides key access permission just to the EKS cluster without changing broader IAM permissions.

upvoted 2 times

✉  **kruasan** 7 months ago

- A. Using a custom plugin requires installing, managing and troubleshooting the plugin. Significant operational overhead.
- C. Modifying the default region encryption could impact other resources with different needs. Should be avoided if possible.
- E. Managing Kubernetes secrets for key access requires operations within the EKS cluster. Additional operational complexity.

upvoted 1 times

✉  **neosis91** 7 months, 1 week ago

Selected Answer: BC

B&C B&C B&C B&C B&C B&C B&C B&C B&C

upvoted 1 times

✉  **ssha2** 7 months, 2 weeks ago

Selected Answer: BD

B. After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.

D. Create the EKS cluster. Create an IAM role that has a policy that grants permission to the customer managed key. Associate the role with the EKS cluster.

Explanation:

Option B is the simplest and most direct way to enable encryption for the EBS volumes associated with the EKS cluster. After the EKS cluster is created, you can manually locate the EBS volumes and enable encryption using the customer managed key through the AWS Management Console, AWS CLI, or SDKs.

Option D involves creating an IAM role with a policy that grants permission to the customer managed key, and then associating that role with the EKS cluster. This allows the EKS cluster to have the necessary permissions to access the customer managed key for encrypting and decrypting data on the EBS volumes. This approach is more automated and can be easily managed through IAM, which provides centralized control and reduces operational overhead.

upvoted 1 times

✉  **kraken21** 8 months ago

Selected Answer: CD

"The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service" : All data leans towards option CD. Least operational overhead.

upvoted 1 times

✉  **Russ99** 8 months, 1 week ago

Selected Answer: BD

Option C is not necessary as enabling EBS encryption by default will apply to all EBS volumes in the region, not just those associated with the EKS cluster. Additionally, it does not specify the use of a customer managed key.

upvoted 2 times

✉  **tommomoe** 7 months, 2 weeks ago

How is it B? Option C is best practice, you can definitely specify a CMK within KMS when setting the default encryption. Please test it out yourself

upvoted 2 times

✉  **Rob1L** 8 months, 1 week ago

Selected Answer: BC

Option A is incorrect because it suggests using a Kubernetes plugin, which may increase operational overhead.

Option D is incorrect because it suggests creating an IAM role and associating it with the EKS cluster, which is not necessary for this scenario.

Option E is incorrect because it suggests storing the customer managed key as a Kubernetes secret, which is not the best practice for managing sensitive data such as encryption keys.

upvoted 1 times

✉  **maver144** 7 months, 4 weeks ago

"Option D is incorrect because it suggests creating an IAM role and associating it with the EKS cluster, which is not necessary for this scenario."

Then your EKS cluster would not be able to access encrypted EBS volumes.

upvoted 1 times

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

Selected Answer: BD

B & D Do exactly what's required in a very simple way with the least overhead.

Options C affects all EBS volumes in the region which is absolutely not necessary here.

upvoted 4 times

✉  **Maximus007** 8 months, 2 weeks ago

Selected Answer: CD

Was thinking about CD vs CE, but CD least overhead

upvoted 1 times

A company wants to migrate an Oracle database to AWS. The database consists of a single table that contains millions of geographic information systems (GIS) images that are high resolution and are identified by a geographic code.

When a natural disaster occurs, tens of thousands of images get updated every few minutes. Each geographic code has a single image or row that is associated with it. The company wants a solution that is highly available and scalable during such events.

Which solution meets these requirements MOST cost-effectively?

- A. Store the images and geographic codes in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.
- B. Store the images in Amazon S3 buckets. Use Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value.
- C. Store the images and geographic codes in an Amazon DynamoDB table. Configure DynamoDB Accelerator (DAX) during times of high load.
- D. Store the images in Amazon S3 buckets. Store geographic codes and image S3 URLs in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.

Correct Answer: B

Community vote distribution

B (51%) D (49%)

✉  **Karlos99** Highly Voted 8 months, 3 weeks ago

Selected Answer: D

The company wants a solution that is highly available and scalable
upvoted 8 times

✉  **[Removed]** 8 months ago

But DynamoDB is also highly available and scalable
<https://aws.amazon.com/dynamodb/faqs/#:~:text=DynamoDB%20automatically%20scales%20throughput%20capacity,high%20availability%20and%20durability.>

upvoted 2 times

✉  **pbpally** 6 months, 3 weeks ago

Yes but has a size limit at 400kb so theoretically it could store images but it's not a plausible solution.
upvoted 1 times

✉  **ruqui** 6 months ago

It doesn't matter the size limit of DynamoDB!!!! The images are saved in S3 buckets. Right answer is B
upvoted 2 times

✉  **jaydesai8** 4 months, 3 weeks ago

but would it be easy and cost-effective to migrate Oracle (relational db) to (Dynamodb)NoSQL?
upvoted 3 times

✉  **wsdasdasdqwdaw** Most Recent 1 month ago

For D - Oracle is not cheap as well. RDS with Oracle vs DynamoDB, I would go for pure AWS provided option. In each exam there is a lot of marketing => B
upvoted 1 times

✉  **jubolano** 1 month ago

Selected Answer: D

Cost effective, D
upvoted 1 times

✉  **wsdasdasdqwdaw** 1 month, 1 week ago

B or D, but the question is MOST cost-effectively DynamoDB is more expensive than RDS, I am going for D
upvoted 1 times

✉  **gouranga45** 2 months ago

Selected Answer: B

Answer is B, DynamoDB is Highly available and scalable
upvoted 1 times

✉  **baba365** 2 months, 1 week ago

A single table in a relational db can have items that are related ? e.g. 'select * from Faculty where department_id in (10, 20) and dept_name = AWS'. In the sql query example above, * means all and Faculty is name of the table.

upvoted 1 times

✉ **Wayne23Fang** 2 months, 2 weeks ago

Selected Answer: B

Amazon prefers people to move from Oracle to its own services like DynamoDB and S3.

upvoted 3 times

✉ **Eminenza22** 3 months ago

Selected Answer: B

B option offers a cost-effective solution for storing and accessing high-resolution GIS images during natural disasters. Storing the images in Amazon S3 buckets provides scalable and durable storage, while using Amazon DynamoDB allows for quick and efficient retrieval of images based on geographic codes. This solution leverages the strengths of both S3 and DynamoDB to meet the requirements of high availability, scalability, and cost-effectiveness.

upvoted 1 times

✉ **cd93** 3 months, 2 weeks ago

Selected Answer: B

What were the company thinking using the most expensive DB on the planet FOR ONE SINGLE TABLE???

Migrate a single table from SQL to NoSQL should be easy enough I guess...

upvoted 1 times

✉ **vini15** 4 months ago

Should be D.

the question says company wants to migrate oracle to AWS. Oracle is a relational db hence RDS makes more sense whereas Dynamodb is non relational db.

upvoted 1 times

✉ **iBanan** 4 months, 1 week ago

I hate these questions:) I can't choose between B and D

upvoted 3 times

✉ **ces_9999** 4 months, 2 weeks ago

Guys the answer is B the oracle database only has one table without any relationships so why we should use a relational database in the first place, second we are storing the images in S3 not in the database why not use this alongside dynamo

upvoted 3 times

✉ **Kp88** 4 months ago

You can't do migration of Oracle to Dynmodb without SCT. I am not the DB guy but since its saying oracle I would go with D otherwise B makes more sense if a company is starting out from scratch.

upvoted 1 times

✉ **Kp88** 4 months ago

Actually now that I think about it , B sounds ok as well. Company just need to use SCT and that would be more cost effective.

upvoted 1 times

✉ **joehong** 5 months, 2 weeks ago

Selected Answer: D

"A company wants to migrate an Oracle database to AWS"

upvoted 2 times

✉ **secdgs** 5 months, 2 weeks ago

D: Wrong

if you caluate License Oracle Database, It is not cost-effectively. Multi-AZ is not scalable and if you set scalable, you need more license for Oracle database.

upvoted 2 times

✉ **secdgs** 5 months, 2 weeks ago

Selected Answer: B

D. wrong because RDS with multi-AZ not autoscale and guarantee database performance when "natural disaster occurs, tens of thousands of images get updated every few minutes"

upvoted 3 times

✉ **Dun6** 5 months, 2 weeks ago

Selected Answer: B

The images are stored in S3. It is the metadata of the object that is stored in DynamoDB which is obviously less than 400kb. DynamoDB key-value pair

upvoted 1 times

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

Selected Answer: D

I voted for D, highly available and scalable

upvoted 1 times

A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Data Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models.

Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.

Which storage solution meets these requirements MOST cost-effectively?

- A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
- C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Correct Answer: D

Community vote distribution

D (90%)	5%
---------	----

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

Selected Answer: D

Access patterns are given, therefore D is the most logical answer.

Intelligent tiering is for random, unpredictable access.

upvoted 7 times

✉  **ealpuche** 6 months, 3 weeks ago

You are missing: <<The data must be available with minimal delay for up to 1 year. After one year, the data must be retained for archival purposes.>> You are secure that data after 1 year is not accessible anymore.

upvoted 1 times

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

Selected Answer: D

This option optimizes costs while meeting the data access requirements:

Store new data in S3 Standard for first 30 days of frequent access
 Transition to S3 Standard-IA after 30 days for infrequent access up to 1 year
 Archive to Glacier Deep Archive after 1 year for long-term archival
 upvoted 1 times

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

Selected Answer: D

First 30 days data accessed every morning = S3 Standard
 Beyond 30 days data accessed quarterly = S3 Standard-Infrequent Access
 Beyond 1 year data retained = S3 Glacier Deep Archive
 upvoted 4 times

✉  **ealpuche** 6 months, 3 weeks ago

Selected Answer: A

Option A meets the requirements most cost-effectively. The S3 Intelligent-Tiering storage class provides automatic tiering of objects between the S3 Standard and S3 Standard-Infrequent Access (S3 Standard-IA) tiers based on changing access patterns, which helps optimize costs. The S3 Lifecycle policy can be used to transition objects to S3 Glacier Deep Archive after 1 year for archival purposes. This solution also meets the requirement for minimal delay in accessing data for up to 1 year. Option B is not cost-effective because it does not include the transition of data to S3 Glacier Deep Archive after 1 year. Option C is not the best solution because S3 Standard-IA is not designed for long-term archival purposes and incurs higher storage costs. Option D is also not the most cost-effective solution as it transitions objects to the S3 Standard-IA tier after 30 days, which is unnecessary for the requirement to retrain the suite of ML models each morning using data from the previous 30 days.

upvoted 1 times

✉  **KAUS2** 8 months, 3 weeks ago

Selected Answer: D

Agree with UnluckyDucky , the correct option is D
upvoted 1 times

✉ **fkie4** 8 months, 3 weeks ago

Selected Answer: D

Should be D. see this:
<https://www.examtopics.com/discussions/amazon/view/68947-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

✉ **Nithin1119** 8 months, 3 weeks ago

Selected Answer: B

Bbbbbbbb
upvoted 1 times

✉ **fkie4** 8 months, 3 weeks ago

hello!???

upvoted 2 times

✉ **taehyeki** 8 months, 3 weeks ago

Selected Answer: D

ddddddd
upvoted 3 times

✉ **taehyeki** 8 months, 3 weeks ago

D because:

- First 30 days- data access every morning (predictable and frequently) – S3 standard
- After 30 days, accessed 4 times a year – S3 infrequently access
- Data preserved- S3 Glacier Deep Archive

upvoted 6 times

A company is running several business applications in three separate VPCs within the us-east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds of gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center.

