

A company wants to use the AWS Cloud to make an existing application highly available and resilient. The current version of the application resides in the company's data center. The application recently experienced data loss after a database server crashed because of an unexpected power outage.

The company needs a solution that avoids any single points of failure. The solution must give the application the ability to scale to meet user demand.

Which solution will meet these requirements?

- A. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration.
- B. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group in a single Availability Zone. Deploy the database on an EC2 instance. Enable EC2 Auto Recovery.
- C. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance with a read replica in a single Availability Zone. Promote the read replica to replace the primary DB instance if the primary DB instance fails.
- D. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Deploy the primary and secondary database servers on EC2 instances across multiple Availability Zones. Use Amazon Elastic Block Store (Amazon EBS) Multi-Attach to create shared storage between the instances.

Correct Answer: A

Community vote distribution

A (88%)	6%
---------	----

✉️  **Guru4Cloud** 3 months ago

Selected Answer: A

Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration

upvoted 2 times

✉️  **czyboi** 3 months, 3 weeks ago

Why is C incorrect ?

upvoted 1 times

✉️  **Guru4Cloud** 3 months ago

C is incorrect because the read replica also resides in a single AZ

upvoted 1 times

✉️  **antropaws** 6 months ago

Selected Answer: A

A most def.

upvoted 2 times

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

Selected Answer: A

Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration.

upvoted 2 times

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

Selected Answer: A

The correct answer is A. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration.

To make an existing application highly available and resilient while avoiding any single points of failure and giving the application the ability to scale to meet user demand, the best solution would be to deploy the application servers using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones and use an Amazon RDS DB instance in a Multi-AZ configuration.

By using an Amazon RDS DB instance in a Multi-AZ configuration, the database is automatically replicated across multiple Availability Zones, ensuring that the database is highly available and can withstand the failure of a single Availability Zone. This provides fault tolerance and avoids any single points of failure.

upvoted 2 times

✉ **Thief** 8 months, 1 week ago

Selected Answer: D

Why not D?

upvoted 1 times

✉ **Guru4Cloud** 3 months ago

D is incorrect because using Multi-Attach EBS adds complexity and doesn't provide automatic DB failover

upvoted 1 times

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

Answer D, deploying the primary and secondary database servers on EC2 instances across multiple Availability Zones and using Amazon Elastic Block Store (Amazon EBS) Multi-Attach to create shared storage between the instances, may provide high availability for the database but may introduce additional complexity, and management overhead, and potential performance issues.

upvoted 1 times

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

Selected Answer: A

Highly available = Multi-AZ approach

upvoted 2 times

✉ **nileshlg** 8 months, 2 weeks ago

Selected Answer: A

Answers is A

upvoted 1 times

✉ **dcp** 8 months, 2 weeks ago

Selected Answer: A

Option A is the correct solution. Deploying the application servers in an Auto Scaling group across multiple Availability Zones (AZs) ensures high availability and fault tolerance. An Auto Scaling group allows the application to scale horizontally to meet user demand. Using Amazon RDS DB instance in a Multi-AZ configuration ensures that the database is automatically replicated to a standby instance in a different AZ. This provides database redundancy and avoids any single point of failure.

upvoted 1 times

✉ **quentin17** 8 months, 2 weeks ago

Selected Answer: C

Highly available

upvoted 1 times

✉ **KAUS2** 8 months, 3 weeks ago

Selected Answer: A

Yes , agree with A

upvoted 1 times

✉ **cegama543** 8 months, 3 weeks ago

Selected Answer: A

agree with that

upvoted 1 times

A company needs to ingest and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams, which is configured with default settings. Every other day, the application consumes the data and writes the data to an Amazon S3 bucket for business intelligence (BI) processing. The company observes that Amazon S3 is not receiving all the data that the application sends to Kinesis Data Streams.

What should a solutions architect do to resolve this issue?

- A. Update the Kinesis Data Streams default settings by modifying the data retention period.
- B. Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.
- C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.
- D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

Correct Answer: A

Community vote distribution

A (60%)	C (36%)	4%
---------	---------	----

 **WhericanIstart** Highly Voted 8 months, 2 weeks ago

Selected Answer: A

"A Kinesis data stream stores records from 24 hours by default, up to 8760 hours (365 days)."
<https://docs.aws.amazon.com/streams/latest/dev/kinesis-extended-retention.html>

The question mentioned Kinesis data stream default settings and "every other day". After 24hrs, the data isn't in the Data stream if the default settings is not modified to store data more than 24hrs.

upvoted 20 times

 **cegama543** Highly Voted 8 months, 3 weeks ago

Selected Answer: C

C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.

The best option is to update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams. Kinesis Data Streams scales horizontally by increasing or decreasing the number of shards, which controls the throughput capacity of the stream. By increasing the number of shards, the application will be able to send more data to Kinesis Data Streams, which can help ensure that S3 receives all the data.

upvoted 14 times

 **CapJackSparrow** 8 months, 2 weeks ago

lets say you had infinity shards... if the retention period is 24 hours and you get the data every 48 hours, you will lose 24 hours of data no matter the amount of shards no?

upvoted 10 times

 **enzomv** 8 months, 2 weeks ago

Amazon Kinesis Data Streams supports changes to the data record retention period of your data stream. A Kinesis data stream is an ordered sequence of data records meant to be written to and read from in real time. Data records are therefore stored in shards in your stream temporarily. The time period from when a record is added to when it is no longer accessible is called the retention period. A Kinesis data stream stores records from 24 hours by default, up to 8760 hours (365 days).

upvoted 4 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Answer C:

C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.

- Answer C updates the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams. By increasing the number of shards, the data is distributed across multiple shards, which allows for increased throughput and ensures that all data is ingested and processed by Kinesis Data Streams.

- Monitoring the Kinesis Data Streams and adjusting the number of shards as needed to handle changes in data throughput can ensure that the application can handle large amounts of streaming data.

upvoted 2 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

@cegama543, my apologies. Moderator if you can disapprove of the post above? I made a mistake. It is supposed to be intended on the post that I submitted.

Thanks.

upvoted 1 times

 **TariqKipkemei** Most Recent 1 month ago

Selected Answer: A

Data records are stored in shards in a kinesis data stream temporarily. The time period from when a record is added, to when it is no longer accessible is called the retention period. This time period is 24 hours by default, but could be adjusted to 365 days.

Kinesis Data Streams automatically scales the number of shards in response to changes in data volume and traffic, so this rules out option C.

<https://docs.aws.amazon.com/streams/latest/dev/service-sizes-and-limits.html#:~:text=the%20number%20of,-shards,-in%20response%20to>
upvoted 1 times

✉ **Ramdi1** 2 months ago

Selected Answer: A

I have only voted A because it mentions the default setting in Kinesis, if it did not mention that then I would look to increase the Shards. By default it is 24 hours and can go to 365 days. I think the question should be rephrased slightly. I had trouble deciding between A & C. Also apparently the most voted answer is the correct answer as per some advice I was given.

upvoted 2 times

✉ **BrijMohan08** 2 months, 3 weeks ago

Selected Answer: A

Default retention is 24 hrs, but the data read is every other day, so the S3 will never receive the data, Change the default retention period to 48 hours.

upvoted 1 times

✉ **Guru4Cloud** 3 months ago

Selected Answer: C

By default, a Kinesis data stream is created with one shard. If the data throughput to the stream is higher than the capacity of the single shard, the data stream may not be able to handle all the incoming data, and some data may be lost.

Therefore, to handle the high volume of data that the application sends to Kinesis Data Streams, the number of Kinesis shards should be increased to handle the required throughput.

Kinesis Data Streams shards are the basic units of scalability and availability. Each shard can process up to 1,000 records per second with a maximum of 1 MB of data per second. If the application is sending more data to Kinesis Data Streams than the shards can handle, then some of the data will be dropped.

upvoted 1 times

✉ **Guru4Cloud** 3 months ago

If you have doubts, Please read about Kinesis Data Streams shards.

Ans: A is not the correct answer here

upvoted 1 times

✉ **Amycert** 3 months, 2 weeks ago

Selected Answer: A

the default retention period is 24 hours "The default retention period of 24 hours covers scenarios where intermittent lags in processing require catch-up with the real-time data."

so we should increment this

upvoted 1 times

✉ **hsinchang** 4 months ago

Selected Answer: A

As "Default settings" is mentioned here, I vote for A.

upvoted 1 times

✉ **jaydesai8** 4 months, 3 weeks ago

Selected Answer: A

keyword here is - default settings and every other day and since "A Kinesis data stream stores records from 24 hours by default, up to 8760 hours (365 days)."

<https://docs.aws.amazon.com/streams/latest/dev/kinesis-extended-retention.html>

Will go with A

upvoted 1 times

✉ **jayce5** 5 months, 4 weeks ago

Selected Answer: A

C is wrong because even if you update the number of Kinesis shards, you still need to change the default data retention period first. Otherwise, you would lose data after 24 hours.

upvoted 2 times

✉ **antropaws** 6 months ago

Selected Answer: C

A is unrelated to the issue. The correct answer is C.

upvoted 1 times

✉ **omoakin** 6 months ago

Correct Ans. is B

upvoted 1 times

✉ **smd_** 6 months, 3 weeks ago

By default, a Kinesis data stream is created with one shard. If the data throughput to the stream is higher than the capacity of the single shard, the data stream may not be able to handle all the incoming data, and some data may be lost.

Therefore, to handle the high volume of data that the application sends to Kinesis Data Streams, the number of Kinesis shards should be increased to handle the required throughput

upvoted 2 times

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

both Option A and Option C could be valid solutions to resolving the issue of data loss, depending on the root cause of the problem. It would be best to analyze the root cause of the data loss issue to determine which solution is most appropriate for this specific scenario.

upvoted 1 times

✉️ **neosis91** 7 months, 1 week ago

Selected Answer: C

CCCCCC

upvoted 2 times

✉️ **kraken21** 8 months ago

Also: <https://www.examtopics.com/discussions/amazon/view/61067-exam-aws-certified-solutions-architect-associate-saa-c02/> for Option A.

upvoted 1 times

✉️ **kraken21** 8 months ago

Selected Answer: A

It comes down to is it a compute issue or a storage issue. Since the keywords of "Default", "every other day" were used and the issue is some data is missing, I am voting for Option A.

upvoted 5 times

A developer has an application that uses an AWS Lambda function to upload files to Amazon S3 and needs the required permissions to perform the task. The developer already has an IAM user with valid IAM credentials required for Amazon S3.

What should a solutions architect do to grant the permissions?

- A. Add required IAM permissions in the resource policy of the Lambda function.
- B. Create a signed request using the existing IAM credentials in the Lambda function.
- C. Create a new IAM user and use the existing IAM credentials in the Lambda function.
- D. Create an IAM execution role with the required permissions and attach the IAM role to the Lambda function.

Correct Answer: A

Community vote distribution

D (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: D

Create Lambda execution role and attach existing S3 IAM role to the lambda function
upvoted 1 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

To grant the necessary permissions to an AWS Lambda function to upload files to Amazon S3, a solutions architect should create an IAM execution role with the required permissions and attach the IAM role to the Lambda function. This approach follows the principle of least privilege and ensures that the Lambda function can only access the resources it needs to perform its specific task.

Therefore, the correct answer is D. Create an IAM execution role with the required permissions and attach the IAM role to the Lambda function.
upvoted 1 times

 **BilalIlg93350** 8 months, 1 week ago

D. Créez un rôle d'exécution IAM avec les autorisations requises et attachez le rôle IAM à la fonction Lambda.

L'architecte de solutions doit créer un rôle d'exécution IAM ayant les autorisations nécessaires pour accéder à Amazon S3 et effectuer les opérations requises (par exemple, charger des fichiers). Ensuite, le rôle doit être associé à la fonction Lambda, de sorte que la fonction puisse assumer ce rôle et avoir les autorisations nécessaires pour interagir avec Amazon S3.

upvoted 2 times

 **nileshlg** 8 months, 2 weeks ago

Selected Answer: D

Answer is D

upvoted 1 times

 **kampatra** 8 months, 2 weeks ago

Selected Answer: D

D - correct ans

upvoted 1 times

 **sitha** 8 months, 3 weeks ago

Selected Answer: D

Create Lambda execution role and attach existing S3 IAM role to the lambda function

upvoted 1 times

 **ktulu2602** 8 months, 3 weeks ago

Selected Answer: D

Definitely D

upvoted 1 times

 **Nithin1119** 8 months, 3 weeks ago

Selected Answer: D

ddddddd

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: D

ddddddd

upvoted 1 times

A company has deployed a serverless application that invokes an AWS Lambda function when new documents are uploaded to an Amazon S3 bucket. The application uses the Lambda function to process the documents. After a recent marketing campaign, the company noticed that the application did not process many of the documents.

What should a solutions architect do to improve the architecture of this application?

- A. Set the Lambda function's runtime timeout value to 15 minutes.
- B. Configure an S3 bucket replication policy. Stage the documents in the S3 bucket for later processing.
- C. Deploy an additional Lambda function. Load balance the processing of the documents across the two Lambda functions.
- D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda.

Correct Answer: D

Community vote distribution

D (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: D

D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: D

D is the best approach

upvoted 1 times

 **Russ99** 8 months, 1 week ago

Selected Answer: D

D is the correct answer

upvoted 1 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Selected Answer: D

To improve the architecture of this application, the best solution would be to use Amazon Simple Queue Service (Amazon SQS) to buffer the requests and decouple the S3 bucket from the Lambda function. This will ensure that the documents are not lost and can be processed at a later time if the Lambda function is not available.

This will ensure that the documents are not lost and can be processed at a later time if the Lambda function is not available. By using Amazon SQS, the architecture is decoupled and the Lambda function can process the documents in a scalable and fault-tolerant manner.

upvoted 1 times

 **BilalIlg93350** 8 months, 1 week ago

D. Créez une file d'attente Amazon Simple Queue Service (Amazon SQS). Envoyez les demandes à la file d'attente. Configurez la file d'attente en tant que source d'événement pour Lambda.

Cette solution permet de gérer efficacement les pics de charge et d'éviter la perte de documents en cas d'augmentation soudaine du trafic. Lorsque de nouveaux documents sont chargés dans le compartiment Amazon S3, les demandes sont envoyées à la file d'attente Amazon SQS, qui agit comme un tampon. La fonction Lambda est déclenchée en fonction des événements dans la file d'attente, ce qui permet un traitement équilibré et évite que l'application ne soit submergée par un grand nombre de documents simultanés.

upvoted 1 times

 **Russ99** 8 months, 1 week ago

exactement. si je pouvais expliquer come cela en Francais aussi

upvoted 1 times

 **Whericanstart** 8 months, 2 weeks ago

Selected Answer: D

D is the correct answer.

upvoted 1 times

 **kampatra** 8 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **dcp** 8 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: D

ddddddd

upvoted 2 times

A solutions architect is designing the architecture for a software demonstration environment. The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The system will experience significant increases in traffic during working hours but is not required to operate on weekends.

Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Choose two.)

- A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate.
- B. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway.
- C. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions.
- D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.
- E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

Correct Answer: D E

Community vote distribution

DE (56%) AD (22%) AE (18%) 4%

 **channn** Highly Voted 8 months ago

Selected Answer: AD

A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate: This will allow the system to scale up or down based on incoming traffic demand. The solutions architect should use AWS Auto Scaling to monitor the request rate and adjust the ALB capacity as needed.

D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization: This will allow the system to scale up or down based on the CPU utilization of the EC2 instances in the Auto Scaling group. The solutions architect should use a target tracking scaling policy to maintain a specific CPU utilization target and adjust the number of EC2 instances in the Auto Scaling group accordingly.

upvoted 8 times

 **cd93** Highly Voted 3 months, 1 week ago

What does "ALB capacity" even mean anyway? It should be "Target Group capacity" no?

Answer should be DE, as D is a more comprehensive answer (and more practical in real life)

upvoted 7 times

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

AD

E - the question doesn't ask about cost. Also, shutting it down during the weekend does nothing to improve scaling during the week. It doesn't address the requirements.

upvoted 2 times

 **Guru4Cloud** 3 months ago

Selected Answer: DE

The solutions architect should take actions D and E:

D) Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization. This will allow the Auto Scaling group to dynamically scale in and out based on demand.

E) Use scheduled scaling to change the Auto Scaling group capacity to zero on weekends when traffic is expected to be low. This will minimize costs by terminating unused instances.

upvoted 4 times

 **fuzzycr** 4 months, 2 weeks ago

Selected Answer: AE

Basado en los requerimientos la opción que se requiere para optimizar los costos de operaciones en los fines de semana

upvoted 1 times

 **jaydesai8** 4 months, 3 weeks ago

Selected Answer: DE

DE - This seems more close for the auto scaling -

A - Its says auto scaling on ALB, but it should always be on EC2 instances and not ELB

upvoted 5 times

 **XaviL** 5 months, 1 week ago

Hi guys, very simple

* A. because the question are asking about request rate!!!! This is a requirement!

* E. The weekend is not necessary to execute anything!

A&D. Is not possible, way you can put an ALB capacity based in cpu and in request rate???? You need to select one or another option (and this is for all questions here guys!)

upvoted 2 times

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

Selected Answer: AE

ALBRequestCountPerTarget—Average Application Load Balancer request count per target.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html#target-tracking-choose-metrics>

It is possible to set to zero. "is not required to operate on weekends" means the instances are not required during the weekends.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-capacity-limits.html>

upvoted 2 times

✉ **Uzi_m** 5 months, 3 weeks ago

Option E is incorrect because the question specifically mentions an increase in traffic during working hours. Therefore, it is not advisable to schedule the instances for 24 hours using default settings throughout the entire week.

E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

upvoted 1 times

✉ **omoakin** 6 months ago

AD are the correct ansns

upvoted 3 times

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

Selected Answer: ADE

Either one or two or all of these combinations will meet the need:

Use AWS Auto Scaling to adjust the ALB capacity based on request rate.

Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.

Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

upvoted 2 times

✉ **TariqKipkemei** 1 month ago

Scheduled scaling was specifically designed to handle these kind of requirements.

I therefore take out target scaling.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html#:~:text=RSS-,Scheduled%20scaling,-helps%20you%20to>

upvoted 1 times

✉ **Joe94KR** 7 months, 1 week ago

Selected Answer: DE

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html#target-tracking-choose-metrics>

Based on docs, ASG can't track ALB's request rate, so the answer is D&E

meanwhile ASG can track CPU rates.

upvoted 4 times

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

The link shows:

ALBRequestCountPerTarget—Average Application Load Balancer request count per target.

upvoted 2 times

✉ **kraken21** 8 months ago

Selected Answer: DE

Scaling should be at the ASG not ALB. So, not sure about "Use AWS Auto Scaling to adjust the ALB capacity based on request rate"

upvoted 4 times

✉ **neosis91** 8 months ago

Selected Answer: AD

A. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization. This approach allows the Auto Scaling group to automatically adjust the number of instances based on the specified metric, ensuring that the system can scale to meet demand during working hours.

D. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week. This approach allows the Auto Scaling group to reduce the number of instances to zero during weekends when traffic is expected to be low. It will help the organization to save costs by not paying for instances that are not needed during weekends.

Therefore, options A and D are the correct answers. Options B and C are not relevant to the scenario, and option E is not a scalable solution as it would require manual intervention to adjust the group capacity every week.

upvoted 1 times

✉ **zooba72** 8 months ago

Selected Answer: DE

This is why I don't believe A is correct use auto scaling to adjust the ALB D&E
upvoted 3 times

 **Russ99** 8 months, 1 week ago

Selected Answer: AD

AD

D there is no requirement for cost minimization in the scenario therefore, A & D are the answers
upvoted 3 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Selected Answer: DE

A comparison of Answers D and E VERSUS another possible answer Answers A and E:

Answers D and E:

D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.

E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

- Answer D scales the Auto Scaling group based on instance CPU utilization, which ensures that the number of instances in the group can be adjusted to handle the increase in traffic during working hours and reduce capacity during periods of low traffic.

- Answer E uses scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends, which ensures that the Auto Scaling group scales down to zero during weekends to save costs.

upvoted 1 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Answers A and E:

A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate.

E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

- Answer A adjusts the capacity of the ALB based on request rate, which ensures that the ALB can handle the increase in traffic during working hours and reduce capacity during periods of low traffic.

- Answer E uses scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends, which ensures that the Auto Scaling group scales down to zero during weekends to save costs.

upvoted 1 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Comparing the two options, both Answers D and A are valid choices for scaling the application based on demand. However, Answer D scales the Auto Scaling group based on instance CPU utilization, which is a more granular metric than request rate and can provide better performance and cost optimization. Answer A only scales the ALB based on the request rate, which may not be sufficient for handling sudden spikes in traffic.

Answer E is a common choice for scaling down to zero during weekends to save costs. Both Answers D and A can be used in conjunction with Answer E to ensure that the Auto Scaling group scales down to zero during weekends. However, Answer D provides more granular control over the scaling of the Auto Scaling group based on instance CPU utilization, which can result in better performance and cost optimization.

upvoted 2 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

In conclusion, answers D and E provide a more granular and flexible solution for scaling the application based on demand and scaling down to zero during weekends, while Answers A and E may not be as granular and may not provide as much performance and cost optimization.

upvoted 3 times

A solutions architect is designing a two-tiered architecture that includes a public subnet and a database subnet. The web servers in the public subnet must be open to the internet on port 443. The Amazon RDS for MySQL DB instance in the database subnet must be accessible only to the web servers on port 3306.

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

- A. Create a network ACL for the public subnet. Add a rule to deny outbound traffic to 0.0.0.0/0 on port 3306.
- B. Create a security group for the DB instance. Add a rule to allow traffic from the public subnet CIDR block on port 3306.
- C. Create a security group for the web servers in the public subnet. Add a rule to allow traffic from 0.0.0.0/0 on port 443.
- D. Create a security group for the DB instance. Add a rule to allow traffic from the web servers' security group on port 3306.
- E. Create a security group for the DB instance. Add a rule to deny all traffic except traffic from the web servers' security group on port 3306.

Correct Answer: CD

Community vote distribution

CD (100%)

✉  **TariqKipkemei** 1 month ago

Selected Answer: CD

'must be accessible only to the web servers' is the key here.
Option B almost threw me off, but with this then all that exists in the public subnet would be able to access the DB security group.
Therefore C,D well applies the principle of least privilege.

upvoted 1 times

✉  **Guru4Cloud** 3 months ago

Selected Answer: CD

Remember guys that SG is not used for Deny action, just Allow

upvoted 2 times

✉  **datmd77** 6 months, 4 weeks ago

Selected Answer: CD

Remember guys that SG is not used for Deny action, just Allow

upvoted 1 times

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

Selected Answer: CD

To meet the requirements of allowing access to the web servers in the public subnet on port 443 and the Amazon RDS for MySQL DB instance in the database subnet on port 3306, the best solution would be to create a security group for the web servers and another security group for the DB instance, and then define the appropriate inbound and outbound rules for each security group.

1. Create a security group for the web servers in the public subnet. Add a rule to allow traffic from 0.0.0.0/0 on port 443.
2. Create a security group for the DB instance. Add a rule to allow traffic from the web servers' security group on port 3306.

This will allow the web servers in the public subnet to receive traffic from the internet on port 443, and the Amazon RDS for MySQL DB instance in the database subnet to receive traffic only from the web servers on port 3306.

upvoted 1 times

✉  **kampatra** 8 months, 2 weeks ago

Selected Answer: CD

CD - Correct ans.

upvoted 2 times

✉  **Eden** 8 months, 2 weeks ago

I choose CE

upvoted 1 times

✉  **lili_9** 8 months, 3 weeks ago

CE support @sitha

upvoted 1 times

✉  **sitha** 8 months, 3 weeks ago

Answer: CE . The solution is to deny accessing DB from Internet and allow only access from webserver.

upvoted 1 times

 **KAUS2** 8 months, 3 weeks ago

Selected Answer: CD

C & D are the right choices. correct

upvoted 1 times

 **KS2020** 8 months, 3 weeks ago

why not CE?

upvoted 2 times

 **kampatra** 8 months, 2 weeks ago

By default Security Group deny all traffic and we need to configure to enable.

upvoted 2 times

 **dcp** 8 months, 3 weeks ago

Characteristics of security group rules

You can specify allow rules, but not deny rules.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: CD

cdcdcdcdcdc

upvoted 2 times

A company is implementing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use Lustre clients to access data. The solution must be fully managed.

Which solution meets these requirements?

- A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
- B. Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- C. Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: C

Community vote distribution

D (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: D

Lustre clients = Amazon FSx for Lustre file system
upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: D

Lustre clients = Amazon FSx for Lustre file system
upvoted 1 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Selected Answer: D

To meet the requirements of a shared storage solution for a gaming application that can be accessed using Lustre clients and is fully managed, the best solution would be to use Amazon FSx for Lustre.

Amazon FSx for Lustre is a fully managed file system that is optimized for compute-intensive workloads, such as high-performance computing, machine learning, and gaming. It provides a POSIX-compliant file system that can be accessed using Lustre clients and offers high performance, scalability, and data durability.

This solution provides a highly available, scalable, and fully managed shared storage solution that can be accessed using Lustre clients. Amazon FSx for Lustre is optimized for compute-intensive workloads and provides high performance and durability.

upvoted 3 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Answer A, creating an AWS DataSync task that shares the data as a mountable file system and mounting the file system to the application server, may not provide the required performance and scalability for a gaming application.

Answer B, creating an AWS Storage Gateway file gateway and connecting the application server to the file share, may not provide the required performance and scalability for a gaming application.

Answer C, creating an Amazon Elastic File System (Amazon EFS) file system and configuring it to support Lustre, may not provide the required performance and scalability for a gaming application and may require additional configuration and management overhead.

upvoted 1 times

 **kampatra** 8 months, 2 weeks ago

Selected Answer: D

D - correct ans
upvoted 2 times

 **kprakashbehera** 8 months, 3 weeks ago

Selected Answer: D

FSx for Lustre
DDDDDD
upvoted 1 times

 **KAUS2** 8 months, 3 weeks ago

Selected Answer: D

Amazon FSx for Lustre is the right answer

- Lustre is a type of parallel distributed file system, for large-scale computing, Machine Learning, High Performance Computing (HPC)
- Video Processing, Financial Modeling, Electronic Design Automation

upvoted 1 times

 **cegama543** 8 months, 3 weeks ago

Selected Answer: D

Option D is the best solution because Amazon FSx for Lustre is a fully managed, high-performance file system that is designed to support compute-intensive workloads, such as those required by gaming applications. FSx for Lustre provides sub-millisecond access to petabyte-scale file systems, and supports Lustre clients natively. This means that the gaming application can access the shared data directly from the FSx for Lustre file system without the need for additional configuration or setup.

Additionally, FSx for Lustre is a fully managed service, meaning that AWS takes care of all maintenance, updates, and patches for the file system, which reduces the operational overhead required by the company.

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: D

ddddddddd

upvoted 1 times

A company runs an application that receives data from thousands of geographically dispersed remote devices that use UDP. The application processes the data immediately and sends a message back to the device if necessary. No data is stored.

The company needs a solution that minimizes latency for the data transmission from the devices. The solution also must provide rapid failover to another AWS Region.

Which solution will meet these requirements?

- A. Configure an Amazon Route 53 failover routing policy. Create a Network Load Balancer (NLB) in each of the two Regions. Configure the NLB to invoke an AWS Lambda function to process the data.
- B. Use AWS Global Accelerator. Create a Network Load Balancer (NLB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the NLB. Process the data in Amazon ECS.
- C. Use AWS Global Accelerator. Create an Application Load Balancer (ALB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB. Process the data in Amazon ECS.
- D. Configure an Amazon Route 53 failover routing policy. Create an Application Load Balancer (ALB) in each of the two Regions. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB. Process the data in Amazon ECS.

Correct Answer: B

Community vote distribution

B (100%)

 **UnluckyDucky** Highly Voted  8 months, 2 weeks ago

Selected Answer: B

Key words: geographically dispersed, UDP.

Geographically dispersed (related to UDP) - Global Accelerator - multiple entrances worldwide to the AWS network to provide better transfer rates.
UDP - NLB (Network Load Balancer).

upvoted 8 times

 **Guru4Cloud** Most Recent  3 months ago

Selected Answer: B

This option meets the requirements:

Global Accelerator provides UDP support and minimizes latency using the AWS global network.
Using NLBs allows the UDP traffic to be load balanced across Availability Zones.

ECS Fargate provides rapid scaling and failover across Regions.
NLB endpoints allow rapid failover if one Region goes down.

upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: B

UDP = AWS Global Accelerator and Network Load Balancer

upvoted 1 times

 **kraken21** 8 months ago

Selected Answer: B

Global accelerator for multi region automatic failover. NLB for UDP.

upvoted 2 times

 **MaxMa** 8 months ago

why not A?

upvoted 1 times

 **kraken21** 8 months ago

NLBs do not support lambda target type. Tricky!!! <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html>

upvoted 6 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Selected Answer: B

To meet the requirements of minimizing latency for data transmission from the devices and providing rapid failover to another AWS Region, the best solution would be to use AWS Global Accelerator in combination with a Network Load Balancer (NLB) and Amazon Elastic Container Service (Amazon ECS).

AWS Global Accelerator is a service that improves the availability and performance of applications by using static IP addresses (Anycast) to route traffic to optimal AWS endpoints. With Global Accelerator, you can direct traffic to multiple Regions and endpoints, and provide automatic failover to another AWS Region.

upvoted 3 times

 **Ruh102** 8 months, 3 weeks ago

Answer should be B.. there is typo mistake in B. Correct Answer is : Use AWS Global Accelerator. Create a Network Load Balancer (NLB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the NLB. Process the data in Amazon ECS.

upvoted 4 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: B

bbbbbbbb

upvoted 1 times

A solutions architect must migrate a Windows Internet Information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS). The solutions architect has proposed migrating the IIS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances.

Which replacement to the on-premises file share is MOST resilient and durable?

- A. Migrate the file share to Amazon RDS.
- B. Migrate the file share to AWS Storage Gateway.
- C. Migrate the file share to Amazon FSx for Windows File Server.
- D. Migrate the file share to Amazon Elastic File System (Amazon EFS).

Correct Answer: A

Community vote distribution

C (94%) 6%

✉️  **channn**  8 months ago

Selected Answer: C

- A) RDS is a database service
- B) Storage Gateway is a hybrid cloud storage service that connects on-premises applications to AWS storage services.
- C) provides shared file storage for Linux-based workloads, but it does not natively support Windows-based workloads.
upvoted 5 times

✉️  **Guru4Cloud**  3 months ago

Selected Answer: C

Windows client = Amazon FSx for Windows File Server
upvoted 1 times

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

Selected Answer: C

Windows client = Amazon FSx for Windows File Server
upvoted 1 times

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

Selected Answer: C

The most resilient and durable replacement for the on-premises file share in this scenario would be Amazon FSx for Windows File Server.

Amazon FSx is a fully managed Windows file system service that is built on Windows Server and provides native support for the SMB protocol. It is designed to be highly available and durable, with built-in backup and restore capabilities. It is also fully integrated with AWS security services, providing encryption at rest and in transit, and it can be configured to meet compliance standards.

upvoted 3 times

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

Migrating the file share to Amazon RDS or AWS Storage Gateway is not appropriate as these services are designed for database workloads and block storage respectively, and do not provide native support for the SMB protocol.

Migrating the file share to Amazon EFS (Linux ONLY) could be an option, but Amazon FSx for Windows File Server would be more appropriate in this case because it is specifically designed for Windows file shares and provides better performance for Windows applications.

upvoted 3 times

✉️  **Grace83** 8 months, 1 week ago

Obviously C is the correct answer - FSx for Windows - Windows
upvoted 4 times

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

Selected Answer: C

FSx for Windows - Windows.
EFS - Linux.
upvoted 2 times

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

Selected Answer: D

Amazon EFS is a scalable and fully-managed file storage service that is designed to provide high availability and durability. It can be accessed by multiple EC2 instances across multiple Availability Zones simultaneously. Additionally, it offers automatic and instantaneous data replication across different availability zones within a region, which makes it resilient to failures.

upvoted 1 times

 **asoli** 8 months, 2 weeks ago

EFS is a wrong choice because it can only work with Linux instances. That application has a Windows web server , so its OS is Windows and EFS cannot connect to it

upvoted 2 times

 **dcp** 8 months, 3 weeks ago

Selected Answer: C

Amazon FSx

upvoted 1 times

 **sitha** 8 months, 3 weeks ago

Amazon FSx makes it easy and cost effective to launch, run, and scale feature-rich, high-performance file systems in the cloud.

Answer : C

upvoted 1 times

 **KAUS2** 8 months, 3 weeks ago

Selected Answer: C

FSx for Windows is a fully managed Windows file system share drive . Hence C is the correct answer.

upvoted 1 times

 **Ruhi02** 8 months, 3 weeks ago

FSx for Windows is ideal in this case. So answer is C.

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: C

cccccccccc

upvoted 1 times

A company is deploying a new application on Amazon EC2 instances. The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes. The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest.

Which solution will meet this requirement?

- A. Create an IAM role that specifies EBS encryption. Attach the role to the EC2 instances.
- B. Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2 instances.
- C. Create an EC2 instance tag that has a key of Encrypt and a value of True. Tag all instances that require encryption at the EBS level.
- D. Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account. Ensure that the key policy is active.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

The solution that will meet the requirement of ensuring that all data that is written to the EBS volumes is encrypted at rest is B. Create the EBS volumes as encrypted volumes and attach the encrypted EBS volumes to the EC2 instances.

When you create an EBS volume, you can specify whether to encrypt the volume. If you choose to encrypt the volume, all data written to the volume is automatically encrypted at rest using AWS-managed keys. You can also use customer-managed keys (CMKs) stored in AWS KMS to encrypt and protect your EBS volumes. You can create encrypted EBS volumes and attach them to EC2 instances to ensure that all data written to the volumes is encrypted at rest.

Answer A is incorrect because attaching an IAM role to the EC2 instances does not automatically encrypt the EBS volumes.

Answer C is incorrect because adding an EC2 instance tag does not ensure that the EBS volumes are encrypted.
upvoted 6 times

 **Kds53829** Most Recent  1 month ago

B is the answer
upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: B

B. Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2 instances.
upvoted 1 times

 **TariqKipkemei** 6 months, 1 week ago

Selected Answer: B

Windows client = Amazon FSx for Windows File Server
upvoted 2 times

 **TariqKipkemei** 1 month ago

ignore this, mind stuck on last question hhhhhh.
Just create the EBS volumes as encrypted volumes then attach the EBS volumes to the EC2 instances.
upvoted 1 times

 **elearningtakai** 8 months ago

Selected Answer: B

The other options either do not meet the requirement of encrypting data at rest (A and C) or do so in a more complex or less efficient manner (D).
upvoted 1 times

 **Bofi** 8 months, 1 week ago

Why not D, EBS encryption require the use of KMS key
upvoted 1 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Answer D is incorrect because creating a KMS key policy that enforces EBS encryption does not automatically encrypt EBS volumes. You need to create encrypted EBS volumes and attach them to EC2 instances to ensure that all data written to the volumes are encrypted at rest.
upvoted 3 times

 **WhericanIstart** 8 months, 2 weeks ago

Selected Answer: B

Create encrypted EBS volumes and attach encrypted EBS volumes to EC2 instances..

upvoted 2 times

 **sitha** 8 months, 3 weeks ago

Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances. Select KMS Keys either default or custom

upvoted 1 times

 **Ruhi02** 8 months, 3 weeks ago

Answer B. You can enable encryption for EBS volumes while creating them.

upvoted 1 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: B

bbbbbbbb

upvoted 1 times

A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications.

Which solution will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon RDS for MySQL
- C. MySQL-compatible Amazon Aurora Serverless
- D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Correct Answer: C

Community vote distribution

C (85%) B (15%)

 **TariqKipkemei** 1 month ago

Selected Answer: C

The is a huge demand for auto-scaling which Amazon RDS cannot do. This contributes to the cost savings as Aurora serverless would scale done in low peak times, this contributes to low costs.

upvoted 1 times

 **JKevin778** 2 months ago

Selected Answer: B

RDS is cheaper than Aurora.

upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: C

Answer C, MySQL-compatible Amazon Aurora Serverless, would be the best solution to meet the company's requirements.

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: C

Since we have sporadic & unpredictable usage for DB, Aurora Serverless would be fit more cost-efficient for this case scenario than RDS MySQL.
<https://www.techtarget.com/searchcloudcomputing/answer/When-should-I-use-Amazon-RDS-vs-Aurora-Serverless>

upvoted 1 times

 **antropaws** 6 months ago

Selected Answer: C

C for sure.

upvoted 2 times

 **channn** 8 months ago

Selected Answer: C

C: Aurora Serverless is a MySQL-compatible relational database engine that automatically scales compute and memory resources based on application usage. no upfront costs or commitments required.

A: DynamoDB is a NoSQL

B: Fixed cost on RDS class

D: More operation requires

upvoted 4 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Selected Answer: C

Answer C, MySQL-compatible Amazon Aurora Serverless, would be the best solution to meet the company's requirements.

Aurora Serverless can be a cost-effective option for databases with sporadic or unpredictable usage patterns since it automatically scales up or down based on the current workload. Additionally, Aurora Serverless is compatible with MySQL, so it does not require any modifications to the application's database code.

upvoted 3 times

 **klayytech** 8 months, 1 week ago

Selected Answer: B

Amazon RDS for MySQL is a cost-effective database platform that will not require database modifications. It makes it easier to set up, operate, and scale MySQL deployments in the cloud. With Amazon RDS, you can deploy scalable MySQL servers in minutes with cost-efficient and resizable hardware capacity².

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB is a good choice for applications that require low-latency data access¹.

MySQL-compatible Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora (MySQL-compatible edition), where the database will automatically start up, shut down, and scale capacity up or down based on your application's needs³.

So, Amazon RDS for MySQL is the best option for your requirements.

upvoted 2 times

✉  **klaytech** 8 months ago

sorry i will change to C , because

Amazon RDS for MySQL is a fully-managed relational database service that makes it easy to set up, operate, and scale MySQL deployments in the cloud. Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora (MySQL-compatible edition), where the database will automatically start up, shut down, and scale capacity up or down based on your application's needs. It is a simple, cost-effective option for infrequent, intermittent, or unpredictable workloads.

upvoted 2 times

✉  **boxu03** 8 months, 2 weeks ago

Selected Answer: C

Amazon Aurora Serverless : a simple, cost-effective option for infrequent, intermittent, or unpredictable workloads

upvoted 3 times

✉  **taehyeki** 8 months, 3 weeks ago

Selected Answer: C

cccccccccccccccccccc

upvoted 2 times

An image-hosting company stores its objects in Amazon S3 buckets. The company wants to avoid accidental exposure of the objects in the S3 buckets to the public. All S3 objects in the entire AWS account need to remain private.

Which solution will meet these requirements?

- A. Use Amazon GuardDuty to monitor S3 bucket policies. Create an automatic remediation action rule that uses an AWS Lambda function to remediate any change that makes the objects public.
- B. Use AWS Trusted Advisor to find publicly accessible S3 buckets. Configure email notifications in Trusted Advisor when a change is detected. Manually change the S3 bucket policy if it allows public access.
- C. Use AWS Resource Access Manager to find publicly accessible S3 buckets. Use Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function when a change is detected. Deploy a Lambda function that programmatically remediates the change.
- D. Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting. Apply the SCP to the account.

Correct Answer: D

Community vote distribution

D (93%) 7%

 **Ruhi02** Highly Voted 8 months, 3 weeks ago

Answer is D ladies and gentlemen. While guard duty helps to monitor s3 for potential threats its a reactive action. We should always be proactive and not reactive in our solutions so D, block public access to avoid any possibility of the info becoming publicly accessible
upvoted 11 times

 **TariqKipkemei** Most Recent 1 month ago

Selected Answer: D

Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting. Apply the SCP to the account
upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: D

Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting. Apply the SCP to the account
upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: A

A is correct!
upvoted 1 times

 **Yadav_Sanjay** 6 months, 1 week ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html>
upvoted 2 times

 **elearningtakai** 8 months ago

Selected Answer: D

This is the most effective solution to meet the requirements.
upvoted 2 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Selected Answer: D

Answer D is the correct solution that meets the requirements. The S3 Block Public Access feature allows you to restrict public access to S3 buckets and objects within the account. You can enable this feature at the account level to prevent any S3 bucket from being made public, regardless of the bucket policy settings. AWS Organizations can be used to apply a Service Control Policy (SCP) to the account to prevent IAM users from changing this setting, ensuring that all S3 objects remain private. This is a straightforward and effective solution that requires minimal operational overhead.
upvoted 4 times

 **Bofi** 8 months, 1 week ago

Selected Answer: D

Option D provided real solution by using bucket policy to restrict public access. Other options were focus on detection which wasn't what was been asked

upvoted 2 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: D

ddddddddd

upvoted 1 times

An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier web application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.