A solutions architect needs to design a network connectivity solution that maximizes cost-effectiveness.

Which solution meets these requirements?

- A. Configure three AWS Site-to-Site VPN connections from the data center to AWS. Establish connectivity by configuring one VPN connection for each VPC.
- B. Launch a third-party virtual network appliance in each VPC. Establish an IPsec VPN tunnel between the data center and each virtual appliance.
- C. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1. Establish connectivity by configuring each VPC to use one of the Direct Connect connections.
- D. Set up one AWS Direct Connect connection from the data center to AWS. Create a transit gateway, and attach each VPC to the transit gateway. Establish connectivity between the Direct Connect connection and the transit gateway.

Correct Answer: D

Community vote distribution

D (100%)

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: D

AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This connection simplifies your network and puts an end to complex peering relationships. Transit Gateway acts as a highly scalable cloud router—each new connection is made only once.

<https://aws.amazon.com/transit-gateway/#:~:text=AWS-,Transit%20Gateway,-connects%20your%20Amazon>
upvoted 1 times

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: D

This option leverages a single Direct Connect for consistent, private connectivity between the data center and AWS. The transit gateway allows each VPC to share the Direct Connect while keeping the VPCs isolated. This provides a cost-effective architecture to meet the requirements.
upvoted 2 times

 **alexandercamachop** 6 months ago

Selected Answer: D

Transit GW, is a hub for connecting all VPCs.
Direct Connect is expensive, therefore only 1 of them connected to the Transit GW (Hub for all our VPCs that we connect to it)
upvoted 1 times

 **KMohsoe** 6 months, 1 week ago

Selected Answer: D

Option D
upvoted 2 times

 **Sivasaa** 7 months ago

Can someone tell why option C will not work here
upvoted 3 times

 **Guru4Cloud** 2 months, 4 weeks ago

Using multiple Site-to-Site VPNs (A) or Direct Connects (C) incurs higher costs without providing significant benefits.
upvoted 1 times

 **jdamian** 6 months, 3 weeks ago

cost-effectiveness, 3 DC are more than 1 (more expensive). There is no need to connect more than 1 DC.
upvoted 1 times

 **SkyZeroZx** 7 months ago

Selected Answer: D

cost-effectiveness

D

upvoted 1 times

 **WhericanIstart** 8 months, 2 weeks ago

Selected Answer: D

Transit Gateway will achieve this result..

upvoted 3 times

 **Karlos99** 8 months, 3 weeks ago

Selected Answer: D

maximizes cost-effectiveness

upvoted 2 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: D

ddddddddd

upvoted 2 times

An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow. A solutions architect needs to design an architecture for the order-processing application. The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications. The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers.

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

- A. Use AWS Step Functions to build the application.
- B. Integrate all the application components in an AWS Glue job.
- C. Use Amazon Simple Queue Service (Amazon SQS) to build the application.
- D. Use AWS Lambda functions and Amazon EventBridge events to build the application.

Correct Answer: B

Community vote distribution

A (100%)

 **kinglong12** Highly Voted 8 months, 2 weeks ago

Selected Answer: A

AWS Step Functions is a fully managed service that makes it easy to build applications by coordinating the components of distributed applications and microservices using visual workflows. With Step Functions, you can combine multiple AWS Lambda functions into responsive serverless applications and orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers. Step Functions also allows for manual approvals as part of the workflow. This solution meets all the requirements with the least operational overhead.

upvoted 7 times

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

Selected Answer: A

involves several serverless functions and AWS services, require manual approvals as part of the workflow, combine the Lambda functions into responsive serverless applications, orchestrate data and services = AWS Step Functions

upvoted 1 times

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: A

AWS Step Functions allow you to easily coordinate multiple Lambda functions and services into serverless workflows with visual workflows. Step Functions are designed for building distributed applications that combine services and require human approval steps.

Using Step Functions provides a fully managed orchestration service with minimal operational overhead.

upvoted 3 times

 **capino** 3 months, 2 weeks ago

Selected Answer: A

Serverless && workflow service that need human approval::::step functions

upvoted 2 times

 **BeeKayENN** 8 months, 1 week ago

Key: Distributed Application Processing, Microservices orchestration (Orchestrate Data and Services)

A would be the best fit.

AWS Step Functions is a visual workflow service that helps developers use AWS services to build distributed applications, automate processes, orchestrate microservices, and create data and machine learning (ML) pipelines.

Reference: [https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20\(ML\)%20pipelines.](https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20(ML)%20pipelines.)
upvoted 2 times

 **COTIT** 8 months, 2 weeks ago

Selected Answer: A

Approval is explicit for the solution. -> "A common use case for AWS Step Functions is a task that requires human intervention (for example, an approval process). Step Functions makes it easy to coordinate the components of distributed applications as a series of steps in a visual workflow called a state machine. You can quickly build and run state machines to execute the steps of your application in a reliable and scalable fashion. (<https://aws.amazon.com/pt/blogs/compute/implementing-serverless-manual-approval-steps-in-aws-step-functions-and-amazon-api-gateway/>)"

upvoted 3 times

 **ktulu2602** 8 months, 3 weeks ago

Selected Answer: A

Option A: Use AWS Step Functions to build the application.

AWS Step Functions is a serverless workflow service that makes it easy to coordinate distributed applications and microservices using visual workflows. It is an ideal solution for designing architectures for distributed applications that involve multiple AWS services and serverless functions, as it allows us to orchestrate the flow of our application components using visual workflows. AWS Step Functions also integrates with other AWS services like AWS Lambda, Amazon EC2, and Amazon ECS, and it has built-in error handling and retry mechanisms. This option provides a serverless solution with the least operational overhead for building the application.

upvoted 3 times

A company has launched an Amazon RDS for MySQL DB instance. Most of the connections to the database come from serverless applications. Application traffic to the database changes significantly at random intervals. At times of high demand, users report that their applications experience database connection rejection errors.

Which solution will resolve this issue with the LEAST operational overhead?

- A. Create a proxy in RDS Proxy. Configure the users' applications to use the DB instance through RDS Proxy.
- B. Deploy Amazon ElastiCache for Memcached between the users' applications and the DB instance.
- C. Migrate the DB instance to a different instance class that has higher I/O capacity. Configure the users' applications to use the new DB instance.
- D. Configure Multi-AZ for the DB instance. Configure the users' applications to switch between the DB instances.

Correct Answer: A

Community vote distribution

A (100%)

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: A

database connection rejection errors = RDS Proxy
upvoted 1 times

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: A

RDS Proxy provides a proxy layer that pools and shares database connections to improve scalability. This allows the proxy to handle connection spikes to the database gracefully.

Using RDS Proxy requires minimal operational overhead - just create the proxy and reconfigure applications to use it. No code changes needed.
upvoted 2 times

 **antropaws** 6 months ago

Wait, why not B?????
upvoted 2 times

 **Guru4Cloud** 2 months, 4 weeks ago

ElastiCache (B) and larger instance type (C) help performance but don't resolve connection issues.
upvoted 1 times

 **live_reply_developers** 4 months, 3 weeks ago

Amazon ElastiCache tends to have a lower operational overhead compared to Amazon RDS Proxy. BUT we already have " Amazon RDS for MySQL DB instance"
upvoted 1 times

 **Guru4Cloud** 2 months, 4 weeks ago

ElastiCache (B) and larger instance type (C) help performance but don't resolve connection issues.
upvoted 1 times

 **roxx529** 6 months, 1 week ago

To reduce application failures resulting from database connection timeouts, the best solution is to enable RDS Proxy on the RDS DB instances
upvoted 1 times

 **COTIT** 8 months, 2 weeks ago

Selected Answer: A

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.
[\(https://aws.amazon.com/rds/proxy/\)](https://aws.amazon.com/rds/proxy/)
upvoted 3 times

 **ktulu2602** 8 months, 3 weeks ago

Selected Answer: A

The correct solution for this scenario would be to create a proxy in RDS Proxy. RDS Proxy allows for managing thousands of concurrent database connections, which can help reduce connection errors. RDS Proxy also provides features such as connection pooling, read/write splitting, and

retries. This solution requires the least operational overhead as it does not involve migrating to a different instance class or setting up a new cache layer. Therefore, option A is the correct answer.

upvoted 4 times

Question #377

Topic 1

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.

Which solution achieves these goals MOST efficiently?

- A. Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.
- B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated.
- C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated.
- D. Run a custom script on the instance operating system to send data to the audit system. Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated.

Correct Answer: B

Community vote distribution

B (100%)

✉ ktulu2602 Highly Voted 8 months, 3 weeks ago

Selected Answer: B

The most efficient solution for this scenario is to use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated. The lifecycle hook can be used to delay instance termination until the script has completed, ensuring that all data is sent to the audit system before the instance is terminated. This solution is more efficient than using a scheduled AWS Lambda function, which would require running the function periodically and may not capture all instances launched and terminated within the interval. Running a custom script through user data is also not an optimal solution, as it may not guarantee that all instances send data to the audit system. Therefore, option B is the correct answer.

upvoted 5 times

✉ TariqKipkemei Most Recent 1 month, 1 week ago

Selected Answer: B

Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated

upvoted 1 times

✉ Guru4Cloud 2 months, 4 weeks ago

Selected Answer: B

EC2 Auto Scaling lifecycle hooks allow you to perform custom actions as instances launch and terminate. This is the most efficient way to trigger the auditing script execution at instance launch and termination.

upvoted 4 times

✉ Whericanstart 8 months, 2 weeks ago

Selected Answer: B

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

upvoted 1 times

✉ COTIT 8 months, 2 weeks ago

Selected Answer: B

Amazon EC2 Auto Scaling offers the ability to add lifecycle hooks to your Auto Scaling groups. These hooks let you create solutions that are aware of events in the Auto Scaling instance lifecycle, and then perform a custom action on instances when the corresponding lifecycle event occurs. (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html>)

upvoted 4 times

✉ fkie4 8 months, 3 weeks ago

it is B. read this:

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

upvoted 1 times

A company is developing a real-time multiplayer game that uses UDP for communications between the client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.

Which solution should a solutions architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: B

This option provides the most scalable and optimized architecture for the real-time multiplayer game:

Network Load Balancer efficiently distributes UDP gaming traffic to the Auto Scaling group of game servers. DynamoDB On-Demand mode provides auto-scaling non-relational data storage for gamer scores and other game data. DynamoDB is optimized for fast, high-scale access patterns seen in gaming. Together, the Network Load Balancer and DynamoDB On-Demand provide an architecture that can smoothly scale up and down to match spikes in gaming demand.

upvoted 2 times

 **TariqKipkemei** 6 months, 2 weeks ago

Selected Answer: B

UDP = NLB

Non-relational data = Dynamo DB

upvoted 3 times

 **elearningtakai** 8 months ago

Selected Answer: B

Option B is a good fit because a Network Load Balancer can handle UDP traffic, and Amazon DynamoDB on-demand can provide automatic scaling without intervention

upvoted 1 times

 **KAUS2** 8 months, 3 weeks ago

Selected Answer: B

Correct option is "B"

upvoted 1 times

 **aragon_saa** 8 months, 3 weeks ago

B

<https://www.examtopics.com/discussions/amazon/view/29756-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Kenp1192** 8 months, 3 weeks ago

B

Because NLB can handle UDP and DynamoDB is Non-Relational

upvoted 1 times

 **fruto123** 8 months, 3 weeks ago

Selected Answer: B

key words - UDP, non-relational data

answers - NLB for UDP application, DynamoDB for non-relational data

upvoted 4 times

A company hosts a frontend application that uses an Amazon API Gateway API backend that is integrated with AWS Lambda. When the API receives requests, the Lambda function loads many libraries. Then the Lambda function connects to an Amazon RDS database, processes the data, and returns the data to the frontend application. The company wants to ensure that response latency is as low as possible for all its users with the fewest number of changes to the company's operations.

Which solution will meet these requirements?

- A. Establish a connection between the frontend application and the database to make queries faster by bypassing the API.
- B. Configure provisioned concurrency for the Lambda function that handles the requests.
- C. Cache the results of the queries in Amazon S3 for faster retrieval of similar datasets.
- D. Increase the size of the database to increase the number of connections Lambda can establish at one time.

Correct Answer: C

Community vote distribution

B (100%)

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

Selected Answer: B

Key: the Lambda function loads many libraries

Configuring provisioned concurrency would get rid of the "cold start" of the function therefore speeding up the process.
upvoted 11 times

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

Selected Answer: B

Provisioned concurrency – Provisioned concurrency initializes a requested number of execution environments so that they are prepared to respond immediately to your function's invocations. Note that configuring provisioned concurrency incurs charges to your AWS account.
upvoted 7 times

✉  **TariqKipkemei**  1 month, 1 week ago

Selected Answer: B

Provisioned concurrency pre-initializes execution environments which are prepared to respond immediately to incoming function requests.
upvoted 1 times

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

Selected Answer: B

Provisioned concurrency ensures a configured number of execution environments are ready to serve requests to the Lambda function. This avoids cold starts where the function would otherwise need to load all the libraries on each invocation.
upvoted 2 times

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

Selected Answer: B

Provisioned concurrency ensures a configured number of execution environments are ready to serve requests to the Lambda function. This avoids cold starts where the function would otherwise need to load all the libraries on each invocation.
upvoted 1 times

✉  **elearningtakai** 8 months ago

Selected Answer: B

Answer B is correct
<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html>
Answer C: need to modify the application
upvoted 4 times

✉  **elearningtakai** 8 months ago

This is relevant to "cold start" with keywords: "Lambda function loads many libraries"

upvoted 1 times

✉  **Karlos99** 8 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html>
upvoted 3 times

A company is migrating its on-premises workload to the AWS Cloud. The company already uses several Amazon EC2 instances and Amazon RDS DB instances. The company wants a solution that automatically starts and stops the EC2 instances and DB instances outside of business hours. The solution must minimize cost and infrastructure maintenance.

Which solution will meet these requirements?

- A. Scale the EC2 instances by using elastic resize. Scale the DB instances to zero outside of business hours.
- B. Explore AWS Marketplace for partner solutions that will automatically start and stop the EC2 instances and DB instances on a schedule.
- C. Launch another EC2 instance. Configure a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule.
- D. Create an AWS Lambda function that will start and stop the EC2 instances and DB instances. Configure Amazon EventBridge to invoke the Lambda function on a schedule.

Correct Answer: A

Community vote distribution

D (100%)

✉  **ktulu2602** Highly Voted 8 months, 3 weeks ago

Selected Answer: D

The most efficient solution for automatically starting and stopping EC2 instances and DB instances on a schedule while minimizing cost and infrastructure maintenance is to create an AWS Lambda function and configure Amazon EventBridge to invoke the function on a schedule.

Option A, scaling EC2 instances by using elastic resize and scaling DB instances to zero outside of business hours, is not feasible as DB instances cannot be scaled to zero.

Option B, exploring AWS Marketplace for partner solutions, may be an option, but it may not be the most efficient solution and could potentially add additional costs.

Option C, launching another EC2 instance and configuring a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule, adds unnecessary infrastructure and maintenance.

upvoted 12 times

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

Selected Answer: D

Create an AWS Lambda function that will start and stop the EC2 instances and DB instances. Configure Amazon EventBridge to invoke the Lambda function on a schedule.

upvoted 1 times

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

Selected Answer: D

This option leverages AWS Lambda and EventBridge to automatically schedule the starting and stopping of resources.

Lambda provides the script/code to stop/start instances without managing servers.

EventBridge triggers the Lambda on a schedule without cronjobs.

No additional code or third party tools needed.

Serverless, maintenance-free solution

upvoted 3 times

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

Selected Answer: D

Minimize cost and maintenance...

upvoted 1 times

✉  **dcp** 8 months, 2 weeks ago

Selected Answer: D

DDDDDDDDDDDD

upvoted 1 times

A company hosts a three-tier web application that includes a PostgreSQL database. The database stores the metadata from documents. The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month. The documents are stored in Amazon S3. The documents are usually written only once, but they are updated frequently.

The reporting process takes a few hours with the use of relational queries. The reporting process must not prevent any document modifications or the addition of new documents. A solutions architect needs to implement a solution to speed up the reporting process.

Which solution will meet these requirements with the LEAST amount of change to the application code?

- A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica. Scale the read replica to generate the reports.
- B. Set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica. Issue queries to the Aurora Replica to generate the reports.
- C. Set up a new Amazon RDS for PostgreSQL Multi-AZ DB instance. Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node.
- D. Set up a new Amazon DynamoDB table to store the documents. Use a fixed write capacity to support new document entries. Automatically scale the read capacity to support the reports.

Correct Answer: D

Community vote distribution

B (94%)	6%
---------	----

✉  **Guru4Cloud** 2 months, 1 week ago

Selected Answer: B

The key reasons are:

Aurora PostgreSQL provides native PostgreSQL compatibility, so minimal code changes would be required.
Using an Aurora Replica separates the reporting workload from the main workload, preventing any slowdown of document updates/inserts.
Aurora can auto-scale read replicas to handle the reporting load.
This allows leveraging the existing PostgreSQL database without major changes. DynamoDB would require more significant rewrite of data access code.
RDS Multi-AZ alone would not fully separate the workloads, as the secondary is for HA/failover more than scaling read workloads.

upvoted 1 times

✉  **KMohsoe** 6 months, 1 week ago

Selected Answer: A

Why not A? :(

upvoted 1 times

✉  **wRhIH** 5 months, 1 week ago

"The reporting process takes a few hours with the use of RELATIONAL queries."

upvoted 2 times

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

Selected Answer: B

Load balancing = Read replica

High availability = Multi AZ

upvoted 2 times

✉  **lexotan** 7 months, 1 week ago

Selected Answer: B

B is the right one. why admin does not correct these wrong answers?

upvoted 3 times

✉  **imvb88** 7 months, 2 weeks ago

Selected Answer: B

The reporting process queries the metadata (not the documents) and use relational queries-> A, D out

C: wrong since secondary RDS node in MultiAZ setup is in standby mode, not available for querying

B: reporting using a Replica is a design pattern. Using Aurora is an exam pattern.

upvoted 4 times

 **Whericanstart** 8 months, 2 weeks ago

Selected Answer: B

B is right..

upvoted 1 times

 **Maximus007** 8 months, 2 weeks ago

Selected Answer: B

While both B&D seems to be a relevant, ChatGPT suggest B as a correct one

upvoted 1 times

 **cegama543** 8 months, 2 weeks ago

Selected Answer: B

Option B (Set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica. Issue queries to the Aurora Replica to generate the reports) is the best option for speeding up the reporting process for a three-tier web application that includes a PostgreSQL database storing metadata from documents, while not impacting document modifications or additions, with the least amount of change to the application code.

upvoted 2 times

 **UnluckyDucky** 8 months, 3 weeks ago

Selected Answer: B

"LEAST amount of change to the application code"

Aurora is a relational database, it supports PostgreSQL and with the help of read replicas we can issue the reporting process that take several hours to the replica, therefore not affecting the primary node which can handle new writes or document modifications.

upvoted 1 times

 **Ashukaushal619** 8 months, 3 weeks ago

its D only ,recorrected

upvoted 1 times

 **Ashukaushal619** 8 months, 3 weeks ago

Selected Answer: B

bbbbbbbb

upvoted 1 times

A company has a three-tier application on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB), then to Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier. The application tier makes calls to a database.

What should a solutions architect do to improve the security of the data in transit?