What should a solutions architect do to meet these requirements?

- A. Create a separate application tier using EC2 instances dedicated to email processing.
- B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).
- C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).
- D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Correct Answer: B

Community vote distribution

B (100%)

 **elearningtakai**  8 months ago

Selected Answer: B

Amazon SES is a cost-effective and scalable email service that enables businesses to send and receive email using their own email addresses and domains. Configuring the web instance to send email through Amazon SES is a simple and effective solution that can reduce the time spent resolving complex email delivery issues and minimize operational overhead.

upvoted 5 times

 **TariqKipkemei**  1 month ago

Selected Answer: B

Amazon Simple Email Service (Amazon SES) lets you reach customers confidently without an on-premises Simple Mail Transfer Protocol (SMTP) email server using the Amazon SES API or SMTP interface.

upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: B

B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES)

upvoted 1 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Selected Answer: B

The best option for addressing the company's needs of minimizing operational overhead and reducing time spent resolving email delivery issues is to use Amazon Simple Email Service (Amazon SES).

Answer A of creating a separate application tier for email processing may add additional complexity to the architecture and require more operational overhead.

Answer C of using Amazon Simple Notification Service (Amazon SNS) is not an appropriate solution for sending marketing and order confirmation emails since Amazon SNS is a messaging service that is designed to send messages to subscribed endpoints or clients.

Answer D of creating a separate application tier using EC2 instances dedicated to email processing placed in an Auto Scaling group is a more complex solution than necessary and may result in additional operational overhead.

upvoted 2 times

 **nileshlg** 8 months, 2 weeks ago

Answer is B

upvoted 2 times

 **Ruhi02** 8 months, 3 weeks ago

Answer B.. SES is meant for sending high volume e-mail efficiently and securely.

SNS is meant as a channel publisher/subscriber service

upvoted 4 times

 **taehyeki** 8 months, 3 weeks ago

Selected Answer: B

bbbbbbbb

upvoted 2 times

A company has a business system that generates hundreds of reports each day. The business system saves the reports to a network share in CSV format. The company needs to store this data in the AWS Cloud in near-real time for analysis.

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

- A. Use AWS DataSync to transfer the files to Amazon S3. Create a scheduled task that runs at the end of each day.
- B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.
- C. Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.
- D. Deploy an AWS Transfer for SFTP endpoint. Create a script that checks for new files on the network share and uploads the new files by using SFTP.

Correct Answer: C

Community vote distribution

B (82%) C (18%)

 **TariqKipkemei** 1 month ago

Selected Answer: B

Both Amazon S3 File Gateway and AWS DataSync are suitable for this scenario.
But there is a requirement for 'LEAST administrative overhead'.
Option C involves the creation of an entirely new application to consume the DataSync API, this rules out this option.
upvoted 3 times

 **Guru4Cloud** 3 months ago

Selected Answer: C

This option has the least administrative overhead because:

Using DataSync avoids having to rewrite the business system to use a new file gateway or SFTP endpoint.
Calling the DataSync API from an application allows automating the data transfer instead of running scheduled tasks or scripts.
DataSync directly transfers files from the network share to S3 without needing an intermediate server
upvoted 1 times

 **antropaws** 6 months ago

Selected Answer: B

B. Data Sync is better for one time migrations.
upvoted 2 times

 **kruasan** 7 months ago

Selected Answer: B

The correct solution here is:

B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.

This option requires the least administrative overhead because:

- It presents a simple network file share interface that the business system can write to, just like a standard network share. This requires minimal changes to the business system.
- The S3 File Gateway automatically uploads all files written to the share to an S3 bucket in the background. This handles the transfer and upload to S3 without requiring any scheduled tasks, scripts or automation.
- All ongoing management like monitoring, scaling, patching etc. is handled by AWS for the S3 File Gateway.
upvoted 2 times

 **kruasan** 7 months ago

The other options would require more ongoing administrative effort:

- A) AWS DataSync would require creating and managing scheduled tasks and monitoring them.
- C) Using the DataSync API would require developing an application and then managing and monitoring it.
- D) The SFTP option would require creating scripts, managing SFTP access and keys, and monitoring the file transfer process.

So overall, the S3 File Gateway requires the least amount of ongoing management and administration as it presents a simple file share interface but handles the upload to S3 in a fully managed fashion. The business system can continue writing to a network share as is, while the files are transparently uploaded to S3.

The S3 File Gateway is the most hands-off, low-maintenance solution in this scenario.

upvoted 2 times

✉ **channn** 8 months ago

Selected Answer: B

Key words:

1. near-real-time (A is out)
2. LEAST administrative (C n D is out)

upvoted 4 times

✉ **elearningtakai** 8 months ago

Selected Answer: B

A - creating a scheduled task is not near-real time.

B - The S3 File Gateway caches frequently accessed data locally and automatically uploads it to Amazon S3, providing near-real-time access to the data.

C - creating an application that uses the DataSync API in the automation workflow may provide near-real-time data access, but it requires additional development effort.

D - it requires additional development effort.

upvoted 3 times

✉ **zooba72** 8 months ago

Selected Answer: B

It's B. DataSync has a scheduler and it runs on hour intervals, it cannot be used real-time

upvoted 1 times

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

Selected Answer: C

The correct answer is C. Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.

To store the CSV reports generated by the business system in the AWS Cloud in near-real time for analysis, the best solution with the least administrative overhead would be to use AWS DataSync to transfer the files to Amazon S3 and create an application that uses the DataSync API in the automation workflow.

AWS DataSync is a fully managed service that makes it easy to automate and accelerate data transfer between on-premises storage systems and AWS Cloud storage, such as Amazon S3. With DataSync, you can quickly and securely transfer large amounts of data to the AWS Cloud, and you can automate the transfer process using the DataSync API.

upvoted 3 times

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

Answer A, using AWS DataSync to transfer the files to Amazon S3 and creating a scheduled task that runs at the end of each day, is not the best solution because it does not meet the requirement of storing the CSV reports in near-real time for analysis.

Answer B, creating an Amazon S3 File Gateway and updating the business system to use a new network share from the S3 File Gateway, is not the best solution because it requires additional configuration and management overhead.

Answer D, deploying an AWS Transfer for the SFTP endpoint and creating a script to check for new files on the network share and upload the new files using SFTP, is not the best solution because it requires additional scripting and management overhead

upvoted 1 times

✉ **COTIT** 8 months, 1 week ago

Selected Answer: B

I think B is the better answer, "LEAST administrative overhead"

https://aws.amazon.com/storagegateway/file/?nc1=h_ls

upvoted 3 times

✉ **andyto** 8 months, 1 week ago

B - S3 File Gateway.

C - this is wrong answer because data migration is scheduled (this is not continuous task), so condition "near-real time" is not fulfilled

upvoted 1 times

✉ **Thief** 8 months, 1 week ago

C is the best ans

upvoted 1 times

✉ **lizard812** 8 months, 1 week ago

Why not A? There is no scheduled job?

upvoted 1 times

A company is storing petabytes of data in Amazon S3 Standard. The data is stored in multiple S3 buckets and is accessed with varying frequency. The company does not know access patterns for all the data. The company needs to implement a solution for each S3 bucket to optimize the cost of S3 usage.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.
- B. Use the S3 storage class analysis tool to determine the correct tier for each object in the S3 bucket. Move each object to the identified storage tier.
- C. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Glacier Instant Retrieval.
- D. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: A

Community vote distribution

A (100%)

✉  **Guru4Cloud** 3 months ago

Selected Answer: A

Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.
upvoted 1 times

✉  **TariqKipkemei** 6 months ago

Selected Answer: A

Unknown access patterns for the data = S3 Intelligent-Tiering
upvoted 3 times

✉  **channn** 8 months ago

Selected Answer: A

Key words: 'The company does not know access patterns for all the data', so A.
upvoted 3 times

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

Selected Answer: A

The correct answer is A.

Creating an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering would be the most efficient solution to optimize the cost of S3 usage. S3 Intelligent-Tiering is a storage class that automatically moves objects between two access tiers (frequent and infrequent) based on changing access patterns. It is a cost-effective solution that does not require any manual intervention to move data to different storage classes, unlike the other options.

upvoted 3 times

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

Answer B, Using the S3 storage class analysis tool to determine the correct tier for each object and manually moving objects to the identified storage tier would be time-consuming and require more operational overhead.

Answer C, Transitioning objects to S3 Glacier Instant Retrieval would be appropriate for data that is accessed less frequently and does not require immediate access.

Answer D, S3 One Zone-IA would be appropriate for data that can be recreated if lost and does not require the durability of S3 Standard or S3 Standard-IA.

upvoted 1 times

✉  **COTIT** 8 months, 1 week ago

Selected Answer: A

For me is A. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.

Why?

"S3 Intelligent-Tiering is the ideal storage class for data with unknown, changing, or unpredictable access patterns"

<https://aws.amazon.com/s3/storage-classes/intelligent-tiering/>

upvoted 2 times

✉  **Bofi** 8 months, 1 week ago

Selected Answer: A

Once the data traffic is unpredictable, Intelligent-Tiering is the best option
upvoted 2 times

 **NIL8891** 8 months, 1 week ago

Selected Answer: A

Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.
upvoted 1 times

 **Maximus007** 8 months, 1 week ago

Selected Answer: A

A: as exact pattern is not clear
upvoted 2 times

A rapidly growing global ecommerce company is hosting its web application on AWS. The web application includes static content and dynamic content. The website stores online transaction processing (OLTP) data in an Amazon RDS database. The website's users are experiencing slow page loads.

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

- A. Configure an Amazon Redshift cluster.
- B. Set up an Amazon CloudFront distribution.
- C. Host the dynamic web content in Amazon S3.
- D. Create a read replica for the RDS DB instance.
- E. Configure a Multi-AZ deployment for the RDS DB instance.

Correct Answer: BD

Community vote distribution

BD (84%) Other

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

Selected Answer: BD

To resolve the issue of slow page loads for a rapidly growing e-commerce website hosted on AWS, a solutions architect can take the following two actions:

1. Set up an Amazon CloudFront distribution
2. Create a read replica for the RDS DB instance

Configuring an Amazon Redshift cluster is not relevant to this issue since Redshift is a data warehousing service and is typically used for the analytical processing of large amounts of data.

Hosting the dynamic web content in Amazon S3 may not necessarily improve performance since S3 is an object storage service, not a web application server. While S3 can be used to host static web content, it may not be suitable for hosting dynamic web content since S3 doesn't support server-side scripting or processing.

Configuring a Multi-AZ deployment for the RDS DB instance will improve high availability but may not necessarily improve performance.
upvoted 8 times

 **Guru4Cloud** Most Recent 3 months ago

Selected Answer: BD

The two options that will best help resolve the slow page loads are:

- B) Set up an Amazon CloudFront distribution
and
E) Configure a Multi-AZ deployment for the RDS DB instance

Explanation:

CloudFront can cache static content globally and improve latency for static content delivery.
Multi-AZ RDS improves performance and availability of the database driving dynamic content.
upvoted 2 times

 **antropaws** 6 months ago

Selected Answer: BD

BD is correct.

upvoted 3 times

 **TariqKipkemei** 6 months ago

Selected Answer: BD

Resolve latency = Amazon CloudFront distribution and read replica for the RDS DB
upvoted 3 times

 **SamDouk** 8 months ago

Selected Answer: BD

B and D

upvoted 2 times

✉  **klayytech** 8 months, 1 week ago

Selected Answer: BD

The website's users are experiencing slow page loads.

To resolve this issue, a solutions architect should take the following two actions:

Create a read replica for the RDS DB instance. This will help to offload read traffic from the primary database instance and improve performance.

upvoted 2 times

✉  **zooba72** 8 months, 1 week ago

Selected Answer: BD

Question asked about performance improvements, not HA. Cloudfront & Read Replica

upvoted 2 times

✉  **thaotnt** 8 months, 1 week ago

Selected Answer: BD

slow page loads. >>> D

upvoted 2 times

✉  **andyto** 8 months, 1 week ago

Selected Answer: BD

Read Replica will speed up Reads on RDS DB.

E is wrong. It brings HA but doesn't contribute to speed which is impacted in this case. Multi-AZ is Active-Standby solution.

upvoted 1 times

✉  **COTIT** 8 months, 1 week ago

Selected Answer: BE

I agree with B & E.

B. Set up an Amazon CloudFront distribution. (Amazon CloudFront is a content delivery network (CDN) service)

E. Configure a Multi-AZ deployment for the RDS DB instance. (Good idea for loadbalance the DB workflow)

upvoted 2 times

✉  **Santosh43** 8 months, 1 week ago

B and E (as there is nothing mention about read transactions)

upvoted 1 times

✉  **Akademik6** 8 months, 1 week ago

Selected Answer: BD

Cloudfront and Read Replica. We don't need HA here.

upvoted 3 times

✉  **acts268** 8 months, 1 week ago

Selected Answer: BD

Cloud Front and Read Replica

upvoted 4 times

✉  **Bofi** 8 months, 1 week ago

Selected Answer: BE

Amazon CloudFront can handle both static and Dynamic contents hence there is not need for option C i.e hosting the static data on Amazon S3. RDS read replica will reduce the amount of reads on the RDS hence leading a better performance. Multi-AZ is for disaster Recovery , which means D is also out.

upvoted 1 times

✉  **Thief** 8 months, 1 week ago

Selected Answer: BC

CloudFont with S3

upvoted 1 times

✉  **NIL8891** 8 months, 1 week ago

Selected Answer: BE

B and E

upvoted 2 times

A company uses Amazon EC2 instances and AWS Lambda functions to run its application. The company has VPCs with public subnets and private subnets in its AWS account. The EC2 instances run in a private subnet in one of the VPCs. The Lambda functions need direct network access to the EC2 instances for the application to work.

The application will run for at least 1 year. The company expects the number of Lambda functions that the application uses to increase during that time. The company wants to maximize its savings on all application resources and to keep network latency between the services low.

Which solution will meet these requirements?

- A. Purchase an EC2 Instance Savings Plan Optimize the Lambda functions' duration and memory usage and the number of invocations. Connect the Lambda functions to the private subnet that contains the EC2 instances.
- B. Purchase an EC2 Instance Savings Plan Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to a public subnet in the same VPC where the EC2 instances run.
- C. Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to the private subnet that contains the EC2 instances.
- D. Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Keep the Lambda functions in the Lambda service VPC.

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

Answer C is the best solution that meets the company's requirements.

By purchasing a Compute Savings Plan, the company can save on the costs of running both EC2 instances and Lambda functions. The Lambda functions can be connected to the private subnet that contains the EC2 instances through a VPC endpoint for AWS services or a VPC peering connection. This provides direct network access to the EC2 instances while keeping the traffic within the private network, which helps to minimize network latency.

Optimizing the Lambda functions' duration, memory usage, number of invocations, and amount of data transferred can help to further minimize costs and improve performance. Additionally, using a private subnet helps to ensure that the EC2 instances are not directly accessible from the public internet, which is a security best practice.

upvoted 9 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Answer A is not the best solution because connecting the Lambda functions directly to the private subnet that contains the EC2 instances may not be scalable as the number of Lambda functions increases. Additionally, using an EC2 Instance Savings Plan may not provide savings on the costs of running Lambda functions.

Answer B is not the best solution because connecting the Lambda functions to a public subnet may not be as secure as connecting them to a private subnet. Also, keeping the EC2 instances in a private subnet helps to ensure that they are not directly accessible from the public internet.

Answer D is not the best solution because keeping the Lambda functions in the Lambda service VPC may not provide direct network access to the EC2 instances, which may impact the performance of the application.

upvoted 4 times

 **TariqKipkemei** Most Recent 1 month ago

Selected Answer: C

Implement Compute Savings Plan because it applies to Lambda usage as well, then connect the Lambda functions to the private subnet that contains the EC2 instances

upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: C

A Compute Savings Plan covers both EC2 and Lambda and allows maximizing savings on all resources.

Optimizing Lambda configuration reduces costs.

Connecting the Lambda functions to the private subnet with the EC2 instances provides direct network access between them, keeping latency low. The Lambda functions are isolated in the private subnet rather than public, improving security.

upvoted 1 times

 **jaehoon090** 3 months, 3 weeks ago

CCCCCCCCCCCCCCCCCCCC

upvoted 1 times

✉  **elearningtakai** 8 months ago

Selected Answer: C

Connect Lambda to Private Subnet contains EC2

upvoted 1 times

✉  **zooba72** 8 months, 1 week ago

Selected Answer: C

Compute savings plan covers both EC2 & Lambda

upvoted 2 times

✉  **Zox42** 8 months, 1 week ago

C. I would go with C, because Compute savings plans cover Lambda as well.

upvoted 2 times

✉  **andyto** 8 months, 1 week ago

A. I would go with A. Saving and low network latency are required.

EC2 instance savings plans offer savings of up to 72%

Compute savings plans offer savings of up to 66%

Placing Lambda on the same private network with EC2 instances provides the lowest latency.

upvoted 1 times

✉  **abitwrong** 8 months, 1 week ago

EC2 Instance Savings Plans apply to EC2 usage only. Compute Savings Plans apply to usage across Amazon EC2, AWS Lambda, and AWS Fargate. (<https://aws.amazon.com/savingsplans/faq/>)

Lambda functions need direct network access to the EC2 instances for the application to work and these EC2 instances are in the private subnet.

So the correct answer is C.

upvoted 1 times

A solutions architect needs to allow team members to access Amazon S3 buckets in two different AWS accounts: a development account and a production account. The team currently has access to S3 buckets in the development account by using unique IAM users that are assigned to an IAM group that has appropriate permissions in the account.

The solutions architect has created an IAM role in the production account. The role has a policy that grants access to an S3 bucket in the production account.

Which solution will meet these requirements while complying with the principle of least privilege?

- A. Attach the Administrator Access policy to the development account users.
- B. Add the development account as a principal in the trust policy of the role in the production account.
- C. Turn off the S3 Block Public Access feature on the S3 bucket in the production account.
- D. Create a user in the production account with unique credentials for each team member.

Correct Answer: B

Community vote distribution

B (100%)

✉️  **kels1** Highly Voted 7 months, 1 week ago

well, if you made it this far, it means you are persistent :) Good luck with your exam!
upvoted 43 times

✉️  **Kimnesh** 3 months, 1 week ago

thank you!
upvoted 1 times

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

Thanks good luck for all
upvoted 4 times

✉️  **TariqKipkemei** Most Recent 1 month ago

Selected Answer: B

Add the development account as a principal in the trust policy of the role in the production account
upvoted 1 times

✉️  **Guru4Cloud** 3 months ago

Selected Answer: B

The best solution is B) Add the development account as a principal in the trust policy of the role in the production account.

This allows cross-account access to the S3 bucket in the production account by assuming the IAM role. The development account users can assume the role to gain temporary access to the production bucket.
upvoted 1 times

✉️  **nilandd44gg** 4 months, 3 weeks ago

Selected Answer: B

<https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/>

An AWS account accesses another AWS account – This use case is commonly referred to as a cross-account role pattern. It allows human or machine IAM principals from one AWS account to assume this role and act on resources within a second AWS account. A role is assumed to enable this behavior when the resource in the target account doesn't have a resource-based policy that could be used to grant cross-account access.

upvoted 1 times

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

Selected Answer: B

By adding the development account as a principal in the trust policy of the IAM role in the production account, you are allowing users from the development account to assume the role in the production account. This allows the team members to access the S3 bucket in the production account without granting them unnecessary privileges.

upvoted 2 times

✉️  **elearningtakai** 8 months ago

Selected Answer: B

About Trust policy – The trust policy defines which principals can assume the role, and under which conditions. A trust policy is a specific type of resource-based policy for IAM roles.

Answer A: overhead permission Admin to development.

Answer C: Block public access is a security best practice and seems not relevant to this scenario.

Answer D: difficult to manage and scale

upvoted 1 times

 **Buruguduystunstugudunstuy** 8 months, 1 week ago

Selected Answer: B

Answer A, attaching the Administrator Access policy to development account users, provides too many permissions and violates the principle of least privilege. This would give users more access than they need, which could lead to security issues if their credentials are compromised.

Answer C, turning off the S3 Block Public Access feature, is not a recommended solution as it is a security best practice to enable S3 Block Public Access to prevent accidental public access to S3 buckets.