- A. Configure a TLS listener. Deploy the server certificate on the NLB.
- B. Configure AWS Shield Advanced. Enable AWS WAF on the NLB.
- C. Change the load balancer to an Application Load Balancer (ALB). Enable AWS WAF on the ALB.
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS).

Correct Answer: A

Community vote distribution

A (100%)

 **fruto123**  8 months, 3 weeks ago

Selected Answer: A

Network Load Balancers now support TLS protocol. With this launch, you can now offload resource intensive decryption/encryption from your application servers to a high throughput, and low latency Network Load Balancer. Network Load Balancer is now able to terminate TLS traffic and set up connections with your targets either over TCP or TLS protocol.

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

https://exampleloadbalancer.com/nlbtls_demo.html

upvoted 12 times

 **imvb88**  7 months, 2 weeks ago

Selected Answer: A

security of data in transit -> think of SSL/TLS. Check: NLB supports TLS

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

B (DDoS), C (SQL Injection), D (EBS) is for data at rest.

upvoted 9 times

 **TariqKipkemei**  1 month, 1 week ago

Selected Answer: A

secure data in transit = TLS

upvoted 1 times

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: A

TLS provides encryption for data in motion over the network, protecting against eavesdropping and tampering. A valid server certificate signed by a trusted CA will provide further security.

upvoted 2 times

 **klayytech** 8 months ago

Selected Answer: A

To improve the security of data in transit, you can configure a TLS listener on the Network Load Balancer (NLB) and deploy the server certificate on it. This will encrypt traffic between clients and the NLB. You can also use AWS Certificate Manager (ACM) to provision, manage, and deploy SSL/TLS certificates for use with AWS services and your internal connected resources1.

You can also change the load balancer to an Application Load Balancer (ALB) and enable AWS WAF on it. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources3.

the A and C correct without transit but the need to improve the security of the data in transit? so he need SSL/TLS certificates

upvoted 1 times

 **Maximus007** 8 months, 2 weeks ago

Selected Answer: A

agree with fruto123

upvoted 3 times

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.

Which Amazon EC2 pricing option is the MOST cost-effective?

- A. Dedicated Reserved Hosts
- B. Dedicated On-Demand Hosts
- C. Dedicated Reserved Instances
- D. Dedicated On-Demand Instances

Correct Answer: A

Community vote distribution

A (83%)	C (17%)
---------	---------

✉  **fkie4** Highly Voted 8 months, 3 weeks ago

Selected Answer: A

"predictable capacity and uptime requirements" means "Reserved"
"sockets and cores" means "dedicated host"

upvoted 6 times

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

Selected Answer: A

Dedicated Hosts give you visibility and control over how instances are placed on a physical server and also enable you to use your existing server-bound software licenses like Windows Server

upvoted 2 times

✉  **wsdasdasdqwdaw** 1 month, 1 week ago

Easy with one, but only 79% up to now answered correctly. It is A. Reserved because of the predictable and sockets and cores means dedicated host.

upvoted 1 times

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

Selected Answer: C

The correct answer is C. Dedicated Reserved Instances.

Dedicated Reserved Instances (DRIs) are the most cost-effective option for workloads that have predictable capacity and uptime requirements. DRIs offer a significant discount over On-Demand Instances, and they can be used to lock in a price for a period of time.

In this case, the company has predictable capacity and uptime requirements because the software has a software licensing model using sockets and cores. The company also wants to use its existing licenses, which were purchased earlier this year. Therefore, DRIs are the most cost-effective option.

upvoted 2 times

✉  **riccardoto** 3 months, 3 weeks ago

Selected Answer: C

I don't agree with people voting "A". The question reference that the COTS Application has a licensing model based on "sockets and cores". The question does not specify if it means TCP sockets (= open connections) or hardware sockets, so I assume that "TCP sockets are intended". If this is the case, sockets and cores can also remain stable with reserved instances - which are cheaper than reserved hosts.

I would go with "A" only if the question would clearly state that the COTS application has some strong dependency on physical hardware.

upvoted 1 times

✉  **riccardoto** 3 months, 3 weeks ago

note: instead, if by socket we mean "CPU sockets", then A would be the right one.

upvoted 1 times

✉  **imvb88** 7 months, 2 weeks ago

Selected Answer: A

Bring custom purchased licenses to AWS -> Dedicated Host -> C,D out
Need cost effective solution -> "reserved" -> A

upvoted 4 times

✉  **imvb88** 7 months, 2 weeks ago

<https://aws.amazon.com/ec2/dedicated-hosts/>

Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2, so that you get the flexibility and cost effectiveness of using your own licenses, but with the resiliency, simplicity and elasticity of AWS.

upvoted 1 times

 **aragon_saa** 8 months, 3 weeks ago

A

<https://www.examtopics.com/discussions/amazon/view/35818-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **fruto123** 8 months, 3 weeks ago

Selected Answer: A

Dedicated Host Reservations provide a billing discount compared to running On-Demand Dedicated Hosts. Reservations are available in three payment options.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-hosts-overview.html>

upvoted 3 times

 **Kenp1192** 8 months, 3 weeks ago

A

is the most cost effective

upvoted 1 times

A company runs an application on Amazon EC2 Linux instances across multiple Availability Zones. The application needs a storage layer that is highly available and Portable Operating System Interface (POSIX)-compliant. The storage layer must provide maximum data durability and must be shareable across the EC2 instances. The data in the storage layer will be accessed frequently for the first 30 days and will be accessed infrequently after that time.

Which solution will meet these requirements MOST cost-effectively?

- A. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Glacier.
- B. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Standard-Infrequent Access (S3 Standard-IA).
- C. Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA).
- D. Use the Amazon Elastic File System (Amazon EFS) One Zone storage class. Create a lifecycle management policy to move infrequently accessed data to EFS One Zone-Infrequent Access (EFS One Zone-IA).

Correct Answer: B

Community vote distribution

C (88%) 12%

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

Selected Answer: C

Multi AZ = both EFS and S3 support
Storage classes = both EFS and S3 support
POSIX file system access = only Amazon EFS supports
upvoted 6 times

✉  **maudsha**  4 weeks, 1 day ago

Selected Answer: C

Both standard and one zone have same durability.
<https://docs.aws.amazon.com/efs/latest/ug/storage-classes.html>

Also EFS one zone can work with multiple EC2s in different AZs. But there will be a cost involved when you are accessing the EFS from a different AZ EC2. (EC2 data access charges)
<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>
So if "all" EC2 instances accessing the files frequently there will be a storage cost + EC2 data access charges if you choose one zone.

So i would choose C.
upvoted 1 times

✉  **beast2091** 1 month ago

Ans: C
upvoted 1 times

✉  **baba365** 2 months, 1 week ago

Ans: D, one-zone IA for 'most cost effective' .

<https://aws.amazon.com/efs/features/infrequent-access/>
upvoted 1 times

✉  **AAAWrekng** 1 month ago

How does D fulfill the data durability requirement? Requirements must be met first, then consider 'most cost effective' - if you go to a tire shop, and say you want 4 new tires as cheap as possible. And they take off 4 tires and put on 2... Then they say you wanted it as cheap as possible...
upvoted 1 times

✉  **LazyTs** 2 months, 3 weeks ago

Selected Answer: C

POSIX => EFS
<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>
upvoted 2 times

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

Selected Answer: C

Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA).

upvoted 1 times

 **RainWhisper** 5 months, 1 week ago

Selected Answer: D

Amazon Elastic File System (Amazon EFS) Standard storage class = "maximum data durability"

upvoted 1 times

 **Yadav_Sanjay** 5 months, 2 weeks ago

Selected Answer: D

D - It should be cost-effective

upvoted 2 times

 **Abrar2022** 5 months, 2 weeks ago

Selected Answer: C

POSIX file system access = only Amazon EFS supports

upvoted 3 times

 **imvb88** 7 months, 2 weeks ago

Selected Answer: C

POSIX + sharable across EC2 instances --> EFS --> A, B out

Instances run across multiple AZ -> C is needed.

upvoted 1 times

 **Whericanstart** 8 months, 2 weeks ago

Selected Answer: C

Linux based system points to EFS plus POSIX-compliant is also EFS related.

upvoted 2 times

 **fkie4** 8 months, 3 weeks ago

Selected Answer: C

"POSIX-compliant" means EFS.

also, file system can be shared with multiple EC2 instances means "EFS"

upvoted 4 times

 **KAUS2** 8 months, 3 weeks ago

Selected Answer: C

Option C is the correct answer .

upvoted 1 times

 **Ruhi02** 8 months, 3 weeks ago

Answer c : <https://aws.amazon.com/efs/features/infrequent-access/>

upvoted 1 times

 **ktulu2602** 8 months, 3 weeks ago

Selected Answer: C

Option A, using S3, is not a good option as it is an object storage service and not POSIX-compliant. Option B, using S3 Standard-IA, is also not a good option as it is an object storage service and not POSIX-compliant. Option D, using EFS One Zone, is not the best option for high availability since it is only stored in a single AZ.

upvoted 2 times

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.

Which additional configuration strategy should the solutions architect use to meet these requirements?

- A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
- C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Correct Answer: C

Community vote distribution

C (100%)

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: C

Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.

upvoted 1 times

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: C

C) Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.

This option follows the principle of least privilege by only allowing necessary access:

Web server SG allows port 443 from load balancer SG (not open to world)

MySQL SG allows port 3306 only from web server SG

upvoted 2 times

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: C

Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group

upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: C

Option C is the correct choice.

upvoted 1 times

 **WhericanIstart** 8 months, 2 weeks ago

Selected Answer: C

Load balancer is public facing accepting all traffic coming towards the VPC (0.0.0.0/0). The web server needs to trust traffic originating from the ALB. The DB will only trust traffic originating from the Web server on port 3306 for MySQL

upvoted 4 times

 **fkie4** 8 months, 3 weeks ago

Selected Answer: C

Just C. plain and simple

upvoted 1 times

 **aragon_saa** 8 months, 3 weeks ago

C

<https://www.examtopics.com/discussions/amazon/view/43796-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: C

CCCCCC

upvoted 1 times

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

- A. Implement Amazon SNS to store the database calls.
- B. Implement Amazon ElastiCache to cache the large datasets.
- C. Implement an RDS for MySQL read replica to cache database calls.
- D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Correct Answer: B

Community vote distribution

B (100%)

✉  **elearningtakai** Highly Voted 8 months ago

Selected Answer: B

the best solution is to implement Amazon ElastiCache to cache the large datasets, which will store the frequently accessed data in memory, allowing for faster retrieval times. This can help to alleviate the frequent calls to the database, reduce latency, and improve the overall performance of the backend tier.

upvoted 6 times

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

Selected Answer: B

B) Implement Amazon ElastiCache to cache the large datasets.

The key issue is repeated calls to return identical datasets from the RDS database causing performance slowdowns.

Implementing Amazon ElastiCache for Redis or Memcached would allow these repeated query results to be cached, improving backend performance by reducing load on the database.

upvoted 2 times

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

B) Implement Amazon ElastiCache to cache the large datasets.

The key issue is repeated calls to return identical datasets from the RDS database causing performance slowdowns.

Implementing Amazon ElastiCache for Redis or Memcached would allow these repeated query results to be cached, improving backend performance by reducing load on the database.

upvoted 1 times

✉  **Abrar2022** 5 months, 2 weeks ago

Selected Answer: B

Thanks Tariq for the simplified answer below:

frequent identical calls = ElastiCache

upvoted 2 times

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

frequent identical calls = ElastiCache

upvoted 1 times

✉  **Mikebonsi70** 8 months, 1 week ago

Tricky question, anyway.

upvoted 2 times

✉  **Mikebonsi70** 8 months, 1 week ago

Yes, cashing is the solution but is Elasticache compatible with RDS MySQL DB? So, what about the answer C with a DB read replica? For me it's C.

upvoted 1 times

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

B

<https://www.examtopics.com/discussions/amazon/view/27874-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **fruto123** 8 months, 3 weeks ago

Selected Answer: B

Key term is identical datasets from the database it means caching can solve this issue by cached in frequently used dataset from DB
upvoted 3 times

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

Which combination of actions should the solutions architect take to accomplish this goal? (Choose two.)

- A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the AdministratorAccess IAM policy attached.
- D. Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.

Correct Answer: DE

Community vote distribution

DE (100%)

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: DE

Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.

Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.

upvoted 1 times

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: DE

The two actions that should be taken to follow the principle of least privilege are:

D) Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.

E) Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.

The principle of least privilege states that users should only be given the minimal permissions necessary to perform their job function.

upvoted 1 times

 **alexandercamachop** 5 months, 4 weeks ago

Selected Answer: DE

Option D, creating a new IAM user and adding them to a group with an IAM policy that allows AWS CloudFormation actions only, ensures that the deployment engineer has the necessary permissions to perform AWS CloudFormation operations while limiting access to other resources and actions. This aligns with the principle of least privilege by providing the minimum required permissions for their job activities.

Option E, creating an IAM role with specific permissions for AWS CloudFormation stack operations and allowing the deployment engineer to assume that role, is another valid approach. By using an IAM role, the deployment engineer can assume the role when necessary, granting them temporary permissions to perform CloudFormation actions. This provides a level of separation and limits the permissions granted to the engineer to only the required CloudFormation operations.

upvoted 1 times

 **Babaaaaa** 6 months ago

Selected Answer: DE

Dddd,Eeee

upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: DE

D & E are a good choices

upvoted 1 times

 **aragon_saa** 8 months, 3 weeks ago

D, E
<https://www.examtopics.com/discussions/amazon/view/46428-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

 **fruto123** 8 months, 3 weeks ago

Selected Answer: DE

I agree DE

upvoted 2 times

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

- A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.
- B. Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and the database tier.
- C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs, and configure VPC peering.
- D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group.

Correct Answer: D

Community vote distribution

D (100%)

 **smartegnine** 5 months, 1 week ago

Selected Answer: D

Security Groups are tied on instance whereas network ACLs are tied to Subnet.

upvoted 3 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: D

Security group defaults block all inbound traffic..Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group

upvoted 3 times

 **elearningtakai** 8 months ago

Selected Answer: D

By default, all inbound traffic to an RDS instance is blocked. Therefore, an inbound rule needs to be added to the security group of the RDS instance to allow traffic from the security group of the web tier's EC2 instances.

upvoted 2 times

 **Russ99** 8 months, 1 week ago

Selected Answer: D

D is the correct answer

upvoted 1 times

 **aragon_saa** 8 months, 3 weeks ago

D

<https://www.examtopics.com/discussions/amazon/view/81445-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **KAUS2** 8 months, 3 weeks ago

Selected Answer: D

D is correct option

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: D

ddddd

upvoted 2 times

A company has a large dataset for its online advertising business stored in an Amazon RDS for MySQL DB instance in a single Availability Zone. The company wants business reporting queries to run without impacting the write operations to the production DB instance.

Which solution meets these requirements?

- A. Deploy RDS read replicas to process the business reporting queries.
- B. Scale out the DB instance horizontally by placing it behind an Elastic Load Balancer.
- C. Scale up the DB instance to a larger instance type to handle write operations and queries.
- D. Deploy the DB instance in multiple Availability Zones to process the business reporting queries.

Correct Answer: D

Community vote distribution

A (100%)

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

Selected Answer: A

A) Deploy RDS read replicas to process the business reporting queries.

The key points are:

RDS read replicas allow read-only copies of the production DB instance to be created

Queries to the read replica don't affect the source DB instance performance

This isolates reporting queries from production traffic and write operations

So using RDS read replicas is the best way to meet the requirements of running reporting queries without impacting production write operations.

upvoted 1 times

✉  **james2033** 4 months, 1 week ago

Selected Answer: A

"single AZ", "large dataset", "Amazon RDS for MySQL database". Want "business report queries". --> Solution "Read replicas", choose A.

upvoted 1 times

✉  **antropaws** 6 months ago

Selected Answer: A

No doubt A.

upvoted 2 times

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

Load balance read operations = read replicas

upvoted 1 times

✉  **TariqKipkemei** 1 month, 1 week ago

reports=read replica

upvoted 1 times

✉  **KAUS2** 8 months, 3 weeks ago

Selected Answer: A

Option "A" is the right answer . Read replica use cases - You have a production database that is taking on 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 production application is unaffected
- Read replicas are used for SELECT (=read) only kind of statements (not INSERT, UPDATE, DELETE)

upvoted 2 times

✉  **taehyeki** 8 months, 3 weeks ago

Selected Answer: A

aaaaaaaaaaaa

upvoted 2 times

 **cegama543** 8 months, 3 weeks ago

Selected Answer: A

option A is the best solution for ensuring that business reporting queries can run without impacting write operations to the production DB instance.

upvoted 3 times

A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). All ecommerce data is stored in an Amazon RDS for MariaDB Multi-AZ DB instance.

The company wants to optimize customer session management during transactions. The application must store session data durably.

Which solutions will meet these requirements? (Choose two.)

- A. Turn on the sticky sessions feature (session affinity) on the ALB.
- B. Use an Amazon DynamoDB table to store customer session information.
- C. Deploy an Amazon Cognito user pool to manage user session information.
- D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.
- E. Use AWS Systems Manager Application Manager in the application to manage user session information.

Correct Answer: BD

Community vote distribution

AD (55%)	AB (34%)	7%
----------	----------	----

 **fruto123** Highly Voted 8 months, 3 weeks ago

Selected Answer: AD

It is A and D. Proof is in link below.

<https://aws.amazon.com/caching/session-management/>
upvoted 17 times

 **maver144** Highly Voted 7 months, 4 weeks ago

Selected Answer: AB

ElastiCache is cache it cannot store sessions durably
upvoted 7 times

 **Fizbo** 1 week, 4 days ago

It can.

<https://aws.amazon.com/caching/session-management/>
upvoted 1 times

 **daniel1** Most Recent 1 month, 1 week ago

Selected Answer: BD

Chatgpt4 says B and D
Option A (Sticky sessions) is more for ensuring that a client's requests are sent to the same target once a session is established, but it doesn't provide a mechanism for durable session data storage across multiple instances. Option C (Amazon Cognito) is more for user identity management rather than session data storage during transactions. Option E (AWS Systems Manager Application Manager) is not a suitable or standard choice for session management in applications.

upvoted 2 times

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: AD

Well, this documentation says it all. Option A is obvious, and D ElastiCache for Redis, can even support replication in case of node failure/session data loss.
<https://aws.amazon.com/caching/session-management/>
upvoted 2 times

 **Guru4Cloud** 2 months, 4 weeks ago

Selected Answer: AD

It is A and D. Proof is in link below.

<https://aws.amazon.com/caching/session-management/>
upvoted 2 times

 **coolkidsclubvip** 3 months, 3 weeks ago

Selected Answer: AB

cache is not durable...at all
upvoted 2 times

 **mrsoa** 4 months ago

Selected Answer: AD

go for AD

upvoted 1 times

 **Kaiden123** 4 months, 1 week ago

Selected Answer: B

go with B

upvoted 2 times

 **msdnpro** 4 months, 2 weeks ago

Selected Answer: AD

For D : "Amazon ElastiCache for Redis is highly suited as a session store to manage session information such as user authentication tokens, session state, and more."

<https://aws.amazon.com/elasticsearch/redis/>

upvoted 2 times

 **mattcl** 5 months, 1 week ago

B and D: "The application must store session data durably" with Sticky sessions the application doesn't store anything.

upvoted 3 times

 **Axeashes** 5 months, 2 weeks ago

An option for data persistence for ElastiCache:

[https://aws.amazon.com/elasticsearch/faqs/#:~:text=Q%3A%20Does%20Amazon%20ElastiCache%20for%20Redis%20support%20Redis%20persistence%3F%0AAmazon%20ElastiCache%20for%20Redis%20doesn%20support%20the%20AOF%20\(Append%20Only%20File\)%20feature%20but%20you%20can%20achieve%20persistence%20by%20snapshotting%20your%20Redis%20data%20using%20the%20Backup%20and%20Restore%20feature.%20Please%20see%20here%20for%20details.](https://aws.amazon.com/elasticsearch/faqs/#:~:text=Q%3A%20Does%20Amazon%20ElastiCache%20for%20Redis%20support%20Redis%20persistence%3F%0AAmazon%20ElastiCache%20for%20Redis%20doesn%20support%20the%20AOF%20(Append%20Only%20File)%20feature%20but%20you%20can%20achieve%20persistence%20by%20snapshotting%20your%20Redis%20data%20using%20the%20Backup%20and%20Restore%20feature.%20Please%20see%20here%20for%20details.)

upvoted 2 times

 **dpaz** 6 months ago

Selected Answer: AB

ElastiCache is not durable so session info has to be stored in DynamoDB.

upvoted 3 times

 **Alizade** 7 months ago

Selected Answer: AD

A. Turn on the sticky sessions feature (session affinity) on the ALB.

D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.