Answer D, creating a user in the production account with unique credentials for each team member, is also not a recommended solution as it can be difficult to manage and scale for large teams. It is also less secure, as individual user credentials can be more easily compromised.

upvoted 2 times

 **klaytech** 8 months, 1 week ago

Selected Answer: B

The solution that will meet these requirements while complying with the principle of least privilege is to add the development account as a principal in the trust policy of the role in the production account. This will allow team members to access Amazon S3 buckets in two different AWS accounts while complying with the principle of least privilege.

Option A is not recommended because it grants too much access to development account users. Option C is not relevant to this scenario. Option D is not recommended because it does not comply with the principle of least privilege.

upvoted 1 times

 **Akademik6** 8 months, 1 week ago

Selected Answer: B

B is the correct answer

upvoted 2 times

A company uses AWS Organizations with all features enabled and runs multiple Amazon EC2 workloads in the ap-southeast-2 Region. The company has a service control policy (SCP) that prevents any resources from being created in any other Region. A security policy requires the company to encrypt all data at rest.

An audit discovers that employees have created Amazon Elastic Block Store (Amazon EBS) volumes for EC2 instances without encrypting the volumes. The company wants any new EC2 instances that any IAM user or root user launches in ap-southeast-2 to use encrypted EBS volumes. The company wants a solution that will have minimal effect on employees who create EBS volumes.

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

- A. In the Amazon EC2 console, select the EBS encryption account attribute and define a default encryption key.
- B. Create an IAM permission boundary. Attach the permission boundary to the root organizational unit (OU). Define the boundary to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.
- C. Create an SCP. Attach the SCP to the root organizational unit (OU). Define the SCP to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.
- D. Update the IAM policies for each account to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.
- E. In the Organizations management account, specify the Default EBS volume encryption setting.

Correct Answer: AD

Community vote distribution

CE (89%) 11%

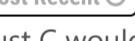
 **Axaus**  6 months, 2 weeks ago

Selected Answer: CE

CE

Prevent future issues by creating a SCP and set a default encryption.

upvoted 5 times

 **Valder21**  2 months, 3 weeks ago

Wondering if just C would be sufficient?

upvoted 1 times

 **bjexamprep** 2 months, 3 weeks ago

Seems many people selected E as part of the correct answer. But I didn't find so called Organization level EBS default setting in my Organization management account. I tried setting default EBS encryption setting in my Organization management account, and it didn't apply to the member account. If E cannot guarantee default encryption in all other account, E has no advantage over A. Anyone can explain why E is better than A?

upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: CE

The correct answer is (C) and (E).

Option (C): Creating an SCP and attaching it to the root organizational unit (OU) will deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false. This means that any IAM user or root user in any account in the organization will not be able to create an EBS volume without encrypting it.

Option (E): Specifying the Default EBS volume encryption setting in the Organizations management account will ensure that all new EBS volumes created in any account in the organization are encrypted by default.

upvoted 3 times

 **novelai_me** 5 months ago

Selected Answer: AE

Option A: By default, EBS encryption is not enabled for EC2 instances. However, you can set an EBS encryption by default in your AWS account in the Amazon EC2 console. This ensures that every new EBS volume that is created is encrypted.

Option E: With AWS Organizations, you can centrally set the default EBS encryption for your organization's accounts. This helps in enforcing a consistent encryption policy across your organization.

Option B, C and D are not correct because while you can use IAM policies or SCPs to restrict the creation of unencrypted EBS volumes, this could potentially impact employees' ability to create necessary resources if not properly configured. They might require additional permissions management, which is not mentioned in the requirements. By setting the EBS encryption by default at the account or organization level (Options A and E), you can ensure all new volumes are encrypted without affecting the ability of employees to create resources.

upvoted 2 times

 **Buruguduystunstugudunstuy** 5 months, 2 weeks ago

Selected Answer: CE

SCPs are a great way to enforce policies across an entire AWS Organization, preventing users from creating resources that do not comply with the set policies.

In AWS Management Console, one can go to EC2 dashboard -> Settings -> Data encryption -> Check "Always encrypt new EBS volumes" and choose a default KMS key. This ensures that every new EBS volume created will be encrypted by default, regardless of how it is created.

upvoted 2 times

✉ **PRASAD180** 6 months ago

1000% CE crt

upvoted 1 times

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

Encryption by default allows you to ensure that all new EBS volumes created in your account are always encrypted, even if you don't specify encrypted=true request parameter.

<https://aws.amazon.com/blogs/compute/must-know-best-practices-for-amazon-ebs-encryption/>

upvoted 1 times

✉ **hiroohiroo** 6 months, 1 week ago

Selected Answer: CE

CとEが正しいと考える。

upvoted 3 times

✉ **Efren** 6 months, 2 weeks ago

Selected Answer: CE

CE for me as well

upvoted 2 times

✉ **nonsense** 6 months, 2 weeks ago

Selected Answer: CE

SCP that denies the ec2>CreateVolume action when the ec2:Encrypted condition equals false. This will prevent users and service accounts in member accounts from creating unencrypted EBS volumes in the ap-southeast-2 Region.

upvoted 2 times

✉ **Efren** 6 months, 2 weeks ago

agreed

upvoted 1 times

A company wants to use an Amazon RDS for PostgreSQL DB cluster to simplify time-consuming database administrative tasks for production database workloads. The company wants to ensure that its database is highly available and will provide automatic failover support in most scenarios in less than 40 seconds. The company wants to offload reads off of the primary instance and keep costs as low as possible.

Which solution will meet these requirements?

- A. Use an Amazon RDS Multi-AZ DB instance deployment. Create one read replica and point the read workload to the read replica.
- B. Use an Amazon RDS Multi-AZ DB cluster deployment. Create two read replicas and point the read workload to the read replicas.
- C. Use an Amazon RDS Multi-AZ DB instance deployment. Point the read workload to the secondary instances in the Multi-AZ pair.
- D. Use an Amazon RDS Multi-AZ DB cluster deployment. Point the read workload to the reader endpoint.

Correct Answer: A

Community vote distribution

D (76%)	A (24%)
---------	---------

 **Buruguduystunstugudunstuy** Highly Voted 5 months, 2 weeks ago

Selected Answer: D

The correct answer is:

D. Use an Amazon RDS Multi-AZ DB cluster deployment. Point the read workload to the reader endpoint.

Explanation:

The company wants high availability, automatic failover support in less than 40 seconds, read offloading from the primary instance, and cost-effectiveness.

Answer D is the best choice for several reasons:

1. Amazon RDS Multi-AZ deployments provide high availability and automatic failover support.
2. In a Multi-AZ DB cluster, Amazon RDS automatically provisions and maintains a standby in a different Availability Zone. If a failure occurs, Amazon RDS performs an automatic failover to the standby, minimizing downtime.
3. The "Reader endpoint" for an Amazon RDS DB cluster provides load-balancing support for read-only connections to the DB cluster. Directing read traffic to the reader endpoint helps in offloading read operations from the primary instance.

upvoted 7 times

 **Kiki_Pass** 4 months ago

Sorry I'm a bit confused... I thought only Aurora DB Cluster has reader endpoint. Do you by any chance has the link to the doc for RDS Reader Endpoint?

upvoted 2 times

 **lemur88** 3 months ago

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/multi-az-db-clusters-concepts-connection-management.html#multi-az-db-clusters-concepts-connection-management-endpoints-reader>

upvoted 2 times

 **ogerber** Highly Voted 6 months, 1 week ago

Selected Answer: D

A - multi-az instance : failover takes between 60-120 sec

D - multi-az cluster: failover around 35 sec

upvoted 5 times

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

Selected Answer: D

It is D.

A is not correct. Multi-AZ DB instance deployment, which creates a primary instance and a standby instance to provide failover support. However, the standby instance does not serve traffic.

upvoted 1 times

 **maudsha** 4 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/database/choose-the-right-amazon-rds-deployment-option-single-az-instance-multi-az-instance-or-multi-az-database-cluster/#:~:text=Unlike%20Multi%20AZ%20instance%20deployment,different%20AZs%20serving%20read%20traffic.>

According to this the answer is D

"Unlike Multi-AZ instance deployment, where the secondary instance can't be accessed for read or writes, Multi-AZ DB cluster deployment consists

of primary instance running in one AZ serving read-write traffic and two other standby running in two different AZs serving read traffic."

You don't have to create read replicas with cluster deployment so B is out.

upvoted 1 times

✉ **kwang312** 2 months, 2 weeks ago

D

Fail-over on Multi-AZ DB instance is 60-120s

On Cluster, the time under 35s

upvoted 3 times

✉ **Guru4Cloud** 3 months ago

Selected Answer: D

D. Use an Amazon RDS Multi-AZ DB cluster deployment. Point the read workload to the reader endpoint

upvoted 1 times

✉ **Guru4Cloud** 3 months ago

Selected Answer: D

Use an Amazon RDS Multi-AZ DB cluster deployment Point the read workload to the reader endpoint.

upvoted 1 times

✉ **Eminenza22** 3 months ago

Selected Answer: A

The solutions architect should use an Amazon RDS Multi-AZ DB instance deployment. The company can create one read replica and point the read workload to the read replica. Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments.

upvoted 1 times

✉ **Gooniegoogoo** 5 months ago

and d..

Multi-AZ DB clusters typically have lower write latency when compared to Multi-AZ DB instance deployments. They also allow read-only workloads to run on reader DB instances.

upvoted 1 times

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

Selected Answer: D

This is as case where both option A and D can work, but option D gives 2 DB instances for read compared to only 1 given by option A. Costwise they are the same as both options use 3 DB instances.

upvoted 1 times

✉ **Henrytm1** 6 months ago

Selected Answer: A

lowest cost option, and effective with read replica

upvoted 3 times

✉ **antropaws** 6 months ago

Selected Answer: D

It's D. Read well: "A company wants to use an Amazon RDS for PostgreSQL DB CLUSTER".

upvoted 3 times

✉ **RainWhisper** 6 months ago

Selected Answer: D

A Multi-AZ DB cluster deployment is a semisynchronous, high availability deployment mode of Amazon RDS with two readable standby DB instances. A Multi-AZ DB cluster has a writer DB instance and two reader DB instances in three separate Availability Zones in the same AWS Region.
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/multi-az-db-clusters-concepts.html>

Amazon RDS Multi-AZ with two readable standbys. Automatically fail over in typically under 35 seconds

<https://aws.amazon.com/rds/features/multi-az/>

upvoted 2 times

✉ **RainWhisper** 6 months ago

A Multi-AZ DB cluster deployment is a semisynchronous, high availability deployment mode of Amazon RDS with two readable standby DB instances. A Multi-AZ DB cluster has a writer DB instance and two reader DB instances in three separate Availability Zones in the same AWS Region.
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/multi-az-db-clusters-concepts.html>

Amazon RDS Multi-AZ with two readable standbys. Automatically fail over in typically under 35 seconds

<https://aws.amazon.com/rds/features/multi-az/>

upvoted 1 times

✉ **omoakin** 6 months ago

D.

Use an Amazon RDS Multi-AZ DB cluster deployment Point the read workload to the reader endpoint.

upvoted 1 times

✉ **coldgin37** 6 months ago

D - Instance deployment Failover times are typically 60–120 seconds, so a clustered deployment is required for 40sec or less
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>

upvoted 2 times

 **elmogy** 6 months, 1 week ago

Selected Answer: D

D for two reasons,

1- Failover times are typically 60–120 seconds in RDS Multi-AZ DB instance deployment.

2- we can use the secondary DB for read (it can be used on RDS Multi-AZ DB cluster), and that's will "keep the cost as low as possible"

upvoted 3 times

A company runs a highly available SFTP service. The SFTP service uses two Amazon EC2 Linux instances that run with elastic IP addresses to accept traffic from trusted IP sources on the internet. The SFTP service is backed by shared storage that is attached to the instances. User accounts are created and managed as Linux users in the SFTP servers.

The company wants a serverless option that provides high IOPS performance and highly configurable security. The company also wants to maintain control over user permissions.

Which solution will meet these requirements?

- A. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the EBS volume to the SFTP service endpoint. Grant users access to the SFTP service.
- B. Create an encrypted Amazon Elastic File System (Amazon EFS) volume. Create an AWS Transfer Family SFTP service with elastic IP addresses and a VPC endpoint that has internet-facing access. Attach a security group to the endpoint that allows only trusted IP addresses. Attach the EFS volume to the SFTP service endpoint. Grant users access to the SFTP service.
- C. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.
- D. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a VPC endpoint that has internal access in a private subnet. Attach a security group that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.

Correct Answer: C

Community vote distribution

B (73%) D (18%) 9%

✉  **NickGordon** 2 weeks, 6 days ago

Selected Answer: B

A is incorrect as EBS is not an option
C is incorrect as when I select public accessible, I don't see an option I can set up trusted IP address
D is incorrect as it is internal.

B, followed the steps and I can set up a sftp in this way
upvoted 1 times

✉  **potomac** 3 weeks, 2 days ago

Selected Answer: B

B
EFS has lower latency and higher throughput than S3 when accessed from within the same availability zone.
upvoted 1 times

✉  **thanhnv142** 1 month, 1 week ago

C: Because it is server-less. definitely not A or B because it utilizes server.
upvoted 1 times

✉  **warp** 1 month, 1 week ago

Amazon Elastic File System - Serverless, fully elastic file storage:
<https://aws.amazon.com/efs/>
upvoted 2 times

✉  **bsbs1234** 2 months ago

B,
A), transfer family does not support EBS
C,D), S3 has lower IOPS than EFS
upvoted 3 times

✉  **Guru4Cloud** 3 months ago

Selected Answer: B

Create an encrypted Amazon Elastic File System (Amazon EFS) volume. Create an AWS Transfer Family SFTP service with elastic IP addresses and a VPC endpoint that has internet-facing access. Attach a security group to the endpoint that allows only trusted IP addresses. Attach the EFS volume to the SFTP service endpoint. Grant users access to the SFTP service.

upvoted 1 times

 **Axeashes** 5 months, 2 weeks ago

<https://aws.amazon.com/blogs/storage/use-ip-whitelisting-to-secure-your-aws-transfer-for-sftp-servers/>
upvoted 1 times

 **TariqKipkemei** 5 months, 3 weeks ago

Selected Answer: B

EFS is best to serve this purpose.
upvoted 1 times

 **alexandercamachop** 5 months, 4 weeks ago

Selected Answer: B

First Serverless - EFS
Second it says it is attached to the Linux instances at the same time, only EFS can do that.
upvoted 2 times

 **envest** 6 months ago

Answer C (from abylead.com)

Transfer Family offers fully managed serverless support for B2B file transfers via SFTP, AS2, FTPS, & FTP directly in & out of S3 or EFS. For a controlled internet access you can use internet-facing endpts with Transfer SFTP servers & restrict trusted internet sources with VPC's default Sgrp. In addition, S3 Access Points aliases allows you to use S3 bkt names for a unique access control plcy on shared S3 datasets.
Transfer SFTP & S3: <https://aws.amazon.com/blogs/apn/how-to-use-aws-transfer-family-to-replace-and-scale-sftp-servers/>

A)Transfer SFTP doesn't support EBS, not for share data, & not serverless: infeasible.
B)EFS mounts via ENIs not endpts: infeasible.
D)pub endpt for internet access is missing: infeasible.
upvoted 4 times

 **omoakin** 6 months ago

BBBBBBBBBBBBBBB
upvoted 1 times

 **vesen22** 6 months ago

Selected Answer: B

EFS all day
upvoted 2 times

 **norris81** 6 months ago

<https://aws.amazon.com/blogs/storage/use-ip-whitelisting-to-secure-your-aws-transfer-for-sftp-servers/> is worth a read
upvoted 2 times

 **odjr** 6 months ago

Selected Answer: B

EFS is serverless. There is no reference in S3 about IOPS
upvoted 2 times

 **willyfoogg** 6 months ago

Selected Answer: B

Option D is incorrect because it suggests using an S3 bucket in a private subnet with a VPC endpoint, which may not meet the requirement of maintaining control over user permissions as effectively as the EFS-based solution.
upvoted 2 times

 **anibinaadi** 6 months ago

It is D
Refer <https://docs.aws.amazon.com/transfer/latest/userguide/create-server-in-vpc.html> for further details.
upvoted 1 times

 **elmogy** 6 months, 1 week ago

Selected Answer: B

EFS is serverless and has high IOPS.
regardless the IOPS, I believe option D is incorrect because it is internal, and the request needs internet access
upvoted 3 times

 **alvinnguyennexcel** 6 months, 1 week ago

Selected Answer: C

The reason is that AWS Transfer Family is a serverless option that provides a fully managed service for transferring files over Secure Shell (SSH) File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS), and File Transfer Protocol (FTP). It allows you to use your existing authentication systems and store your data in Amazon S3 or Amazon EFS. It also provides high IOPS performance and highly configurable security option
upvoted 1 times

A company is developing a new machine learning (ML) model solution on AWS. The models are developed as independent microservices that fetch approximately 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which design should a solutions architect recommend to meet these requirements?

- A. Direct the requests from the API to a Network Load Balancer (NLB). Deploy the models as AWS Lambda functions that are invoked by the NLB.
- B. Direct the requests from the API to an Application Load Balancer (ALB). Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from an Amazon Simple Queue Service (Amazon SQS) queue. Use AWS App Mesh to scale the instances of the ECS cluster based on the SQS queue size.
- C. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as AWS Lambda functions that are invoked by SQS events. Use AWS Auto Scaling to increase the number of vCPUs for the Lambda functions based on the SQS queue size.
- D. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from the queue. Enable AWS Auto Scaling on Amazon ECS for both the cluster and copies of the service based on the queue size.

Correct Answer: D*Community vote distribution*

D (100%)

✉️  **examtopictempacc** Highly Voted 6 months, 1 week ago
asynchronous=SQS, microservices=ECS.
Use AWS Auto Scaling to adjust the number of ECS services.
upvoted 5 times

✉️  **TariqKipkemei** 5 months, 3 weeks ago
good breakdown :)
upvoted 1 times

✉️  **Guru4Cloud** Most Recent 3 months ago
Selected Answer: D
I go with everyone D.
upvoted 1 times

✉️  **TariqKipkemei** 5 months, 3 weeks ago
Selected Answer: D
For once examtopic answer is correct :) haha...

Batch requests/async = Amazon SQS
Microservices = Amazon ECS
Workload variations = AWS Auto Scaling on Amazon ECS
upvoted 3 times

✉️  **alexandercamachop** 5 months, 4 weeks ago
Selected Answer: D
D, no need for an App Load balancer like C says, no where in the text.
SQS is needed to ensure all request gets routed properly in a Microservices architecture and also that it waits until its picked up.
ECS with Autoscaling, will scale based on the unknown pattern of usage as mentioned.
upvoted 1 times

✉️  **anibinaadi** 6 months ago
It is D
Refer <https://aws.amazon.com/blogs/containers/amazon-elastic-container-service-ecs-auto-scaling-using-custom-metrics/> for additional information/knowledge.
upvoted 1 times

✉️  nosense 6 months, 2 weeks ago

Selected Answer: D

because it is scalable, reliable, and efficient.
C does not scale the models automatically
upvoted 3 times

✉️  deechean 2 months, 4 weeks ago

why C doesn't scale the model? Application Auto Scaling can apply to lambda.
upvoted 1 times

Question #423

Topic 1

A solutions architect wants to use the following JSON text as an identity-based policy to grant specific permissions:

```
{ "Statement": [ { "Action": [ "ssm>ListDocuments", "ssm>GetDocument" ], "Effect": "Allow", "Resource": "*", "Sid": "" } ], "Version": "2012-10-17" }
```

Which IAM principals can the solutions architect attach this policy to? (Choose two.)

- A. Role
- B. Group
- C. Organization
- D. Amazon Elastic Container Service (Amazon ECS) resource
- E. Amazon EC2 resource

Correct Answer: AB

Community vote distribution

AB (100%)

✉️  nosense  6 months, 2 weeks ago

Selected Answer: AB

identity-based policy used for role and group
upvoted 9 times

✉️  Guru4Cloud  3 months ago

Selected Answer: AB

A. Role
B. Group
upvoted 2 times

✉️  TariqKipkemei 5 months, 3 weeks ago

Selected Answer: AB

Role or group
upvoted 1 times

A company is running a custom application on Amazon EC2 On-Demand Instances. The application has frontend nodes that need to run 24 hours a day, 7 days a week and backend nodes that need to run only for a short time based on workload. The number of backend nodes varies during the day.

The company needs to scale out and scale in more instances based on workload.

Which solution will meet these requirements MOST cost-effectively?

- A. Use Reserved Instances for the frontend nodes. Use AWS Fargate for the backend nodes.
- B. Use Reserved Instances for the frontend nodes. Use Spot Instances for the backend nodes.
- C. Use Spot Instances for the frontend nodes. Use Reserved Instances for the backend nodes.
- D. Use Spot Instances for the frontend nodes. Use AWS Fargate for the backend nodes.

Correct Answer: B

Community vote distribution

A (50%) B (50%)

 **Ramdi1**  1 month, 3 weeks ago

Selected Answer: A

Has to be A, It can scale down if required and you will be charged for what you use with fargate. Secondly they have not said the backend can have timeouts or can be down for a little period of time or something. So it has to rule out any spot instances even though they are cheaper.
upvoted 8 times

 **nonsense**  6 months, 2 weeks ago

Selected Answer: B

Reserved+ spot.
Fargate for serverless
upvoted 7 times

 **Goutham4981**  6 days, 7 hours ago

Selected Answer: B

AWS Fargate is a serverless compute engine for containers that allows you to run containers without having to manage the underlying infrastructure. It simplifies the process of deploying and managing containerized applications by abstracting away the complexities of server management, scaling, and cluster orchestration.

No containerized application requirements are mentioned in the question. Plain EC2 instances. So Fargate is not actually an option
upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

A is fargate, which is none sense. B seems more OK (though none-sense)
upvoted 2 times

 **dilaaziz** 1 month, 4 weeks ago

Selected Answer: A

Fargate for backend node
upvoted 2 times

 **Wayne23Fang** 2 months ago

Selected Answer: A

(B) would take chance, though unlikely (A) is server-less auto-scaling. In case backend is idle, it might scale down, save money but no need to worry for interruption by Spot instance.
upvoted 2 times

 **Ale1973** 3 months, 2 weeks ago

Selected Answer: A

If you will use spot instances you must assume lost any job in course. This scenario has not explicit mentions about application can tolerate this situations, then, on my opinion, option A is the most suitable.
upvoted 3 times

 **james2033** 4 months, 1 week ago

Selected Answer: B

Question keyword "scale out and scale in more instances". Therefore not related Kubernetes. Choose B, reserved instance for front-end and spot instance for back-end.

upvoted 1 times

 **Gooniegoogoo** 5 months ago

im on the fence for SPOT because you could lose your spot during a workload and it doesnt mention that, that is acceptable.. Business needs to define requirements and document acceptability for this or you lose your job..

upvoted 1 times

 **Ale1973** 3 months, 2 weeks ago

Totally agree, lose job in course is an assumption for use spot instances and scenary has not explicit mentions about

upvoted 1 times

 **TariqKipkemei** 5 months, 3 weeks ago

Option B will meet this requirement:

Frontend nodes that need to run 24 hours a day, 7 days a week = Reserved Instances

Backend nodes run only for a short time = Spot Instances

upvoted 1 times

 **udo2020** 6 months ago

But Spot Instances are not based on workloads! Maybe it should be A...!?

upvoted 3 times

 **Ale1973** 3 months, 2 weeks ago

Additionally, lose job in course is an assumption for use spot instances, and scenary has not explicit mentions about this assumption

upvoted 1 times

 **alvinnguyennexel** 6 months, 1 week ago

Selected Answer: B

short time = SPOT

upvoted 4 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: B

Agreed

upvoted 2 times

A company uses high block storage capacity to runs its workloads on premises. The company's daily peak input and output transactions per second are not more than 15,000 IOPS. The company wants to migrate the workloads to Amazon EC2 and to provision disk performance independent of storage capacity.

Which Amazon Elastic Block Store (Amazon EBS) volume type will meet these requirements MOST cost-effectively?

- A. GP2 volume type
- B. io2 volume type
- C. GP3 volume type
- D. io1 volume type

Correct Answer: C

Community vote distribution

C (92%)	8%
---------	----

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

Selected Answer: C

Gp3 \$ 0.08 usd per gb
 Gp2 \$ 0.10 usd per gb
 upvoted 8 times

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

Selected Answer: C

Both GP2 and GP3 has max IOPS 16000 but GP3 is cost effective.
<https://aws.amazon.com/blogs/storage/migrate-your-amazon-ebs-volumes-from-gp2-to-gp3-and-save-up-to-20-on-costs/>
 upvoted 5 times

✉️  **Guru4Cloud**  3 months ago

Selected Answer: C

C. GP3 volume type
 upvoted 2 times

✉️  **james2033** 4 months, 1 week ago

Selected Answer: C

Quote "customers can scale up to 16,000 IOPS and" at <https://aws.amazon.com/about-aws/whats-new/2020/12/introducing-new-amazon-ebs-general-purpose-volumes-gp3/>
 upvoted 2 times

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

Selected Answer: C

The GP3 (General Purpose SSD) volume type in Amazon Elastic Block Store (EBS) is the most cost-effective option for the given requirements. GP3 volumes offer a balance of price and performance and are suitable for a wide range of workloads, including those with moderate I/O needs.

GP3 volumes allow you to provision performance independently from storage capacity, which means you can adjust the baseline performance (measured in IOPS) and throughput (measured in MiB/s) separately from the volume size. This flexibility allows you to optimize your costs while meeting the workload requirements.

In this case, since the company's daily peak input and output transactions per second are not more than 15,000 IOPS, GP3 volumes provide a suitable and cost-effective option for their workloads.

upvoted 1 times

✉️  **maver144** 6 months ago

Selected Answer: B

It is not C pals. The company wants to migrate the workloads to Amazon EC2 and to provision disk performance independent of storage capacity. With GP3 we have to increase storage capacity to increase IOPS over baseline.

You can only chose IOPS independently with IO family and IO2 is in general better then IO1.

upvoted 2 times

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

@maver144 - That's the case with GP2 volumes. With GP3 we can define IOPS independent of storage capacity.

upvoted 1 times

 **Joselucho38** 6 months, 1 week ago

Selected Answer: C

Therefore, the most suitable and cost-effective option in this scenario is the GP3 volume type (option C).

upvoted 1 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: C

GPS3 allows 16000 IOPS

upvoted 3 times

A company needs to store data from its healthcare application. The application's data frequently changes. A new regulation requires audit access at all levels of the stored data.

The company hosts the application on an on-premises infrastructure that is running out of storage capacity. A solutions architect must securely migrate the existing data to AWS while satisfying the new regulation.

Which solution will meet these requirements?

- A. Use AWS DataSync to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
- B. Use AWS Snowcone to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.
- C. Use Amazon S3 Transfer Acceleration to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
- D. Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.

Correct Answer: B

Community vote distribution

A (50%) D (50%)

 **chikawan** 6 days, 4 hours ago

Selected Answer: A

both DataSync and Storage Gateway are fine to sync data...but to "audit access at all levels of the stored data" ...it should be data events(data plane operation)..management event is some account level things.

So answer should be A

upvoted 1 times

 **bogobob** 1 week, 5 days ago

Selected Answer: D

While both DataSync and Storage Gateway allow syncing of data between on-premise and cloud, DataSync is built for rapid shifting of data into a cloud environment, not specifically for continued use in on-premise servers.

upvoted 1 times

 **potomac** 3 weeks, 2 days ago

Selected Answer: A

AWS DataSync is an online data transfer service that simplifies, automates, and accelerates the process of copying large amounts of data to and from AWS storage services over the Internet or over AWS Direct Connect.

upvoted 1 times

 **canonlycontainletters1** 1 month ago

Selected Answer: A

A seems to be more convincing to me.

upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

A is better because:

- Data sync is used for migrate. Storage gw is used to connect on-prem to AWS.
- dataevents is to log for access, management events is for config or management

upvoted 3 times

 **Wayne23Fang** 1 month, 1 week ago

Selected Answer: A

tabbyDolly 1 month ago is right. Also Data Sync is designed for data changes.

upvoted 1 times

 **brian202308** 1 month, 1 week ago

Selected Answer: D

The company hosts applications on on-premises infrastructure, so they should use a Storage Gateway solution.

upvoted 2 times

 **Ramdi1** 1 month, 3 weeks ago

Selected Answer: D

Needs access to all data hence I have put D. if it said migrating to AWS and then an audit or something then I would have chosen datasync

upvoted 3 times

 **bsbs1234** 2 months ago

A,
B) snowcone will interrupt app, or need additional step to copy data generate during transfer
C,D) are not for migrate data

And cloudTrail can log data plane events
upvoted 1 times

 **Ramdi1** 2 months ago

Selected Answer: A
A - The way I look at this after some other questions a helpful comment was migrate use Data Sync if you need to still retain on site and move to cloud then storage/volume gateways.
upvoted 1 times

 **michalf84** 2 months, 1 week ago

The answer is storage gateway as per cloudfuru. Data synch is for one time migration for continuous synch storage gateway
upvoted 2 times

 **tabbyDolly** 2 months, 1 week ago

A
audit access at all levels of the stored data -> data event is more suitable than management event
<https://repost.aws/knowledge-center/cloudtrail-data-management-events>
upvoted 1 times

 **ssa03** 2 months, 4 weeks ago

Selected Answer: D
1- The application's data frequently changes, so we need to keep the data updated on AWS
2- Running out of storage capacity, we need a new storage capacity on-premise
upvoted 3 times

 **Guru4Cloud** 3 months ago

Selected Answer: D
AWS Storage Gateway allows secure migration of on-premises data to S3 while integrating with existing infrastructure. Storage Gateway can be configured in gateway-cached mode to provide low-latency access to frequently changed data.

Enabling AWS CloudTrail logging of management events will capture the required audit data for all API actions taken on the S3 bucket and objects.
upvoted 1 times

 **TariqKipkemei** 5 months, 3 weeks ago

Selected Answer: A
For a scenario where they want to maintain some/all of the data on prem then AWS Storage Gateway would be the option to offer hybrid cloud storage.
In this case they want to migrate all the data to the cloud so AWS Datasync is the best option.
upvoted 2 times

 **alexandercamachop** 5 months, 4 weeks ago

Selected Answer: A
Datasync, this way we can monitor and audit all of the data at all times.
With Snowcone / Snowball we lose access to audit the data while it arrives into AWS Data centers / Region / Availability Zone.
upvoted 1 times

 **alexandercamachop** 5 months, 4 weeks ago

AWS DataSync is a data transfer service that simplifies and accelerates moving large amounts of data to and from AWS. It is designed to securely and efficiently migrate data from on-premises storage systems to AWS services like Amazon S3.

In this scenario, the company needs to securely migrate its healthcare application data to AWS while satisfying the new regulation for audit access. By using AWS DataSync, the existing data can be securely transferred to Amazon S3, ensuring the data is stored in a scalable and durable storage service.

Additionally, using AWS CloudTrail to log data events ensures that all access and activity related to the data stored in Amazon S3 is audited. This helps meet the regulatory requirement for audit access at all levels of the stored data.

upvoted 1 times

 **Felix_br** 5 months, 4 weeks ago

DataSync can be used to backup data from one AWS storage service into another. Services such as Amazon S3 already has built-in tools for automatic data replication from one bucket to another. However, the replication only occurs for new data added to the bucket after the replication setting was turned on. So, is it possible to use datasync from onpremis to aws ?

upvoted 2 times

A solutions architect is implementing a complex Java application with a MySQL database. The Java application must be deployed on Apache Tomcat and must be highly available.

What should the solutions architect do to meet these requirements?

- A. Deploy the application in AWS Lambda. Configure an Amazon API Gateway API to connect with the Lambda functions.
 - B. Deploy the application by using AWS Elastic Beanstalk. Configure a load-balanced environment and a rolling deployment policy.
 - C. Migrate the database to Amazon ElastiCache. Configure the ElastiCache security group to allow access from the application.
 - D. Launch an Amazon EC2 instance. Install a MySQL server on the EC2 instance. Configure the application on the server. Create an AMI. Use the AMI to create a launch template with an Auto Scaling group.

Correct Answer: B

Community vote distribution

B (100%)

 Guru4Cloud 3 months ago

Selected Answer: B

- B. Deploy the application by using AWS Elastic Beanstalk. Configure a load-balanced environment and a rolling deployment policy.
upvoted 3 times

 james2033 4 months, 1 week ago

Selected Answer: B

Keyword "AWS Elastic Beanstalk" for re-architecture from Java web-app inside Apache Tomcat to AWS Cloud.
upvoted 2 times

 TariqKipkemei 5 months, 3 weeks ago

Selected Answer: B

Definitely B
upvoted 1 times

 antropaws 6 months ago

Selected Answer: B

Clearly B.
upvoted 2 times

 cloudenthusiast 6 months, 2 weeks ago

B

AWS Elastic Beanstalk provides an easy and quick way to deploy, manage, and scale applications. It supports a variety of platforms, including Java and Apache Tomcat. By using Elastic Beanstalk, the solutions architect can upload the Java application and configure the environment to run Apache Tomcat.

upvoted 4 times

 nosense 6 months, 2 weeks ago

Selected Answer: B

Easy deploy, management and scale
upvoted 2 times

 greyrose 6 months, 2 weeks ago

Selected Answer: B

A serverless application uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. The Lambda function needs permissions to read and write to the DynamoDB table.

Which solution will give the Lambda function access to the DynamoDB table MOST securely?

- A. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters as part of the Lambda environment variables. Ensure that other AWS users do not have read and write access to the Lambda function configuration.
- B. Create an IAM role that includes Lambda as a trusted service. Attach a policy to the role that allows read and write access to the DynamoDB table. Update the configuration of the Lambda function to use the new role as the execution role.
- C. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters in AWS Systems Manager Parameter Store as secure string parameters. Update the Lambda function code to retrieve the secure string parameters before connecting to the DynamoDB table.
- D. Create an IAM role that includes DynamoDB as a trusted service. Attach a policy to the role that allows read and write access from the Lambda function. Update the code of the Lambda function to attach to the new role as an execution role.

Correct Answer: B

Community vote distribution

B (100%)

 **james2033** 4 months, 1 week ago

Selected Answer: B

Keyword B. " IAM role that includes Lambda as a trusted service", not "IAM role that includes DynamoDB as a trusted service" in D. It is IAM role, not IAM user.

upvoted 1 times

 **antropaws** 6 months ago

Selected Answer: B

B sounds better.

upvoted 1 times

 **omoakin** 6 months ago

BBBBBBBBBB

upvoted 1 times

 **alvinnguyennexcel** 6 months, 1 week ago

Selected Answer: B

vote B

upvoted 1 times

 **cloudenthusiast** 6 months, 2 weeks ago

B

Option B suggests creating an IAM role that includes Lambda as a trusted service, meaning the role is specifically designed for Lambda functions. The role should have a policy attached to it that grants the required read and write access to the DynamoDB table.