upvoted 1 times

 **Lalo** 7 months, 1 week ago

<https://aws.amazon.com/es/caching/session-management/>

Sticky sessions, also known as session affinity, allow you to route a site user to the particular web server that is managing that individual user's session

In order to address scalability and to provide a shared data storage for sessions that can be accessible from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution to for this is to leverage an In-Memory Key/Value store such as Redis and Memcached.

upvoted 4 times

 **pmd2023** 7 months, 2 weeks ago

Redis was not built to be a durable and consistent database. If you need a durable, Redis-compatible database, consider Amazon MemoryDB for Redis. Because MemoryDB uses a durable transactional log that stores data across multiple Availability Zones (AZs), you can use it as your primary database. MemoryDB is purpose-built to enable developers to use the Redis API without worrying about managing a separate cache, database, or the underlying infrastructure. <https://aws.amazon.com/redis/>

upvoted 1 times

 **kraken21** 8 months ago

Selected Answer: AD

optimize customer session management during transactions. Since the session store will be during the transaction and we have another DB for pre/post transaction storage(Maria DB).

upvoted 1 times

 **test_devops_aws** 8 months, 1 week ago

D is incorrect but dyamodb not support mariaDB. can someone explain?

upvoted 1 times

 **Keglic** 8 months ago

DynamoDB here is a new DB just for the purpose of storing session data... MariaDB is for eCommerce data.

upvoted 1 times

A company needs a backup strategy for its three-tier stateless web application. The web application runs on Amazon EC2 instances in an Auto Scaling group with a dynamic scaling policy that is configured to respond to scaling events. The database tier runs on Amazon RDS for PostgreSQL. The web application does not require temporary local storage on the EC2 instances. The company's recovery point objective (RPO) is 2 hours.

The backup strategy must maximize scalability and optimize resource utilization for this environment.

Which solution will meet these requirements?

- A. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances and database every 2 hours to meet the RPO.
- B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.
- C. Retain the latest Amazon Machine Images (AMIs) of the web and application tiers. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.
- D. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances every 2 hours. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.

Correct Answer: D

Community vote distribution

C (82%)	Other
---------	-------

✉  **elearningtakai** Highly Voted 8 months, 2 weeks ago

Selected Answer: C

that if there is no temporary local storage on the EC2 instances, then snapshots of EBS volumes are not necessary. Therefore, if your application does not require temporary storage on EC2 instances, using AMIs to back up the web and application tiers is sufficient to restore the system after a failure.

Snapshots of EBS volumes would be necessary if you want to back up the entire EC2 instance, including any applications and temporary data stored on the EBS volumes attached to the instances. When you take a snapshot of an EBS volume, it backs up the entire contents of that volume. This ensures that you can restore the entire EC2 instance to a specific point in time more quickly. However, if there is no temporary data stored on the EBS volumes, then snapshots of EBS volumes are not necessary.

upvoted 23 times

✉  **MssP** 8 months, 1 week ago

I think "temporal local storage" refers to "instance store", no instance store is required. EBS is durable storage, not temporal.
upvoted 1 times

✉  **MssP** 8 months, 1 week ago

Look at the first paragraph. <https://repost.aws/knowledge-center/instance-store-vs-ebs>
upvoted 1 times

✉  **CloudForFun** Highly Voted 8 months, 2 weeks ago

Selected Answer: C

The web application does not require temporary local storage on the EC2 instances => No EBS snapshot is required, retaining the latest AMI is enough.

upvoted 9 times

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

Selected Answer: C

"The web application does not require temporary local storage on the EC2 instances" rules out any option to back up the EC2 EBS volumes.
upvoted 1 times

✉  **darekw** 4 months ago

Question says: ...stateless web application.. that means application doesn't store any data, so no EBS required
upvoted 1 times

✉  **kruasan** 7 months ago

Selected Answer: C

Since the application has no local data on instances, AMIs alone can meet the RPO by restoring instances from the most recent AMI backup. When combined with automated RDS backups for the database, this provides a complete backup solution for this environment.
The other options involving EBS snapshots would be unnecessary given the stateless nature of the instances. AMIs provide all the backup needed for the app tier.

This uses native, automated AWS backup features that require minimal ongoing management:

- AMI automated backups provide point-in-time recovery for the stateless app tier.
- RDS automated backups provide point-in-time recovery for the database.

upvoted 2 times

✉ **neosis91** 7 months, 1 week ago

Selected Answer: B

BBBBBBBBBBB

upvoted 1 times

✉ **Rob1L** 8 months, 1 week ago

Selected Answer: D

I vote for D

upvoted 1 times

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

Selected Answer: C

makes more sense.

upvoted 2 times

✉ **nileshlg** 8 months, 2 weeks ago

Selected Answer: C

Answer is C. Keyword to notice "Stateless"

upvoted 2 times

✉ **cra2yk** 8 months, 2 weeks ago

Selected Answer: C

why B? I mean "stateless" and "does not require temporary local storage" have indicate that we don't need to take snapshot for ec2 volume.
upvoted 3 times

✉ **ktulu2602** 8 months, 3 weeks ago

Selected Answer: B

Option B is the most appropriate solution for the given requirements.

With this solution, a snapshot lifecycle policy can be created to take Amazon Elastic Block Store (Amazon EBS) snapshots periodically, which will ensure that EC2 instances can be restored in the event of an outage. Additionally, automated backups can be enabled in Amazon RDS for PostgreSQL to take frequent backups of the database tier. This will help to minimize the RPO to 2 hours.

Taking snapshots of Amazon EBS volumes of the EC2 instances and database every 2 hours (Option A) may not be cost-effective and efficient, as this approach would require taking regular backups of all the instances and volumes, regardless of whether any changes have occurred or not. Retaining the latest Amazon Machine Images (AMIs) of the web and application tiers (Option C) would provide only an image backup and not a data backup, which is required for the database tier. Taking snapshots of Amazon EBS volumes of the EC2 instances every 2 hours and enabling automated backups in Amazon RDS and using point-in-time recovery (Option D) would result in higher costs and may not be necessary to meet the RPO requirement of 2 hours.

upvoted 4 times

✉ **cegama543** 8 months, 3 weeks ago

Selected Answer: B

B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.

The best solution is to configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots, and enable automated backups in Amazon RDS to meet the RPO. An RPO of 2 hours means that the company needs to ensure that the backup is taken every 2 hours to minimize data loss in case of a disaster. Using a snapshot lifecycle policy to take Amazon EBS snapshots will ensure that the web and application tier can be restored quickly and efficiently in case of a disaster. Additionally, enabling automated backups in Amazon RDS will ensure that the database tier can be restored quickly and efficiently in case of a disaster. This solution maximizes scalability and optimizes resource utilization because it uses automated backup solutions built into AWS.

upvoted 3 times

A company wants to deploy a new public web application on AWS. The application includes a web server tier that uses Amazon EC2 instances. The application also includes a database tier that uses an Amazon RDS for MySQL DB instance.

The application must be secure and accessible for global customers that have dynamic IP addresses.

How should a solutions architect configure the security groups to meet these requirements?

- A. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
- B. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
- C. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the IP addresses of the customers.
- D. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from 0.0.0.0/0.

Correct Answer: A

Community vote distribution

A (80%)

B (20%)

 **Guru4Cloud** 3 months ago

Selected Answer: A

It allows HTTPS access from any public IP address, meeting the requirement for global customer access.

HTTPS provides encryption for secure communication.

And for the database security group, only allowing inbound port 3306 from the web server security group properly restricts access to only the resources that need it.

upvoted 1 times

 **jayce5** 5 months, 4 weeks ago

Selected Answer: A

Should be A since the customer IPs are dynamically.

upvoted 1 times

 **antropaws** 6 months ago

Selected Answer: A

A no doubt.

upvoted 2 times

 **omoakin** 6 months ago

BBBBBBBBBBBBBBBBBBBBBBB

from customers IPs

upvoted 1 times

 **MostafaWardany** 5 months, 2 weeks ago

Correct answer A, customer dynamic IPs ==> 443 from 0.0.0.0/0

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: A

dynamic source ips = allow all traffic - Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.

upvoted 2 times

 **elearningtakai** 8 months ago

Selected Answer: A

If the customers have dynamic IP addresses, option A would be the most appropriate solution for allowing global access while maintaining security.

upvoted 3 times

 **Kenzo** 8 months, 1 week ago

Correct answer is A.

B and C are out.

D is out because it is accepting traffic from every where instead of from webservers only
upvoted 3 times

 **Grace83** 8 months, 1 week ago

A is correct

upvoted 3 times

 **WheretocanIstart** 8 months, 2 weeks ago

Selected Answer: B

Keyword dynamic ...A is the right answer. If the IP were static and specific, B would be the right answer

upvoted 3 times

 **boxu03** 8 months, 2 weeks ago

Selected Answer: A

aaaaaaa

upvoted 1 times

 **kprakashbehera** 8 months, 3 weeks ago

Selected Answer: A

Ans - A

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: A

aaaaaaa

upvoted 1 times

A payment processing company records all voice communication with its customers and stores the audio files in an Amazon S3 bucket. The company needs to capture the text from the audio files. The company must remove from the text any personally identifiable information (PII) that belongs to customers.

What should a solutions architect do to meet these requirements?

- A. Process the audio files by using Amazon Kinesis Video Streams. Use an AWS Lambda function to scan for known PII patterns.
- B. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start an Amazon Textract task to analyze the call recordings.
- C. Configure an Amazon Transcribe transcription job with PII redaction turned on. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start the transcription job. Store the output in a separate S3 bucket.
- D. Create an Amazon Connect contact flow that ingests the audio files with transcription turned on. Embed an AWS Lambda function to scan for known PII patterns. Use Amazon EventBridge to start the contact flow when an audio file is uploaded to the S3 bucket.