upvoted 2 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

B is right

Role key word and trusted service lambda

upvoted 3 times

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "1",  
            "Effect": "Allow",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Region": "us-east-1"  
                }  
            }  
        },  
        {  
            "Sid": "2",  
            "Effect": "Deny",  
            "Action": [  
                "ec2:StopInstances",  
                "ec2:TerminateInstances"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}  
            }  
        }  
    ]  
}
```

What are the effective IAM permissions of this policy for group members?

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.
- B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).
- C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.
- D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Correct Answer: D

Community vote distribution

D (100%)

✉  **youdelin** 1 month, 2 weeks ago

the json is describing a lot of things apparently, so I go with the longest answer lol
upvoted 1 times

✉  **Guru4Cloud** 3 months ago

Selected Answer: D

D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region
upvoted 1 times

✉  **james2033** 4 months, 1 week ago

Selected Answer: D

- A. "Statements after the Allow permission are not applied." --> Wrong.
- B. "denied any Amazon EC2 permissions in the us-east-1 Region" --> Wrong. Just deny 2 items.
- C. "allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions" --> Wrong. Just region us-east-1.
- D. ok.

upvoted 1 times

✉  **jack79** 5 months, 2 weeks ago

came in exam today

upvoted 4 times

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

Selected Answer: D

Only D makes sense

upvoted 1 times

✉  **antropaws** 6 months ago

Selected Answer: D

D sounds about right.

upvoted 1 times

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

Selected Answer: D

D is correct

upvoted 2 times

✉  **omoakin** 6 months, 2 weeks ago

D is correct

upvoted 1 times

✉  **nonsense** 6 months, 2 weeks ago

Selected Answer: D

D is right

upvoted 2 times

A manufacturing company has machine sensors that upload .csv files to an Amazon S3 bucket. These .csv files must be converted into images and must be made available as soon as possible for the automatic generation of graphical reports.

The images become irrelevant after 1 month, but the .csv files must be kept to train machine learning (ML) models twice a year. The ML trainings and audits are planned weeks in advance.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Launch an Amazon EC2 Spot Instance that downloads the .csv files every hour, generates the image files, and uploads the images to the S3 bucket.
- B. Design an AWS Lambda function that converts the .csv files into images and stores the images in the S3 bucket. Invoke the Lambda function when a .csv file is uploaded.
- C. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Glacier 1 day after they are uploaded. Expire the image files after 30 days.
- D. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 1 day after they are uploaded. Expire the image files after 30 days.
- E. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 1 day after they are uploaded. Keep the image files in Reduced Redundancy Storage (RRS).

Correct Answer: BC

Community vote distribution

BC (88%) 12%

✉  **Xin123** 2 months ago

Selected Answer: BC

Answer is B&C. For D, you must store data for 30 days in s3 standard before move to IA tiers, glacier is fine

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html#:~:text=Before%20you%20transition%20objects%20to%20S3%20Standard%2DIA%20or%20S3%20One%20Zone%2DIA%2C%20you%20must%20store%20them%20for%20at%20least%2030%20days%20in%20Amazon%20S3>
upvoted 1 times

✉  **Guru4Cloud** 3 months ago

Selected Answer: BC

Definitely B & C

upvoted 1 times

✉  **jayce5** 4 months ago

Selected Answer: BC

A. Wrong, the .csv files must be processed asap.

D and E are incorrect since Glacier is the most cost-effective option, and plans for using .csv files are known weeks in advance.

upvoted 1 times

✉  **james2033** 4 months, 1 week ago

Why need "These .csv files must be converted into images"?

upvoted 1 times

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

Selected Answer: BC

the key word is Weeks in advance, even you save data in S3 Gracia will also OK to take couples days to retrieve the data

upvoted 2 times

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

Selected Answer: BC

Definitely B & C

upvoted 1 times

✉  **Abrar2022** 5 months, 4 weeks ago

Selected Answer: BC

A. Wrong because Lifecycle rule is not mentioned.

B. CORRECT

C. CORRECT

D. Why Store on S3 One Zone-Infrequent Access (S3 One Zone-IA) when the files are going to irrelevant after 1 month? (Availability 99.99% - consider cost)

E. again, Why use Reduced Redundancy Storage (RRS) when the files are irrelevant after 1 month? (Availability 99.99% - consider cost)
upvoted 2 times

✉  **vesen22** 6 months ago

Selected Answer: BC

<https://docs.aws.amazon.com/amazonglacier/latest/dev/introduction.html>
upvoted 3 times

✉  **RoroJ** 6 months ago

Selected Answer: BE

B: Serverless and fast responding
E: will keep .csv file for a year, C and D expires the file after 30 days.
upvoted 2 times

✉  **RoroJ** 6 months ago

B&C, misread the question, expires the image files after 30 days.
upvoted 1 times

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

Selected Answer: BC

<https://aws.amazon.com/jp/about-aws/whats-new/2021/11/amazon-s3-glacier-storage-class-amazon-s3-glacier-flexible-retrieval/>
upvoted 2 times

✉  **nonsense** 6 months, 2 weeks ago

Selected Answer: BC

B severless and cost effective
C corrctl rule to store
upvoted 2 times

A company has developed a new video game as a web application. The application is in a three-tier architecture in a VPC with Amazon RDS for MySQL in the database layer. Several players will compete concurrently online. The game's developers want to display a top-10 scoreboard in near-real time and offer the ability to stop and restore the game while preserving the current scores.

What should a solutions architect do to meet these requirements?

- A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.
- B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.
- C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.
- D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

Correct Answer: B

Community vote distribution

B (92%) 8%

✉️  **potomac** 3 weeks, 2 days ago

Selected Answer: B

ElastiCache for Redis sorts and ranks datasets
upvoted 1 times

✉️  **TariqKipkemei** 1 month ago

Selected Answer: B

Real-time gaming leaderboards are easy to create with Amazon ElastiCache for Redis. Just use the Redis Sorted Set data structure, which provides uniqueness of elements while maintaining the list sorted by their scores. Creating a real-time ranked list is as simple as updating a user's score each time it changes. You can also use Sorted Sets to handle time series data by using timestamps as the score.

<https://aws.amazon.com/elasticsearch/redis/#:~:text=ElastiCache%20for%20Redis.-,Gaming,-Leaderboards>
upvoted 1 times

✉️  **5ab5e39** 2 months, 2 weeks ago

<https://aws.amazon.com/blogs/database/building-a-real-time-gaming-leaderboard-with-amazon-elasticsearch-for-redis/>
upvoted 2 times

✉️  **Guru4Cloud** 3 months ago

Selected Answer: B

Redis provides fast in-memory data storage and processing. It can compute the top 10 scores and update the cache in milliseconds. ElastiCache Redis supports sorting and ranking operations needed for the top 10 leaderboard. The cached leaderboard can be retrieved from Redis vs hitting the MySQL database for every read. This reduces load on the database. Redis supports persistence, so scores are preserved if the cache stops/restarts
upvoted 2 times

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

Selected Answer: A

concurrently = memcached
upvoted 1 times

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

Selected Answer: B

See case study of leaderboard with Redis at <https://redis.io/docs/data-types/sorted-sets/>, it is feature "sorted sets". See comparison between Redis and Memcached at <https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug>SelectEngine.html>, the different at feature "Sorted sets"
upvoted 2 times

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

Selected Answer: B

advanced data structures, complex querying, pub/sub messaging, or persistence, Redis may be a better fit.
upvoted 1 times

✉️  **haoAWS** 5 months, 1 week ago

B is correct
upvoted 1 times

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

B correct.

upvoted 1 times

✉  **hirohiroo** 6 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/jp/blogs/news/building-a-real-time-gaming-leaderboard-with-amazon-elasticsearch-for-redis/>

upvoted 3 times

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

Amazon ElastiCache for Redis is a highly scalable and fully managed in-memory data store. It can be used to store and compute the scores in real time for the top-10 scoreboard. Redis supports sorted sets, which can be used to store the scores as well as perform efficient queries to retrieve the top scores. By utilizing ElastiCache for Redis, the web application can quickly retrieve the current scores without the need to perform complex and potentially resource-intensive database queries.

upvoted 1 times

✉  **nonsense** 6 months, 2 weeks ago

Selected Answer: B

B is right

upvoted 1 times

✉  **Efren** 6 months, 2 weeks ago

More questions!!!

upvoted 3 times

An ecommerce company wants to use machine learning (ML) algorithms to build and train models. The company will use the models to visualize complex scenarios and to detect trends in customer data. The architecture team wants to integrate its ML models with a reporting platform to analyze the augmented data and use the data directly in its business intelligence dashboards.

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

- A. Use AWS Glue to create an ML transform to build and train models. Use Amazon OpenSearch Service to visualize the data.
- B. Use Amazon SageMaker to build and train models. Use Amazon QuickSight to visualize the data.
- C. Use a pre-built ML Amazon Machine Image (AMI) from the AWS Marketplace to build and train models. Use Amazon OpenSearch Service to visualize the data.
- D. Use Amazon QuickSight to build and train models by using calculated fields. Use Amazon QuickSight to visualize the data.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: B

Use Amazon SageMaker to build and train models. Use Amazon QuickSight to visualize the data.

upvoted 1 times

 **james2033** 4 months, 1 week ago

Selected Answer: B

Question keyword "machine learning", answer keyword "Amazon SageMaker". Choose B. Use Amazon QuickSight for visualization. See "Gaining insights with machine learning (ML) in Amazon QuickSight" at <https://docs.aws.amazon.com/quicksight/latest/user/making-data-driven-decisions-with-ml-in-quicksight.html>

upvoted 1 times

 **VellaDevil** 4 months, 3 weeks ago

Selected Answer: B

Sagemaker.

upvoted 1 times

 **TariqKipkemei** 5 months, 3 weeks ago

Selected Answer: B

Business intelligence, visualiations = AmazonQuicksight

ML = Amazon SageMaker

upvoted 1 times

 **antropaws** 6 months ago

Selected Answer: B

Most likely B.

upvoted 1 times

 **omoakin** 6 months, 2 weeks ago

Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy ML models quickly.

upvoted 1 times

 **cloudenthusiast** 6 months, 2 weeks ago

Amazon SageMaker is a fully managed service that provides a complete set of tools and capabilities for building, training, and deploying ML models. It simplifies the end-to-end ML workflow and reduces operational overhead by handling infrastructure provisioning, model training, and deployment.

To visualize the data and integrate it into business intelligence dashboards, Amazon QuickSight can be used. QuickSight is a cloud-native business intelligence service that allows users to easily create interactive visualizations, reports, and dashboards from various data sources, including the augmented data generated by the ML models.

upvoted 2 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: B

ML== SageMaker

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

B sagemaker provide deploy ml models

upvoted 1 times

A company is running its production and nonproduction environment workloads in multiple AWS accounts. The accounts are in an organization in AWS Organizations. The company needs to design a solution that will prevent the modification of cost usage tags.

Which solution will meet these requirements?

- A. Create a custom AWS Config rule to prevent tag modification except by authorized principals.
- B. Create a custom trail in AWS CloudTrail to prevent tag modification.
- C. Create a service control policy (SCP) to prevent tag modification except by authorized principals.
- D. Create custom Amazon CloudWatch logs to prevent tag modification.

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: C

Tip: AWS Organziation + service control policy (SCP) - This for any questions, you see both together. then you tell me
C. Create a service control policy (SCP) to prevent tag modification except by authorized principals.

upvoted 1 times

 **james2033** 4 months, 1 week ago

Selected Answer: C

D "Amazon CloudWatch" just for logging, not for prevent tag modification
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies-cwe.html

Amazon Organiation has "Service Control Policy (SCP)" with "tag policy"
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html . Choose C.

AWS Config for technical stuff, not for tag policies. Not A.

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: C

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization.

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: C

Anytime we need to restrict anything in an AWS Organization, it is SCP Policies.

upvoted 1 times

 **Abrar2022** 5 months, 4 weeks ago

AWS Config is for tracking configuration changes

upvoted 1 times

 **Abrar2022** 5 months, 4 weeks ago

so it's wrong. Right asnwer is C

upvoted 2 times

 **antropaws** 6 months ago

Selected Answer: C

I'd say C.

upvoted 2 times

 **hiroohiroo** 6 months, 1 week ago

Selected Answer: C

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

upvoted 3 times

 **nosense** 6 months, 2 weeks ago

Selected Answer: C

Denies tag: modify

upvoted 2 times

A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in another AWS Region with minimal downtime.

What should a solutions architect do to meet these requirements with the LEAST amount of downtime?

- A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be launched when needed. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be launched when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

Correct Answer: A

Community vote distribution

A (64%)	C (23%)	14%
---------	---------	-----

✉  **lucdt4** Highly Voted 6 months, 1 week ago

Selected Answer: A

A and D is correct.
But Route 53 has a feature DNS failover when instances down so we don't need use Cloudwatch and lambda to trigger
-> A correct
upvoted 7 times

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

Did not see Route 53 in this question right? So my opinion is D
upvoted 1 times

✉  **Wablo** 5 months, 1 week ago

Yes it does but you configure it. Its not automated anymore. D is the best answer!
upvoted 1 times

✉  **Kp88** 4 months ago

What are you talking about configuring ? Yes you have to configure everything at some point
<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring.html>
upvoted 1 times

✉  **bogobob** Most Recent 1 week, 5 days ago

Selected Answer: A

Assuming they're using Route53 as a DNS then A <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>
upvoted 1 times

✉  **EEK2k** 2 weeks, 2 days ago

Selected Answer: C

Only B and C take care of EC2 instances. But since B does not take care of Data in the Dynamo DB, C is the only correct Answer.
upvoted 1 times

✉  **potomac** 3 weeks, 2 days ago

Selected Answer: A

Route 53 has a feature DNS failover when instances down
upvoted 1 times

✉  **thanhnv142** 1 month, 1 week ago

C is the best choice here
upvoted 1 times

✉  **Wayne23Fang** 1 month, 1 week ago

Selected Answer: C

I think CloudFormation is easier than manual provision of Auto Scaling group and load balancer in DR region.

upvoted 1 times

✉ **Guru4Cloud** 3 months ago

Selected Answer: A

Creating Auto Scaling group and load balancer in DR region allows fast launch of capacity when needed. Configuring DynamoDB as a global table provides continuous data replication. Using DNS failover via Route 53 to point to the DR region's load balancer enables rapid traffic shifting.

upvoted 2 times

✉ **Wablo** 5 months, 1 week ago

Both Option A and Option D include the necessary steps of setting up an Auto Scaling group and load balancer in the disaster recovery Region, configuring the DynamoDB table as a global table, and updating DNS records. However, Option D provides a more detailed approach by explicitly mentioning the use of an Amazon CloudWatch alarm and AWS Lambda function to automate the DNS update process.

By leveraging an Amazon CloudWatch alarm, Option D allows for an automated failover mechanism. When triggered, the CloudWatch alarm can execute an AWS Lambda function, which in turn can update the DNS records in Amazon Route 53 to redirect traffic to the disaster recovery load balancer in the new Region. This automation helps reduce the potential for human error and further minimizes downtime.

Answer is D

upvoted 2 times

✉ **Kp88** 4 months ago

Failover policy takes care of DNS record update so no need for cloud watch/lambda

upvoted 1 times

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

Selected Answer: C

The company wants to ensure the application 'CAN' be made available in another AWS Region with minimal downtime. Meaning they want to be able to launch infra on need basis.

Best answer is C.

upvoted 1 times

✉ **dajform** 5 months, 1 week ago

B, C are not OK because "launching resources when needed", which will increase the time to recover "DR"

upvoted 1 times

✉ **Wablo** 5 months, 1 week ago

minimal downtime not minimal effort!

D

upvoted 1 times

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

I feel it is A

Configure DNS failover: Use DNS failover to point the application's DNS record to the load balancer in the disaster recovery Region. DNS failover allows you to route traffic to the disaster recovery Region in case of a failure in the primary Region.

upvoted 2 times

✉ **Wablo** 5 months, 1 week ago

Once you configure manually the DNS , its no more automated like Lambda does.

upvoted 1 times

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

Selected Answer: C

C suits best

upvoted 2 times

✉ **hiroohiroo** 6 months, 1 week ago

Selected Answer: A

AがDNS フェイルオーバー

upvoted 1 times

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

A

By configuring the DynamoDB table as a global table, you can replicate the table data across multiple AWS Regions, including the primary Region and the disaster recovery Region. This ensures that data is available in both Regions and can be seamlessly accessed during a failover event.

upvoted 1 times

✉ **Efren** 6 months, 2 weeks ago

Selected Answer: A

A for ME, DNS should failover

upvoted 2 times

✉ **nonsense** 6 months, 2 weeks ago

Selected Answer: D

D for me
upvoted 3 times

✉️ 🚩 **Macosxfan** 6 months, 2 weeks ago

I would pick A
upvoted 1 times

✉️ 🚩 **nonsense** 6 months, 2 weeks ago

Misunderstanding. Only A valid
upvoted 2 times

✉️ 🚩 **Efren** 6 months, 2 weeks ago

I would go for A. If we have DNS failover, why to burden with lambda updating the DNS records?

upvoted 1 times

A company needs to migrate a MySQL database from its on-premises data center to AWS within 2 weeks. The database is 20 TB in size. The company wants to complete the migration with minimal downtime.

Which solution will migrate the database MOST cost-effectively?

- A. Order an AWS Snowball Edge Storage Optimized device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes. Send the Snowball Edge device to AWS to finish the migration and continue the ongoing replication.
- B. Order an AWS Snowmobile vehicle. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with ongoing changes. Send the Snowmobile vehicle back to AWS to finish the migration and continue the ongoing replication.
- C. Order an AWS Snowball Edge Compute Optimized with GPU device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with ongoing changes. Send the Snowball device to AWS to finish the migration and continue the ongoing replication
- D. Order a 1 GB dedicated AWS Direct Connect connection to establish a connection with the data center. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes.

Correct Answer: D

Community vote distribution

A (81%)

D (19%)

 **Goutham4981** 1 week, 4 days ago

Selected Answer: A

Direct Connect takes at least 1 month to setup - D is invalid
 AWS Snowmobile is used for transferring large amounts of data (petabytes) from remote locations where establishing a connection to the cloud is impossible - B is invalid
 AWS Snowball Edge Compute Optimized provides higher vCPU performance and lower storage as compared to Snowball storage optimized. As our need is solely data transfer, high vCPU performance is not required but high storage is - C is invalid
 upvoted 1 times

 **EEK2k** 2 weeks, 2 days ago

Selected Answer: D

To calculate the time it would take to transfer 20TB of data over a 1 GB dedicated AWS Direct Connect, we can use the formula:

time = data size / data transfer rate

Here, the data size is 20TB, which is equivalent to 20,000 GB or 20,000,000 MB. The data transfer rate is 1 GB/s.

Converting the data size to MB, we get:

20,000,000 MB / 1 GB/s = 20,000 seconds

Therefore, it would take approximately 20,000 seconds or 5.56 hours to transfer 20TB of data over a 1 GB dedicated AWS Direct Connect.

upvoted 1 times

 **potomac** 3 weeks, 2 days ago

Selected Answer: A

C is wrong, GPU is not needed

upvoted 1 times

 **Ramdi1** 1 month, 3 weeks ago

Selected Answer: A

Has to be A. the option for D would only work if they said they have like 6 Months plus. It would take too long to set up.

upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: A

I agreed with A.

Why not D.?

When you initiate the process by requesting an AWS Direct Connect connection, it typically starts with the AWS Direct Connect provider. This provider may need to coordinate with AWS to allocate the necessary resources. This initial setup phase can take anywhere from a few days to a

couple of weeks.
Couple of weeks? No Good
upvoted 2 times

✉ **Guru4Cloud** 3 months ago

When you create a Snowball job in the AWS console, it will estimate the delivery date based on your location. Being near a facility shows 1-2 day estimated delivery.
For extremely urgent requests, you can contact AWS Support and inquire about expedited Snowball delivery. If inventory is available, they may be able to ship same day or next day.
upvoted 1 times

✉ **james2033** 4 months, 1 week ago

Selected Answer: A

Keyword "20 TB", choose "AWS Snowball", there are A or C. C has word "GPU" what is not related, therefore choose A.
upvoted 2 times

✉ **Zox42** 4 months, 3 weeks ago

Selected Answer: A

Answer A
upvoted 1 times

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

Selected Answer: D

D is correct
upvoted 1 times

✉ **DrWatson** 5 months, 3 weeks ago

Selected Answer: A

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_LargeDBs.Process.html
upvoted 1 times

✉ **RoroJ** 6 months ago

Selected Answer: A

D Direct Connection will need a long time to setup plus need to deal with Network and Security changes with existing environment. Ad then plus the Data trans time... No way can be done in 2 weeks.
upvoted 4 times

✉ **Joselucho38** 6 months, 1 week ago

Selected Answer: D

Overall, option D combines the reliability and cost-effectiveness of AWS Direct Connect, AWS DMS, and AWS SCT to migrate the database efficiently and minimize downtime.
upvoted 2 times

✉ **Abhineet9148232** 6 months, 1 week ago

Selected Answer: A

D - Direct Connect takes atleast a month to setup! Requirement is for within 2 weeks.
upvoted 4 times

✉ **Rob1L** 6 months, 1 week ago

Selected Answer: D

AWS Snowball Edge Storage Optimized device is used for large-scale data transfers, but the lead time for delivery, data transfer, and return shipping would likely exceed the 2-week time frame. Also, ongoing database changes wouldn't be replicated while the device is in transit.
upvoted 1 times

✉ **Rob1L** 6 months, 1 week ago

Change to A because "Most cost effective"
upvoted 2 times

✉ **hiroohiroo** 6 months, 1 week ago

Selected Answer: A

https://docs.aws.amazon.com/ja_jp/snowball/latest/developer-guide/device-differences.html#device-options
Aです。
upvoted 2 times

✉ **norris81** 6 months, 2 weeks ago

Selected Answer: A

How long does direct connect take to provision ?
upvoted 2 times

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

At least one month and expensive.
upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: A

- A) 300 first 10 days. 150 shipping
- D) 750 for 2 weeks

upvoted 4 times

 **Efren** 6 months, 2 weeks ago

Thanks, i was checking the speed more than price. Thanks for the clarification

upvoted 1 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: D

- 20 TB 1G/S would take around 44 hours. I guess it takes less than snow devices to receive and send it back

upvoted 1 times

 **Efren** 6 months, 2 weeks ago

Wrong myself, i was checking time, but not price

upvoted 1 times

A company moved its on-premises PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. The company successfully launched a new product. The workload on the database has increased. The company wants to accommodate the larger workload without adding infrastructure.

Which solution will meet these requirements MOST cost-effectively?

- A. Buy reserved DB instances for the total workload. Make the Amazon RDS for PostgreSQL DB instance larger.
- B. Make the Amazon RDS for PostgreSQL DB instance a Multi-AZ DB instance.
- C. Buy reserved DB instances for the total workload. Add another Amazon RDS for PostgreSQL DB instance.
- D. Make the Amazon RDS for PostgreSQL DB instance an on-demand DB instance.

Correct Answer: A

Community vote distribution

A (80%)	13%	7%
---------	-----	----

✉  **elmogy**  6 months ago

Selected Answer: A

A.
"without adding infrastructure" means scaling vertically and choosing larger instance.
"MOST cost-effectively" reserved instances
upvoted 7 times

✉  **wsdasdasdqwdaw** 1 month, 1 week ago

"MOST cost-effectively" doesn't mean reserved instances. Only in this case it is but not in general.
upvoted 1 times

✉  **Goutham4981**  1 week, 4 days ago

Selected Answer: A

Cannot add more infrastructure - C is invalid
Multi AZ DB instance is for high availability and failure mitigation, does not increase performance, higher workload support - B is invalid
On demand instances are costlier than Reserved instances - D is invalid
upvoted 1 times

✉  **bogobob** 1 week, 5 days ago

Selected Answer: D

Not A : "launched a new product", reserved instances are for known workloads, a new product doesn't have known workload.
Not B : "accommodate the larger workload", while Multi-AZ can help with larger workloads, they are more for higher availability.
Not C : "without adding infrastructure", adding a PostgresQL instance is new infrastructure.
upvoted 1 times

✉  **Guru4Cloud** 3 months ago

Selected Answer: B

B is the best approach in this scenario overall:

Making the RDS PostgreSQL instance Multi-AZ adds a standby replica to handle larger workloads and provides high availability.
Even though it adds infrastructure, the cost is less than doubling the infrastructure with a separate DB instance.
It provides better performance, availability, and disaster recovery than a single larger instance.
upvoted 2 times

✉  **BillyBlunts** 1 month, 4 weeks ago

Agreed the answer is B

Multi-AZ deployments are cost-effective because they leverage the standby instance without incurring additional charges. You only pay for the primary instance's regular usage costs.
upvoted 1 times

✉  **james2033** 4 months, 1 week ago

Selected Answer: A

Buy larger instance.
upvoted 1 times

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

Selected Answer: A

Keyword "Amazon RDS for PostgreSQL instance large" . See list of size of instance at <https://aws.amazon.com/rds/instance-types/>

upvoted 1 times

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

Selected Answer: A

A.

Not C: without adding infrastructure

upvoted 2 times

✉️  **EA100** 6 months, 1 week ago

Answer - C

Option B, making the Amazon RDS for PostgreSQL DB instance a Multi-AZ DB instance, would provide high availability and fault tolerance but may not directly address the need for increased capacity to handle the larger workload.

Therefore, the recommended solution is Option C: Buy reserved DB instances for the workload and add another Amazon RDS for PostgreSQL DB instance to accommodate the increased workload in a cost-effective manner.

upvoted 1 times

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

C

Option C: buying reserved DB instances for the total workload and adding another Amazon RDS for PostgreSQL DB instance seems to be the most appropriate choice. It allows for workload distribution across multiple instances, providing scalability and potential performance improvements. Additionally, reserved instances can provide cost savings in the long term.

upvoted 1 times

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

A for me, because without adding additional infrastructure

upvoted 3 times

✉️  **th3k33n** 6 months, 2 weeks ago

Should be C

upvoted 1 times

✉️  **Efren** 6 months, 2 weeks ago

That would add more infrastructure. A would increase the size, keeping the number of instances, i think

upvoted 1 times

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

Option A involves making the existing Amazon RDS for PostgreSQL DB instance larger. While this can improve performance, it may not be sufficient to handle a significantly increased workload. It also doesn't distribute the workload or provide scalability.

upvoted 1 times

✉️  **nonsense** 6 months, 1 week ago

The main not HA, cost-effectively and without adding infrastructure

upvoted 1 times

✉️  **omoakin** 6 months ago

A is the best

upvoted 1 times

A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.

What should a solutions architect recommend?

- A. Deploy Amazon Inspector and associate it with the ALB.
- B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
- C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
- D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Correct Answer: B

Community vote distribution

B (90%) 5%

✉️  **Guru4Cloud** 3 months ago

Selected Answer: A

This case is A

upvoted 1 times

✉️  **james2033** 4 months, 1 week ago

Selected Answer: B

AWS Web Application Firewall (WAF) + ALB (Application Load Balancer) See image at <https://aws.amazon.com/waf/> .
<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-responding.html> .

Question keyword "high request rate", answer keyword "rate-limiting rule" <https://docs.aws.amazon.com/waf/latest/developerguide/waf-rate-based-example-limit-login-page-keys.html>

Amazon GuardDuty for threat detection <https://aws.amazon.com/guardduty/> , not for DDoS.

upvoted 1 times

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

Selected Answer: B

As no shield protect here so WAF rate limit

upvoted 4 times

✉️  **hydro143** 1 month, 3 weeks ago

Where's your Shield Advanced now, in your hour of need he has abandoned you

upvoted 1 times

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

Selected Answer: B

B in swahili 'ba' :)

external systems, incoming requests = AWS WAF

upvoted 1 times

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

Selected Answer: B

layer 7 DDoS protection with WAF

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-get-started-web-acl-rbr.html>

upvoted 1 times

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

Selected Answer: B

B no doubt.

upvoted 1 times

✉️  **Joselucho38** 6 months, 1 week ago

Selected Answer: B

AWS WAF (Web Application Firewall) is a service that provides protection for web applications against common web exploits. By associating AWS WAF with the Application Load Balancer (ALB), you can inspect incoming traffic and define rules to allow or block requests based on various

criteria.

upvoted 4 times

 **cloudenthusiast** 6 months, 2 weeks ago

B

AWS Web Application Firewall (WAF) is a service that helps protect web applications from common web exploits and provides advanced security features. By deploying AWS WAF and associating it with the ALB, the company can set up rules to filter and block incoming requests based on specific criteria, such as IP addresses.

In this scenario, the company is facing performance issues due to a high request rate from illegitimate external systems with changing IP addresses. By configuring a rate-limiting rule in AWS WAF, the company can restrict the number of requests coming from each IP address, preventing excessive traffic from overwhelming the website. This will help mitigate the impact of potential DDoS attacks and ensure that legitimate users can access the site without interruption.

upvoted 3 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: B

If not AWS Shield, then WAF

upvoted 3 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

B obv for this

upvoted 3 times

 **Efren** 6 months, 2 weeks ago

My mind slipped with AWS Shield. GuardDuty can be working along with WAF for DDOS attack, but ultimately would be WAF

<https://aws.amazon.com/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/>

upvoted 2 times

 **Mia2009687** 4 months, 2 weeks ago

Same here, I was looking for AWS Shield

upvoted 1 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: D

D, Guard Duty for me

upvoted 1 times

A company wants to share accounting data with an external auditor. The data is stored in an Amazon RDS DB instance that resides in a private subnet. The auditor has its own AWS account and requires its own copy of the database.

What is the MOST secure way for the company to share the database with the auditor?

- A. Create a read replica of the database. Configure IAM standard database authentication to grant the auditor access.
- B. Export the database contents to text files. Store the files in an Amazon S3 bucket. Create a new IAM user for the auditor. Grant the user access to the S3 bucket.
- C. Copy a snapshot of the database to an Amazon S3 bucket. Create an IAM user. Share the user's keys with the auditor to grant access to the object in the S3 bucket.
- D. Create an encrypted snapshot of the database. Share the snapshot with the auditor. Allow access to the AWS Key Management Service (AWS KMS) encryption key.

Correct Answer: D

Community vote distribution

D (100%)

 **alexandercamachop** Highly Voted  5 months, 3 weeks ago

Selected Answer: D

The most secure way for the company to share the database with the auditor is option D: Create an encrypted snapshot of the database, share the snapshot with the auditor, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

By creating an encrypted snapshot, the company ensures that the database data is protected at rest. Sharing the encrypted snapshot with the auditor allows them to have their own copy of the database securely.

In addition, granting access to the AWS KMS encryption key ensures that the auditor has the necessary permissions to decrypt and access the encrypted snapshot. This allows the auditor to restore the snapshot and access the data securely.

This approach provides both data protection and access control, ensuring that the database is securely shared with the auditor while maintaining the confidentiality and integrity of the data.

upvoted 9 times

 **TariqKipkemei** 5 months, 2 weeks ago

best explanation ever

upvoted 2 times

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

Selected Answer: D

MOST secure way

upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: D

Key word: "Secure way"

The snapshot contents are encrypted using KMS keys for data security.

Sharing the snapshot directly removes risks of extracting/transferring data.

The auditor can restore the snapshot into their own RDS instance.

Access is controlled through sharing the encrypted snapshot and KMS key.

upvoted 2 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: D

Most likely D.

upvoted 2 times

 **cloudenthusiast** 6 months, 2 weeks ago

Option D (Creating an encrypted snapshot of the database, sharing the snapshot, and allowing access to the AWS Key Management Service encryption key) is generally considered a better option for sharing the database with the auditor in terms of security and control.

upvoted 2 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: D

D for me

upvoted 2 times

A solutions architect configured a VPC that has a small range of IP addresses. The number of Amazon EC2 instances that are in the VPC is increasing, and there is an insufficient number of IP addresses for future workloads.

Which solution resolves this issue with the LEAST operational overhead?

- A. Add an additional IPv4 CIDR block to increase the number of IP addresses and create additional subnets in the VPC. Create new resources in the new subnets by using the new CIDR.
- B. Create a second VPC with additional subnets. Use a peering connection to connect the second VPC with the first VPC. Update the routes and create new resources in the subnets of the second VPC.
- C. Use AWS Transit Gateway to add a transit gateway and connect a second VPC with the first VPC. Update the routes of the transit gateway and VPCs. Create new resources in the subnets of the second VPC.
- D. Create a second VPC. Create a Site-to-Site VPN connection between the first VPC and the second VPC by using a VPN-hosted solution on Amazon EC2 and a virtual private gateway. Update the route between VPCs to the traffic through the VPN. Create new resources in the subnets of the second VPC.

Correct Answer: A

Community vote distribution

A (100%)

 **potomac** 3 weeks, 2 days ago

Selected Answer: A

After you've created your VPC, you can associate additional IPv4 CIDR blocks with the VPC
upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: A

the architect just needs to:

Add the CIDR using the AWS console or CLI
Create new subnets in the VPC using the new CIDR
Launch resources in the new subnets
upvoted 2 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: A

A is best
upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: A

A is correct: You assign a single CIDR IP address range as the primary CIDR block when you create a VPC and can add up to four secondary CIDR blocks after creation of the VPC.
upvoted 3 times

 **Yadav_Sanjay** 6 months, 1 week ago

Selected Answer: A

Add additional CIDR of bigger range
upvoted 2 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: A

Add new bigger subnets
upvoted 2 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: A

A valid
upvoted 1 times

A company used an Amazon RDS for MySQL DB instance during application testing. Before terminating the DB instance at the end of the test cycle, a solutions architect created two backups. The solutions architect created the first backup by using the mysqldump utility to create a database dump. The solutions architect created the second backup by enabling the final DB snapshot option on RDS termination.

The company is now planning for a new test cycle and wants to create a new DB instance from the most recent backup. The company has chosen a MySQL-compatible edition of Amazon Aurora to host the DB instance.

Which solutions will create the new DB instance? (Choose two.)

- A. Import the RDS snapshot directly into Aurora.
- B. Upload the RDS snapshot to Amazon S3. Then import the RDS snapshot into Aurora.
- C. Upload the database dump to Amazon S3. Then import the database dump into Aurora.
- D. Use AWS Database Migration Service (AWS DMS) to import the RDS snapshot into Aurora.
- E. Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora.

Correct Answer: AD

Community vote distribution

AC (70%) 10% 10% 5%

✉  **oras2023**  6 months ago

Selected Answer: AC

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Import.html>
upvoted 5 times

✉  **Axaus**  6 months, 2 weeks ago

Selected Answer: AC

A,C
A because the snapshot is already stored in AWS.
C because you dont need a migration tool going from MySQL to MySQL. You would use the MySQL utility.
upvoted 5 times

✉  **potomac**  3 weeks, 2 days ago

Selected Answer: AD

A and C
upvoted 1 times

✉  **TariqKipkemei** 1 month ago

Selected Answer: AC

Either import the RDS snapshot directly into Aurora or upload the database dump to Amazon S3, then import the database dump into Aurora.
upvoted 1 times

✉  **thanhnv142** 1 month, 1 week ago

AC:
- store dump in s3 then upload to aurora
- no need to store snapshot in s3 because is in AWS already
upvoted 1 times

✉  **Guru4Cloud** 3 months ago

Selected Answer: CE

C and E are the solutions that can restore the backups into Amazon Aurora.

The RDS DB snapshot contains backup data in a proprietary format that cannot be directly imported into Aurora.
The mysqldump database dump contains SQL statements that can be imported into Aurora after uploading to S3.
AWS DMS can migrate the dump file from S3 into Aurora.
upvoted 2 times

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

Selected Answer: AC

Amazon RDS for MySQL --> Amazon Aurora MySQL-compatible.

* mysqldump, database dump --> (C) Upload to Amazon S3, Import dump to Aurora.

* DB snapshot --> (A) Import RDS Snapshot directly Aurora. The correct word should be "migration". "Use console to migrate the DB snapshot and

create an Aurora MySQL DB cluster with the same databases as the original MySQL DB instance."

Exclude B, because no need upload DB snapshot to Amazon S3. Exclude D, because no need Migration service. Exclude E, because no need Migration service. Use exclusion method is more easy for this question.

Related links:

- Amazon RDS create database snapshot https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_CreateSnapshot.html
 - <https://aws.amazon.com/rds/aurora/>
- upvoted 1 times

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

CE

Since the backup created by the solutions architect was a database dump using the mysqldump utility, it cannot be directly imported into Aurora using RDS snapshots. Amazon Aurora has its own specific backup format that is different from RDS snapshots

upvoted 2 times

✉ **Guru4Cloud** 3 months ago

C and E are the solutions that can restore the backups into Amazon Aurora.

The RDS DB snapshot contains backup data in a proprietary format that cannot be directly imported into Aurora.

The mysqldump database dump contains SQL statements that can be imported into Aurora after uploading to S3.

AWS DMS can migrate the dump file from S3 into Aurora.

upvoted 1 times

✉ **antropaws** 5 months, 3 weeks ago

Selected Answer: AC

Migrating data from MySQL by using an Amazon S3 bucket

You can copy the full and incremental backup files from your source MySQL version 5.7 database to an Amazon S3 bucket, and then restore an Amazon Aurora MySQL DB cluster from those files.

This option can be considerably faster than migrating data using mysqldump, because using mysqldump replays all of the commands to recreate the schema and data from your source database in your new Aurora MySQL DB cluster.

By copying your source MySQL data files, Aurora MySQL can immediately use those files as the data for an Aurora MySQL DB cluster.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.ExtMySQL.html>

upvoted 2 times

✉ **omoakin** 6 months, 2 weeks ago

BE

Upload the RDS snapshot to Amazon S3. Then import the RDS snapshot into Aurora.

Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora

upvoted 1 times

✉ **Efren** 6 months, 2 weeks ago

Selected Answer: BC

I'd say B and C

You can create a dump of your data using the mysqldump utility, and then import that data into an existing Amazon Aurora MySQL DB cluster.

c>- Because Amazon Aurora MySQL is a MySQL-compatible database, you can use the mysqldump utility to copy data from your MySQL or MariaDB database to an existing Amazon Aurora MySQL DB cluster.

B.- You can copy the source files from your source MySQL version 5.5, 5.6, or 5.7 database to an Amazon S3 bucket, and then restore an Amazon Aurora MySQL DB cluster from those files.

upvoted 2 times

✉ **nonsense** 6 months, 2 weeks ago

Selected Answer: BE

Rds required upload to s3

upvoted 1 times

✉ **nonsense** 6 months, 2 weeks ago

in the end, apparently the A and C.

- a) because it creates a new DB
- b) no sense to load in s3. can directly
- c) yes, creates a new inst
- d and e migration

upvoted 1 times

✉ **nonsense** 6 months, 2 weeks ago

If too be honestly can't decide between be and bc...

upvoted 1 times

✉ **Guru4Cloud** 3 months ago

using the mysqldump database dump provide valid solutions to restore into Aurora. Options A, B, and D using the RDS snapshot cannot directly restore into Aurora.

upvoted 1 times

Question #441

Topic 1

A company hosts a multi-tier web application on Amazon Linux Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The company observes that the Auto Scaling group launches more On-Demand Instances when the application's end users access high volumes of static web content. The company wants to optimize cost.

What should a solutions architect do to redesign the application MOST cost-effectively?

- A. Update the Auto Scaling group to use Reserved Instances instead of On-Demand Instances.
- B. Update the Auto Scaling group to scale by launching Spot Instances instead of On-Demand Instances.
- C. Create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket.
- D. Create an AWS Lambda function behind an Amazon API Gateway API to host the static website contents.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Guru4Cloud** 3 months ago

Selected Answer: C

implementing CloudFront to serve static content is the most cost-optimal architectural change for this use case.

upvoted 1 times

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

Selected Answer: C

Keyword "Amazon CloudFront", "high volumes of static web content", choose C.

upvoted 1 times

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

Selected Answer: C

static web content = Amazon CloudFront

upvoted 1 times

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

Selected Answer: C

Static Web Content = S3 Always.

CloudFront = Closer to the users locations since it will cache in the Edge nodes.

upvoted 1 times

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

By leveraging Amazon CloudFront, you can cache and serve the static web content from edge locations worldwide, reducing the load on your EC2 instances. This can help lower the number of On-Demand Instances required to handle high volumes of static web content requests. Storing the static content in an Amazon S3 bucket and using CloudFront as a content delivery network (CDN) improves performance and reduces costs by reducing the load on your EC2 instances.

upvoted 2 times

✉  **Efren** 6 months, 2 weeks ago

Selected Answer: C

Static content, cloudFront plus S3

upvoted 2 times

✉  **nonsense** 6 months, 2 weeks ago

Selected Answer: C

c for me

upvoted 1 times

A company stores several petabytes of data across multiple AWS accounts. The company uses AWS Lake Formation to manage its data lake. The company's data science team wants to securely share selective data from its accounts with the company's engineering team for analytical purposes.

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

- A. Copy the required data to a common account. Create an IAM access role in that account. Grant access by specifying a permission policy that includes users from the engineering team accounts as trusted entities.
- B. Use the Lake Formation permissions Grant command in each account where the data is stored to allow the required engineering team users to access the data.
- C. Use AWS Data Exchange to privately publish the required data to the required engineering team accounts.
- D. Use Lake Formation tag-based access control to authorize and grant cross-account permissions for the required data to the engineering team accounts.

Correct Answer: D

Community vote distribution

D (100%)

 **clouduenthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: D

By utilizing Lake Formation's tag-based access control, you can define tags and tag-based policies to grant selective access to the required data for the engineering team accounts. This approach allows you to control access at a granular level without the need to copy or move the data to a common account or manage permissions individually in each account. It provides a centralized and scalable solution for securely sharing data across accounts with minimal operational overhead.

upvoted 8 times

 **Guru4Cloud** Most Recent 3 months ago

Selected Answer: D

D is the correct option with the least operational overhead.

Using Lake Formation tag-based access control allows granting cross-account permissions to access data in other accounts based on tags, without having to copy data or configure individual permissions in each account.

This provides a centralized, tag-based way to share selective data across accounts to authorized users with least operational overhead.

upvoted 1 times

 **luisgu** 6 months, 1 week ago

Selected Answer: D

<https://aws.amazon.com/blogs/big-data/securing-share-your-data-across-aws-accounts-using-aws-lake-formation/>

upvoted 3 times

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Correct Answer: A

Community vote distribution

A (54%)

C (46%)

 **Goutham4981** 1 week, 4 days ago

Selected Answer: A

Downloading data upto gigabytes in size - Cloudfront is a content delivery service that acts as an edge caching layer for images and other data. Not a service that minimizes upload and download latency.

upvoted 1 times

 **potomac** 3 weeks, 2 days ago

Selected Answer: A

The question is focused on large downloads and uploads. S3 Transfer Acceleration is what fits. CloudFront is for caching which cannot be used when the data is unique. They aren't as concerned with regular web traffic.

C didn't mention S3. Where the data is stored?

upvoted 1 times

 **beast2091** 3 weeks, 6 days ago

It is A.

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

upvoted 1 times

 **danielmakita** 1 month ago

It is A as the Transfer Acceleration will minimize upload and download latency.

If you choose C, where would the files be stored? There is no mention of any S3. Will it be stored inside the EC2? That's why I didn't go for C
upvoted 3 times

 **Sindokuhlep** 1 month ago

Selected Answer: C

Amazon S3 with Transfer Acceleration (option A) is designed for speeding up uploads to Amazon S3, and it's not used for hosting scalable web applications. It doesn't mention using EC2 instances for hosting the application.

upvoted 1 times

 **canonlycontainletters1** 1 month ago

Selected Answer: C

My answer is C

upvoted 1 times

 **chris0975** 1 month, 1 week ago

Selected Answer: A

The question is focused on large downloads and uploads. S3 Transfer Acceleration is what fits. CloudFront is for caching which cannot be used when the data is unique. They aren't as concerned with regular web traffic.

Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects.

upvoted 3 times

 **thanhnv142** 1 month, 1 week ago

C because A is for upload data to S3, not for web app

upvoted 1 times

 **DamyanG** 1 month, 2 weeks ago

Selected Answer: C

The correct answer is C!!! It is not A, because

- Amazon S3 with Transfer Acceleration (option A) is designed for speeding up uploads to Amazon S3, and it's not used for hosting scalable web applications. It doesn't mention using EC2 instances for hosting the application.

upvoted 1 times

 **Victory007** 1 month, 3 weeks ago

Selected Answer: C

Amazon CloudFront is a global content delivery network (CDN) that delivers web content to users with low latency and high transfer speeds. It does this by caching content at edge locations around the world, which are closer to the users than the origin server.

By using Amazon EC2 with Auto Scaling and Amazon CloudFront, the company can create a scalable and high-performance web application that is accessible to users from different geographic regions of the world.

upvoted 1 times

 **Ramdi1** 1 month, 3 weeks ago

Selected Answer: A