Correct Answer: C

Community vote distribution

C (100%)

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: C

speech to text = Amazon Transcribe
upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: C

Amazon Transcribe is a service provided by Amazon Web Services (AWS) that converts speech to text using automatic speech recognition (ASR) technology
upvoted 2 times

 **james2033** 4 months, 2 weeks ago

Selected Answer: C

AWS Transcribe <https://aws.amazon.com/transcribe/> . Redacting or identifying (Personally identifiable instance) PII in real-time stream <https://docs.aws.amazon.com/transcribe/latest/dg/pii-redaction-stream.html> .
upvoted 1 times

 **SimiTik** 7 months, 1 week ago

C
Amazon Transcribe is a service provided by Amazon Web Services (AWS) that converts speech to text using automatic speech recognition (ASR) technology. gtp
upvoted 2 times

 **elearningtakai** 8 months ago

Selected Answer: C

Option C is the most suitable solution as it suggests using Amazon Transcribe with PII redaction turned on. When an audio file is uploaded to the S3 bucket, an AWS Lambda function can be used to start the transcription job. The output can be stored in a separate S3 bucket to ensure that the PII redaction is applied to the transcript. Amazon Transcribe can redact PII such as credit card numbers, social security numbers, and phone numbers.
upvoted 3 times

 **WhericanIstart** 8 months, 2 weeks ago

Selected Answer: C

C for sure.....
upvoted 1 times

 **WhericanIstart** 8 months, 2 weeks ago

C for sure
upvoted 1 times

 **boxu03** 8 months, 2 weeks ago

Selected Answer: C

cccccccc

upvoted 1 times

 **Ruhi02** 8 months, 3 weeks ago

answer c

upvoted 1 times

 **KAUS2** 8 months, 3 weeks ago

Selected Answer: C

Option C is correct..

upvoted 1 times

A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the application during periods of high demand.

A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance always degrades when the number of read and write IOPS is higher than 20,000.

What should a solutions architect do to improve the application performance?

- A. Replace the volume with a magnetic volume.
- B. Increase the number of IOPS on the gp3 volume.
- C. Replace the volume with a Provisioned IOPS SSD (io2) volume.
- D. Replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes.

Correct Answer: C

Community vote distribution

B (46%) D (40%) 14%

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

Selected Answer: D

- A - Magnetic Max IOPS 200 - Wrong
- B - gp3 Max IOPS 16000 per volume - Wrong
- C - RDS not supported io2 - Wrong
- D - Correct; 2 gp3 volume with 16 000 each $2 \times 16000 = 32\,000$ IOPS
upvoted 25 times

 **baba365** 2 months, 1 week ago

'the application performance always degrades when the number of read and write IOPS is higher than 20,000' ... question didn't say read and write IOPs can't be higher than 32,000. Answer: C if it's based on performance and not cost related.

'Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1), and magnetic (also known as standard). They differ in performance characteristics and price, which means that you can tailor your storage performance and cost to the needs of your database workload.'

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

 **joechen2023** 5 months, 2 weeks ago

<https://repost.aws/knowledge-center/ebs-volume-type-differences>

RDS does support io2

upvoted 2 times

 **wRhIh** 5 months, 1 week ago

that Link is to EBS instead of RDS

upvoted 5 times

 **Michal_L_95** Highly Voted 8 months, 2 weeks ago

Selected Answer: B

It can not be option C as RDS does not support io2 storage type (only io1).

Here is a link to the RDS storage documentation: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

Also it is not the best option to take Magnetic storage as it supports max 1000 IOPS.

I vote for option B as gp3 storage type supports up to 64 000 IOPS where question mentioned with problem at level of 20 000.

upvoted 11 times

 **joechen2023** 5 months, 2 weeks ago

check the link below <https://repost.aws/knowledge-center/ebs-volume-type-differences>

it states:

General Purpose SSD volumes are good for a wide variety of transactional workloads that require less than the following:

16,000 IOPS

1,000 MiB/s of throughput

160-TiB volume size

upvoted 1 times

 **GalileoEC2** 8 months ago

is this true? Amazon RDS (Relational Database Service) supports the Provisioned IOPS SSD (io2) storage type for its database instances. The io2 storage type is designed to deliver predictable performance for critical and highly demanding database workloads. It provides higher durability, higher IOPS, and lower latency compared to other Amazon EBS (Elastic Block Store) storage types. RDS offers the option to choose between the General Purpose SSD (gp3) and Provisioned IOPS SSD (io2) storage types for database instances.

upvoted 1 times

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

Selected Answer: B

MySQL for gp3
support with 12,000–64,000 IOPS

When increase volume should increase the baseline 12000 to higher

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: D

1 x gp3 volume = max IOPS 16000
2 x gp3 volume = max IOPS 32000

upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: D

In this case, the database performance is degrading when the number of read and write IOPS is higher than 20,000. This indicates that the application is demanding more IOPS than the gp3 volume can provide.

Replacing the gp3 volume with two 1,000 GB gp3 volumes will allow the application to achieve the required IOPS and improve its performance. This is because two 1,000 GB gp3 volumes can provide up to 40,000 IOPS, which is more than the 20,000 IOPS that the application is demanding.

upvoted 2 times

 **Guru4Cloud** 3 months ago

Selected Answer: C

Option C, which involves replacing the gp3 volume with a Provisioned IOPS SSD (io2) volume and provisioning the necessary IOPS, is the most appropriate choice to improve application performance in this scenario. Your explanation is spot on, and it's essential to ensure that the provisioned IOPS exceed the 20,000 IOPS required to handle the database workload during periods of high demand.

Your analysis effectively rules out the other options (A, B, and D) and provides a clear justification for selecting option C. Well done!

upvoted 3 times

 **Sat897** 3 months, 2 weeks ago

Selected Answer: D

GP3 - Max IOPS 16000, So D is correct when they required more than 20000 IOPS

upvoted 2 times

 **Amycert** 3 months, 2 weeks ago

Selected Answer: B

B is the only one that makes sense.
A will actually be detrimental.
C is not supported, only io1
D is exactly the same

upvoted 2 times

 **riccardoto** 3 months, 3 weeks ago

Selected Answer: D

A: no, that would actually reduce the IOPS
B GP3 is not supported on multi-AZ RDS. See https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html
C: io2 is not supported in RDS (only io1)
D: correct answer ☐ that would result in aggregated IOPS of $16000 + 16000 = 320000$

upvoted 2 times

 **Chef_couincouin** 2 weeks, 5 days ago

General Purpose SSD gp3 storage is supported on Single-AZ and Multi-AZ DB instances, but isn't supported on Multi-AZ DB clusters

upvoted 1 times

 **IlaS** 4 months ago

Can anyone pls tell why B option is most voted ? For general purpose Ssd gp2 gp3 , the max oops can be 16000 only

upvoted 3 times

 **fuzzycr** 4 months, 2 weeks ago

Selected Answer: D

2 discos para multiplicar la cantidad de iops por disco, logrando mas de los 20k requeridos

upvoted 1 times

 **jaydesai8** 4 months, 3 weeks ago

Selected Answer: B

GP3 scales up to 64,000 IOPS - with an additional cost

<https://aws.amazon.com/about-aws/whats-new/2022/11/amazon-rds-general-purpose-gp3-storage-volumes/>

upvoted 4 times

 **riccardoto** 3 months, 3 weeks ago

gp3 is not supported on multi-AZ deployments - https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

 **MNotABot** 4 months, 3 weeks ago

whoever has picked B and D, be ready to repeat your solution to readjust IOPS, when more scalability is required in future. With C, issue will get fixed better.

upvoted 1 times

 **jaydesai8** 4 months, 3 weeks ago

RDS does not support IO2, it not supports io1 currently

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

 **samehpalass** 5 months, 1 week ago

Selected Answer: B

B-increase GP3 IOPS

DB storage size for gp3 above 400 G support up to 64,000 IOPS, please check the below link:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 3 times

 **mattcl** 5 months, 1 week ago

Answer B: For RDS MySql -> 12,000–64,000 IOPS

upvoted 1 times

 **secdgs** 5 months, 2 weeks ago

Selected Answer: B

B- RDS gp3 max iops 64000

C- RDS have only io1 disk type

D- RDS not have menu for separate EBS disk.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

 **AnishGS** 5 months, 2 weeks ago

Selected Answer: B

gp3 Support flexible IOPS , tested 13th June 2023

upvoted 1 times

An IAM user made several configuration changes to AWS resources in their company's account during a production deployment last week. A solutions architect learned that a couple of security group rules are not configured as desired. The solutions architect wants to confirm which IAM user was responsible for making changes.

Which service should the solutions architect use to find the desired information?

- A. Amazon GuardDuty
- B. Amazon Inspector
- C. AWS CloudTrail
- D. AWS Config

Correct Answer: B

Community vote distribution

C (100%)

 **cegama543** Highly Voted 8 months, 3 weeks ago

Selected Answer: C

C. AWS CloudTrail

The best option is to use AWS CloudTrail to find the desired information. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS account activities. CloudTrail can be used to log all changes made to resources in an AWS account, including changes made by IAM users, EC2 instances, AWS management console, and other AWS services. By using CloudTrail, the solutions architect can identify the IAM user who made the configuration changes to the security group rules.

upvoted 8 times

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

This is how you know not to trust the moderators with their answers.

upvoted 1 times

 **Wayne23Fang** 2 months, 2 weeks ago

There is an article "How to use AWS Config and CloudTrail to find who made changes to a resource" in aws blog. Given CloudTrail provided AWS config original info, it seems for this particular one, C is better than AWS config.

upvoted 2 times

 **Guru4Cloud** 3 months ago

Selected Answer: C

AWS CloudTrail is the correct service to use here to identify which user was responsible for the security group configuration changes

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: C

AWS CloudTrail

upvoted 1 times

 **Bezha** 8 months, 1 week ago

Selected Answer: C

AWS CloudTrail

upvoted 1 times

 **dcp** 8 months, 3 weeks ago

Selected Answer: C

C. AWS CloudTrail

upvoted 2 times

 **kprakashbehera** 8 months, 3 weeks ago

Selected Answer: C

CloudTrail logs will tell who did that

upvoted 2 times

 **KAUS2** 8 months, 3 weeks ago

Selected Answer: C

Option "C" AWS CloudTrail is correct.

upvoted 2 times

 **Nithin1119** 8 months, 3 weeks ago

CCCCCC

upvoted 2 times

A company has implemented a self-managed DNS service on AWS. The solution consists of the following:

- Amazon EC2 instances in different AWS Regions
- Endpoints of a standard accelerator in AWS Global Accelerator

The company wants to protect the solution against DDoS attacks.

What should a solutions architect do to meet this requirement?

- A. Subscribe to AWS Shield Advanced. Add the accelerator as a resource to protect.
- B. Subscribe to AWS Shield Advanced. Add the EC2 instances as resources to protect.
- C. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the accelerator.
- D. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the EC2 instances.

Correct Answer: A

Community vote distribution

A (94%) 6%

✉️  **WhericanIstart** Highly Voted 8 months, 2 weeks ago

Selected Answer: A

DDoS attacks = AWS Shield Advance
Shield Advance protects Global Accelerator, NLB, ALB, etc
upvoted 7 times

✉️  **Guru4Cloud** Most Recent 3 months ago

Selected Answer: B

So, the correct option is:

- B. Subscribe to AWS Shield Advanced. Add the EC2 instances as resources to protect.

Here's why this option is the most appropriate:

- A. While you can add the accelerator as a resource to protect with AWS Shield Advanced, it's generally more effective to protect the individual resources (in this case, the EC2 instances) because AWS Shield Advanced will automatically protect resources associated with Global Accelerator
upvoted 1 times

✉️  **Abrar2022** 5 months, 2 weeks ago

Selected Answer: A

DDoS attacks = AWS Shield Advance
resource as Global Acc
upvoted 2 times

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

Selected Answer: A

DDoS attacks = AWS Shield Advanced
upvoted 2 times

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

Selected Answer: A

Answer is A
<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-event-mitigation-logic-gax.html>
upvoted 1 times

✉️  **ktulu2602** 8 months, 3 weeks ago

Selected Answer: A

AWS Shield is a managed service that provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53.
upvoted 2 times

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

Selected Answer: A

aaaaa

accelator can not be attached to shield

upvoted 2 times

✉  **ktulu2602** 8 months, 3 weeks ago

Yes it can:

AWS Shield is a managed service that provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53.

upvoted 1 times

✉  **taehyeki** 8 months, 3 weeks ago

bbbbbbbbbb

upvoted 1 times

✉  **enzomv** 8 months, 3 weeks ago

Your origin servers can be Amazon Simple Storage Service (S3), Amazon EC2, Elastic Load Balancing, or a custom server outside of AWS. You can also enable AWS Shield Advanced directly on Elastic Load Balancing or Amazon EC2 in the following AWS Regions - Northern Virginia, Ohio, Oregon, Northern California, Montreal, São Paulo, Ireland, Frankfurt, London, Paris, Stockholm, Singapore, Tokyo, Sydney, Seoul, Mumbai, Milan, and Cape Town.

My answer is B

upvoted 1 times

✉  **enzomv** 8 months, 3 weeks ago

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-event-mitigation-logic-gax.html>

Sorry I meant A

upvoted 1 times

An ecommerce company needs to run a scheduled daily job to aggregate and filter sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 GB in size. Based on the number of sales events, the job can take up to an hour to complete. The CPU and memory usage of the job are constant and are known in advance.

A solutions architect needs to minimize the amount of operational effort that is needed for the job to run.

Which solution meets these requirements?

- A. Create an AWS Lambda function that has an Amazon EventBridge notification. Schedule the EventBridge event to run once a day.
- B. Create an AWS Lambda function. Create an Amazon API Gateway HTTP API, and integrate the API with the function. Create an Amazon EventBridge scheduled event that calls the API and invokes the function.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

Correct Answer: C

Community vote distribution

C (100%)

 **ktulu2602** Highly Voted 8 months, 3 weeks ago

Selected Answer: C

The requirement is to run a daily scheduled job to aggregate and filter sales records for analytics in the most efficient way possible. Based on the requirement, we can eliminate option A and B since they use AWS Lambda which has a limit of 15 minutes of execution time, which may not be sufficient for a job that can take up to an hour to complete.

Between options C and D, option C is the better choice since it uses AWS Fargate which is a serverless compute engine for containers that eliminates the need to manage the underlying EC2 instances, making it a low operational effort solution. Additionally, Fargate also provides instant scale-up and scale-down capabilities to run the scheduled job as per the requirement.

Therefore, the correct answer is:

C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

upvoted 16 times

 **Guru4Cloud** Most Recent 3 months ago

Selected Answer: C

C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: C

The best option is C.

'The job can take up to an hour to complete' rules out lambda functions as they only execute up to 15 mins. Hence option A and B are out.

'The CPU and memory usage of the job are constant and are known in advance' rules out the need for autoscaling. Hence option D is out.

upvoted 2 times

 **imvb88** 7 months, 2 weeks ago

Selected Answer: C

"1-hour job" -> A, B out since max duration for Lambda is 15 min

Between C and D, "minimize operational effort" means Fargate -> C

upvoted 4 times

 **klayytech** 8 months, 1 week ago

Selected Answer: C

The solution that meets the requirements with the least operational overhead is to create a **Regional AWS WAF web ACL with a rate-based rule** and associate the web ACL with the API Gateway stage. This solution will protect the application from HTTP flood attacks by monitoring incoming requests and blocking requests from IP addresses that exceed the predefined rate.

Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint is also a good solution but it requires more

operational overhead than the previous solution.

Using Amazon CloudWatch metrics to monitor the Count metric and alerting the security team when the predefined rate is reached is not a solution that can protect against HTTP flood attacks.

Creating an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours is not a solution that can protect against HTTP flood attacks.

upvoted 1 times

 **klayytech** 8 months, 1 week ago

Selected Answer: C

The solution that meets these requirements is C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job. This solution will minimize the amount of operational effort that is needed for the job to run.

AWS Lambda which has a limit of 15 minutes of execution time,

upvoted 1 times

A company needs to transfer 600 TB of data from its on-premises network-attached storage (NAS) system to the AWS Cloud. The data transfer must be complete within 2 weeks. The data is sensitive and must be encrypted in transit. The company's internet connection can support an upload speed of 100 Mbps.

Which solution meets these requirements MOST cost-effectively?

- A. Use Amazon S3 multi-part upload functionality to transfer the files over HTTPS.
- B. Create a VPN connection between the on-premises NAS system and the nearest AWS Region. Transfer the data over the VPN connection.
- C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.
- D. Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.

Correct Answer: B

Community vote distribution

C (100%)

✉  **shanwford** Highly Voted 7 months, 3 weeks ago

Selected Answer: C

With the existing data link the transfer takes ~ 600 days in the best case. Thus, (A) and (B) are not applicable. Solution (D) could meet the target with a transfer time of 6 days, but the lead time for the direct connect deployment can take weeks! Thus, (C) is the only valid solution.
upvoted 5 times

✉  **Guru4Cloud** Most Recent 3 months ago

Selected Answer: C

Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.

upvoted 1 times

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

Selected Answer: C

C is the best option considering the time and bandwidth limitations
upvoted 1 times

✉  **pbpally** 6 months, 3 weeks ago

Selected Answer: C

We need the admin in here to tell us how they plan on this being achieved over connection with such a slow connection lol.
It's C, folks.
upvoted 2 times

✉  **KAUS2** 8 months, 3 weeks ago

Selected Answer: C

Best option is to use multiple AWS Snowball Edge Storage Optimized devices. Option "C" is the correct one.
upvoted 1 times

✉  **ktulu2602** 8 months, 3 weeks ago

Selected Answer: C

All others are limited by the bandwidth limit
upvoted 1 times

✉  **ktulu2602** 8 months, 3 weeks ago

Or provisioning time in the D case
upvoted 1 times

✉  **KZM** 8 months, 3 weeks ago

It is C. Snowball (from Snow Family).
upvoted 1 times

✉  **cegama543** 8 months, 3 weeks ago

Selected Answer: C

C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.

The best option is to use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices and use the devices to transfer the data to Amazon S3. Snowball Edge is a petabyte-scale data transfer device that can help transfer large amounts of data securely and quickly. Using Snowball Edge can be the most cost-effective solution for transferring large amounts of data over long distances and can help meet the requirement of transferring 600 TB of data within two weeks.

upvoted 3 times

A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.

A solutions architect must design a solution to protect the application from this type of attack.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.
- B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
- C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.
- D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: B

Regional AWS WAF web ACL is a managed web application firewall that can be used to protect your API Gateway API from a variety of attacks, including HTTP flood attacks.

Rate-based rule is a type of rule that can be used to limit the number of requests that can be made from a single IP address within a specified period of time.

API Gateway stage is a logical grouping of API resources that can be used to control access to your API.

upvoted 4 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: B

Answer is B

upvoted 1 times

 **maxicalypse** 7 months, 3 weeks ago

B os correct

upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: B

A rate-based rule in AWS WAF allows the security team to configure thresholds that trigger rate-based rules, which enable AWS WAF to track the rate of requests for a specified time period and then block them automatically when the threshold is exceeded. This provides the ability to prevent HTTP flood attacks with minimal operational overhead.

upvoted 3 times

 **kampatra** 8 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html>

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: B

bbbbbbbb

upvoted 3 times

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.

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

- A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: C

Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe

upvoted 2 times

 **james2033** 4 months, 1 week ago

Selected Answer: C

Question keyword: "sends an alert", a new weather event is recorded". Answer keyword C "Amazon DynamoDB Streams on the table", "Amazon Simple Notification Service" (Amazon SNS). Choose C. Easy question.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html>

<https://aws.amazon.com/blogs/database/dynamodb-streams-use-cases-and-design-patterns/>

upvoted 2 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: C

Best answer is C

upvoted 1 times

 **TariqKipkemei** 1 month ago

DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table and stores this information in a log for up to 24 hours. This capture activity can also invoke triggers to write the event to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe to.

upvoted 2 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Selected Answer: C

The best solution to meet these requirements with the least amount of operational overhead is to enable Amazon DynamoDB Streams on the table and use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe. This solution requires minimal configuration and infrastructure setup, and Amazon DynamoDB Streams provide a low-latency way to capture changes to the DynamoDB table. The triggers automatically capture the changes and publish them to the SNS topic, which notifies the internal teams.

upvoted 4 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Answer A is not a suitable solution because it requires additional configuration to notify the internal teams, and it could add operational overhead to the application.

Answer B is not the best solution because it requires changes to the current application, which may affect its performance, and it creates additional work for the teams to subscribe to multiple topics.

Answer D is not a good solution because it requires a cron job to scan the table every minute, which adds additional operational overhead to the system.

Therefore, the correct answer is C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon SNS topic to which the teams can subscribe.

upvoted 2 times

 **Hemanthgowda1932** 8 months, 1 week ago

C is correct

upvoted 1 times

 **Santosh43** 8 months, 1 week ago

definitely C

upvoted 1 times

 **Bezha** 8 months, 1 week ago

Selected Answer: C

DynamoDB Streams

upvoted 3 times

 **sitha** 8 months, 3 weeks ago

Selected Answer: C

Answer : C

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: C

CCCCCC

upvoted 1 times