I believe it would be A - my thinking maybe wrong but im just thinking specifically about the S3 put allows upto 5gb not sure about cloudfront. Second way of thinking is that cached content on edge locations but would it not have to go to source still to retrieve if another person wants to download that content in a different part of the world?

upvoted 2 times

 **bsbs1234** 1 month, 4 weeks ago

C,

1. Cloudfront cache data at edge, which provide better performance for read. Global Accelerator will always goto origin for content.
2. Cloudfront can also help performance for dynamic content, which is good for Web app

upvoted 1 times

 **Ramdi1** 2 months ago

Selected Answer: C

I think C is correct the question mentions geographic locations and cloudfront had 500 + edge locations. Gigabytes in size - s3 has a max limit of a 5gb put - even though the question does not say 5gb or less just something to think about and s3 cant hold dynamic content

upvoted 2 times

 **garuta** 2 months ago

Selected Answer: A

S3TA shortens the distance between client applications and AWS servers that acknowledge PUTS and GETS to Amazon S3 using our global network of hundreds of CloudFront Edge Locations. We automatically route your uploads and downloads through the closest Edge Locations to your application.

upvoted 1 times

 **nnecode** 2 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

 **CHOTADON** 2 months, 2 weeks ago

Selected Answer: C

I think C is correct as it provides caching at edge which minimizes latency

upvoted 1 times

 **Hades2231** 3 months ago

Selected Answer: C

Should be C, I will never host a "scalable application" using S3. They might be fast in data transfer but that is not the whole point

upvoted 1 times

A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone.

An employee recently deleted the DB instance, and the application was unavailable for 24 hours as a result. The company is concerned with the overall reliability of its environment.

What should the solutions architect do to maximize reliability of the application's infrastructure?

- A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.
- B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.
- C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.
- D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On-Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances. Update the DB instance to be Multi-AZ, and enable deletion protection.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: B

The key points:

- RDS Multi-AZ and deletion protection provide high availability for the database.
- The load balancer and Auto Scaling group across AZs give high availability for EC2.
- Options A, C, D have limitations that would reduce reliability vs option B.

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: B

Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones

upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: B

B for sure.

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: B

It is the only one with High Availability.

Amazon RDS with Multi AZ

EC2 with Auto Scaling Group in Multi Az

upvoted 1 times

 **omoakin** 6 months, 2 weeks ago

same question from

<https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-associate-saa-c02/>

long time ago and still same option B

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

B is correct. HA ensured by DB in Multi-AZ and EC2 in AG

upvoted 4 times

A company is storing 700 terabytes of data on a large network-attached storage (NAS) system in its corporate data center. The company has a hybrid environment with a 10 Gbps AWS Direct Connect connection.

After an audit from a regulator, the company has 90 days to move the data to the cloud. The company needs to move the data efficiently and without disruption. The company still needs to be able to access and update the data during the transfer window.

Which solution will meet these requirements?

- A. Create an AWS DataSync agent in the corporate data center. Create a data transfer task Start the transfer to an Amazon S3 bucket.
- B. Back up the data to AWS Snowball Edge Storage Optimized devices. Ship the devices to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.
- C. Use rsync to copy the data directly from local storage to a designated Amazon S3 bucket over the Direct Connect connection.
- D. Back up the data on tapes. Ship the tapes to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: A

AWS DataSync can efficiently transfer large datasets from on-premises NAS to Amazon S3 over Direct Connect.

DataSync allows accessing and updating the data continuously during the transfer process.

upvoted 1 times

 **hsinchang** 4 months ago

Selected Answer: A

Access during the transfer window -> DataSync

upvoted 2 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: A

AWS DataSync is a secure, online service that automates and accelerates moving data between on premises and AWS Storage services.

upvoted 1 times

 **wRhlH** 5 months, 2 weeks ago

For those who wonders why not B. Snowball Edge Storage Optimized device for data transfer is up to 100TB
<https://docs.aws.amazon.com/snowball/latest/developer-guide/device-differences.html>

upvoted 4 times

 **smartegnine** 5 months, 1 week ago

10GBs * 24*60*60 =864,000 GB estimate around 864 TB a day, 2 days will transfer all data. But for snowball at least 4 days for delivery to the data center.

upvoted 1 times

 **siGma182** 4 months, 1 week ago

This account is wrong but I get your point. It is wrong cause 10Gb/s is not the same as 10GB/s (Gigabits vs Gigabytes). However, the correct count is 864Tb/8 = 108TB per day. In one week you should've transferred all the data.

upvoted 3 times

 **omoakin** 6 months, 2 weeks ago

A

<https://www.examtopics.com/discussions/amazon/view/46492-exam-aws-certified-solutions-architect-associate-saa-c02/#:~:text=Exam%20question%20from,Question%20%23%3A%20385>

upvoted 1 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: A

By leveraging AWS DataSync in combination with AWS Direct Connect, the company can efficiently and securely transfer its 700 terabytes of data to an Amazon S3 bucket without disruption. The solution allows continued access and updates to the data during the transfer window, ensuring business continuity throughout the migration process.

upvoted 2 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: A

A for me, bcs egde storage up to 100tb

upvoted 4 times

A company stores data in PDF format in an Amazon S3 bucket. The company must follow a legal requirement to retain all new and existing data in Amazon S3 for 7 years.

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

- A. Turn on the S3 Versioning feature for the S3 bucket. Configure S3 Lifecycle to delete the data after 7 years. Configure multi-factor authentication (MFA) delete for all S3 objects.
- B. Turn on S3 Object Lock with governance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.
- C. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.
- D. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Use S3 Batch Operations to bring the existing data into compliance.

Correct Answer: C

Community vote distribution

D (79%)	C (21%)
---------	---------

 **moonster** 2 weeks, 1 day ago

Its C because you only need to recopy all existing objects one time, so why use S3 batch operations if new data is going to be in compliance retention mode? I can see why its C although my initial gut answer was D.

upvoted 2 times

 **kwang312** 2 months, 2 weeks ago

You can only enable Object Lock for new buckets. If you want to turn on Object Lock for an existing bucket, contact AWS Support.

upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: D

Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Use S3 Batch Operations to bring the existing data into compliance.

upvoted 1 times

 **MrAWSAssociate** 5 months, 2 weeks ago

Selected Answer: D

To replicate existing object/data in S3 Bucket to bring them to compliance, optionally we use "S3 Batch Replication", so option D is the most appropriate, especially if we have big data in S3.

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: D

For minimum ops D is best

upvoted 1 times

 **DrWatson** 5 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-retention-date.html>

upvoted 2 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: C

Batch operations will add operational overhead.

upvoted 3 times

 **Abrar2022** 5 months, 4 weeks ago

Use Object Lock in Compliance mode. Then Use Batch operation.

WRONG>>manual work and not automated>>>Recopy all existing objects to bring the existing data into compliance.

upvoted 1 times

 **omoakin** 6 months, 2 weeks ago

C

When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode

helps ensure that an object version can't be overwritten or deleted for the duration of the retention period.

upvoted 3 times

✉️ **lucdt4** 6 months, 1 week ago

No, D for me because the requirement is LEAST operational overhead

So RECOPY is the manual operation -> C is wrong

D is correct

upvoted 2 times

✉️ **omoakin** 6 months, 2 weeks ago

error i meant to type D

i wont do recopy

upvoted 1 times

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

Recopying vs. S3 Batch Operations: In Option C, the recommendation is to recopy all existing objects to ensure they have the appropriate retention settings. This can be done using simple S3 copy operations. On the other hand, Option D suggests using S3 Batch Operations, which is a more advanced feature and may require additional configuration and management. S3 Batch Operations can be beneficial if you have a massive number of objects and need to perform complex operations, but it might introduce more overhead for this specific use case.

Operational complexity: Option C has a straightforward process of recopying existing objects. It is a well-known operation in S3 and doesn't require additional setup or management. Option D introduces the need to set up and configure S3 Batch Operations, which can involve creating job definitions, specifying job parameters, and monitoring the progress of batch operations. This additional complexity may increase the operational overhead.

upvoted 2 times

✉️ **Efren** 6 months, 2 weeks ago

Selected Answer: D

You need AWS Batch to re-apply certain config to files that were already in S3, like encryption

upvoted 4 times

✉️ **nonsense** 6 months, 2 weeks ago

Selected Answer: D

D for me, bcs no sense to recopy all data

upvoted 2 times

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

But D will introduce operation overhead

upvoted 1 times

A company has a stateless web application that runs on AWS Lambda functions that are invoked by Amazon API Gateway. The company wants to deploy the application across multiple AWS Regions to provide Regional failover capabilities.

What should a solutions architect do to route traffic to multiple Regions?

- A. Create Amazon Route 53 health checks for each Region. Use an active-active failover configuration.
- B. Create an Amazon CloudFront distribution with an origin for each Region. Use CloudFront health checks to route traffic.
- C. Create a transit gateway. Attach the transit gateway to the API Gateway endpoint in each Region. Configure the transit gateway to route requests.
- D. Create an Application Load Balancer in the primary Region. Set the target group to point to the API Gateway endpoint hostnames in each Region.

Correct Answer: A

Community vote distribution

A (83%)

B (18%)

 **examtopicempacc** Highly Voted 6 months, 1 week ago

Selected Answer: A

A. I'm not an expert in this area, but I still want to express my opinion. After carefully reviewing the question and thinking about it for a long time, I actually don't know the reason. As I mentioned at the beginning, I'm not an expert in this field.

upvoted 12 times

 **TariqKipkemei** Highly Voted 5 months, 2 weeks ago

Selected Answer: A

Global, Reduce latency, health checks, no failover = Amazon CloudFront

Global ,Reduce latency, health checks, failover, Route traffic = Amazon Route 53
option A has more weight.

upvoted 7 times

 **Anmol_1010** 1 month, 1 week ago

nicley explained

upvoted 1 times

 **Goutham4981** Most Recent 1 week, 4 days ago

Selected Answer: A

In activ active failover config, route53 continuously monitors its endpoints and if one of them is unhealthy, it excludes the region/endpoint from its valid traffic route - Only Sensible option

Cloudfront is a content delivery network - not used to route traffic

Transit gateway for traffic routing - aws devs will hit us with a stick on hearing this option

You cant use a load balancer for cross region load balancing - invalid

upvoted 1 times

 **potomac** 3 weeks, 2 days ago

Selected Answer: A

Global ,Reduce latency, health checks, failover, Route traffic = Amazon Route 53

upvoted 1 times

 **youdelin** 1 month, 2 weeks ago

"What the?" yeah I know right

upvoted 1 times

 **jrestrepob** 3 months ago

Selected Answer: B

"Stateless applications provide one service or function and use content delivery network (CDN), web, or print servers to process these short-term requests.

<https://docs.aws.amazon.com/architecture-diagrams/latest/multi-region-api-gateway-with-cloudfront/multi-region-api-gateway-with-cloudfront.html>

upvoted 1 times

 **deechean** 2 months, 4 weeks ago

its not static content, actually they deployed a API Gateway backed by lambda

upvoted 1 times

 **MrAWSAssociate** 5 months, 2 weeks ago

Selected Answer: A

A option does make sense.

upvoted 1 times

 **Sangsation** 5 months, 2 weeks ago

Selected Answer: B

By creating an Amazon CloudFront distribution with origins in each AWS Region where the application is deployed, you can leverage CloudFront's global edge network to route traffic to the closest available Region. CloudFront will automatically route the traffic based on the client's location and the health of the origins using CloudFront health checks.

Option A (creating Amazon Route 53 health checks with an active-active failover configuration) is not suitable for this scenario as it is primarily used for failover between different endpoints within the same Region, rather than routing traffic to different Regions.

upvoted 1 times

 **Axeashes** 5 months, 2 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/compute/building-a-multi-region-serverless-application-with-amazon-api-gateway-and-aws-lambda/>

upvoted 3 times

 **Gooniegoogoo** 5 months ago

that is from 2017.. i wonder if it is still relevant..

upvoted 1 times

 **DrWatson** 5 months, 3 weeks ago

Selected Answer: A

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

upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: A

I understand that you can use Route 53 to provide regional failover.

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: A

To route traffic to multiple AWS Regions and provide regional failover capabilities for a stateless web application running on AWS Lambda functions invoked by Amazon API Gateway, you can use Amazon Route 53 with an active-active failover configuration.

By creating Amazon Route 53 health checks for each Region and configuring an active-active failover configuration, Route 53 can monitor the health of the endpoints in each Region and route traffic to healthy endpoints. In the event of a failure in one Region, Route 53 automatically routes traffic to the healthy endpoints in other Regions.

This setup ensures high availability and failover capabilities for your web application across multiple AWS Regions.

upvoted 2 times

 **udo2020** 5 months, 4 weeks ago

I think it's A because the keyword is "route" traffic.

upvoted 2 times

 **omoakin** 6 months ago

BBBBBBBBBBBBBBB

upvoted 1 times

 **karbob** 6 months ago

CloudFront does not support health checks for routing traffic. It is designed primarily for content distribution and caching, rather than for load balancing or traffic routing based on health checks.

upvoted 1 times

 **Rob1L** 6 months, 1 week ago

Selected Answer: A

It's A

It's not B because Amazon CloudFront can distribute traffic to multiple origins, but it does not support automatic failover between regions based on health checks. CloudFront is primarily 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 4 times

 **y0** 6 months, 1 week ago

I agree with A - active-active failover means considering resources across all regions. So, in this case, to distribute traffic across all regions, Route 53 seems good. Cloudfront usage is more towards reducing latency for applications used globally by caching content at edge locations. It somehow does not fit the use case for distributing traffic. Also, not sure of the term "cloudfront healthchecks"

upvoted 1 times

 **omoakin** 6 months, 2 weeks ago

A

check this out Qtn 3

<https://dumpsgate.com/wp-content/uploads/2021/01/SAA-C02.pdf>

upvoted 1 times

A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.

What should a solutions architect do to mitigate any single point of failure in this architecture?

- A. Add a set of VPNs between the Management and Production VPCs.
- B. Add a second virtual private gateway and attach it to the Management VPC.
- C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
- D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Correct Answer: C

Community vote distribution

C (100%)

✉  **bsbs1234** 1 month, 4 weeks ago

C,

(production) --PrivateGateway----->Direct Connect Gateway 1 ---> cgw 1 ---> DataCenter
(production) -- PrivateGateway -----> Direct Connect Gateway 2 --->cgw 2 --> DataCenter
(Management) -- > VPN ---- > (Direct Connect Gateway 1?) --- >cgw1 ---> dataCenter---> device in dataCenter
upvoted 1 times

✉  **Guru4Cloud** 3 months ago

Selected Answer: C

C is the correct option to mitigate the single point of failure.

The Management VPC currently has a single VPN connection through one customer gateway device. This is a single point of failure.

Adding a second set of VPN connections from the Management VPC to a second customer gateway device provides redundancy and eliminates this single point of failure.

upvoted 1 times

✉  **Guru4Cloud** 3 months ago

As @Abrar2022 explains

(production) VPN 1-----> cgw 1
(management) VPN 2-----> cgw
upvoted 1 times

✉  **Abrar2022** 5 months, 4 weeks ago

(production) VPN 1-----> cgw 1
(management) VPN 2-----> cgw 2
upvoted 2 times

✉  **Abrar2022** 5 months, 4 weeks ago

ANSWER IS C

upvoted 1 times

✉  **omoakin** 6 months, 2 weeks ago

I agree to C

upvoted 1 times

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

Selected Answer: C

option D is not a valid solution for mitigating single points of failure in the architecture. I apologize for the confusion caused by the incorrect information.

To mitigate single points of failure in the architecture, you can consider implementing option C: adding a second set of VPNs to the Management VPC from a second customer gateway device. This will introduce redundancy at the VPN connection level for the Management VPC, ensuring that if one customer gateway or VPN connection fails, the other connection can still provide connectivity to the data center.

upvoted 2 times

✉  **Efren** 6 months, 2 weeks ago

Selected Answer: C

Redundant VPN connections: Instead of relying on a single device in the data center, the Management VPC should have redundant VPN connections established through multiple customer gateways. This will ensure high availability and fault tolerance in case one of the VPN connections or customer gateways fails.

upvoted 3 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/53908-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company runs its application on an Oracle database. The company plans to quickly migrate to AWS because of limited resources for the database, backup administration, and data center maintenance. The application uses third-party database features that require privileged access.

Which solution will help the company migrate the database to AWS MOST cost-effectively?

- A. Migrate the database to Amazon RDS for Oracle. Replace third-party features with cloud services.
- B. Migrate the database to Amazon RDS Custom for Oracle. Customize the database settings to support third-party features.
- C. Migrate the database to an Amazon EC2 Amazon Machine Image (AMI) for Oracle. Customize the database settings to support third-party features.
- D. Migrate the database to Amazon RDS for PostgreSQL by rewriting the application code to remove dependency on Oracle APEX.

Correct Answer: C

Community vote distribution

B (91%) 9%

 **Guru4Cloud** 3 months ago

Selected Answer: B

Migrate the database to Amazon RDS Custom for Oracle. Customize the database settings to support third-party features.
upvoted 2 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: B

Custom database features = Amazon RDS Custom for Oracle
upvoted 2 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: B

Most likely B.
upvoted 1 times

 **Abrar2022** 5 months, 4 weeks ago

Selected Answer: B

RDS Custom since it's related to 3rd vendor
RDS Custom since it's related to 3rd vendor
RDS Custom since it's related to 3rd vendor
upvoted 2 times

 **omoakin** 6 months ago

CCCCCCCCCC
upvoted 1 times

 **aqmdla2002** 6 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/about-aws/whats-new/2021/10/amazon-rds-custom-oracle/>
upvoted 1 times

 **hiroohiroo** 6 months, 1 week ago

Selected Answer: B

https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/Oracle.Resources.html
upvoted 1 times

 **karbob** 6 months ago

Amazon RDS Custom for Oracle, which is not an actual service. !!!!
upvoted 1 times

 **nonsense** 6 months, 1 week ago

Option C is also a valid solution, but it is not as cost-effective as option B.
Option C requires the company to manage its own database infrastructure, which can be expensive and time-consuming. Additionally, the company will need to purchase and maintain Oracle licenses.
upvoted 2 times

 **y0** 6 months, 1 week ago

RDS Custom enables the capability to access the underlying database and OS so as to configure additional settings to support 3rd party. This feature is applicable only for Oracle and Postgresql

upvoted 1 times

✉  **y0** 6 months, 1 week ago

Sorry Oracle and sql server (not posstgresql)

upvoted 1 times

✉  **omoakin** 6 months, 2 weeks ago

I will say C cos of this
"application uses third-party "

upvoted 1 times

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

Selected Answer: C

Should not it be since for Ec2, the company will have full control over the database and this is the reason that they are moving to AWS in the first place "The company plans to quickly migrate to AWS because of limited resources for the database, backup administration, and data center maintenance?"

upvoted 1 times

✉  **Efren** 6 months, 2 weeks ago

Selected Answer: B

RDS Custom when is something related to 3rd vendor, for me

upvoted 1 times

✉  **nonsense** 6 months, 2 weeks ago

not sure, but b probably

upvoted 2 times

A company has a three-tier web application that is in a single server. The company wants to migrate the application to the AWS Cloud. The company also wants the application to align with the AWS Well-Architected Framework and to be consistent with AWS recommended best practices for security, scalability, and resiliency.

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

- A. Create a VPC across two Availability Zones with the application's existing architecture. Host the application with existing architecture on an Amazon EC2 instance in a private subnet in each Availability Zone with EC2 Auto Scaling groups. Secure the EC2 instance with security groups and network access control lists (network ACLs).
- B. Set up security groups and network access control lists (network ACLs) to control access to the database layer. Set up a single Amazon RDS database in a private subnet.
- C. Create a VPC across two Availability Zones. Refactor the application to host the web tier, application tier, and database tier. Host each tier on its own private subnet with Auto Scaling groups for the web tier and application tier.
- D. Use a single Amazon RDS database. Allow database access only from the application tier security group.
- E. Use Elastic Load Balancers in front of the web tier. Control access by using security groups containing references to each layer's security groups.
- F. Use an Amazon RDS database Multi-AZ cluster deployment in private subnets. Allow database access only from application tier security groups.

Correct Answer: ACF

Community vote distribution

CEF (100%)

✉  **arg1995** 4 months, 3 weeks ago

option A cannot be the answer as Security group is at instance level whereas a NACL is at the subnet level. Having said that option C is the right one as the VPC cannot span across the regions and here it is mentioned two AZs for which I am guessing it is a default VPC which is created in each region with a subnet in each AZ.

upvoted 1 times

✉  **arg1995** 4 months, 3 weeks ago

So, CEF is the right answer

upvoted 1 times

✉  **Gooniegoogoo** 5 months ago

How can you create a VPC across 2 AZ? i only see EF here.. if they mean 2 separate VPC then that is different but a VPC cannot span two AZ..
upvoted 1 times

✉  **lemur88** 3 months ago

A VPC most definitely can span across 2 AZ. You may be thinking of subnets.

upvoted 1 times

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

I also agree with CEF but chatGPT answer is ACE. A and C is the similar
Another Logic F is not True because in the question not mentioned about DB
upvoted 1 times

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

Selected Answer: CEF

CEF is best

upvoted 1 times

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

Selected Answer: CEF

It's clearly CEF.

upvoted 1 times

✉  **Abrar2022** 5 months, 4 weeks ago

Selected Answer: CEF

C-scalable and resilient

E-high availability of the application

F-Multi-AZ configuration provides high availability
upvoted 4 times

✉ **omoakin** 6 months ago

B- to control access to database
C-scalable and resilient
E-high availability of the application
upvoted 1 times

✉ **lucdt4** 6 months, 1 week ago

Selected Answer: CEF

CEF
A: application's existing architecture is wrong (single AZ)
B: single AZ
D: Single AZ
upvoted 2 times

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

C.
This solution follows the recommended architecture pattern of separating the web, application, and database tiers into different subnets. It provides better security, scalability, and fault tolerance.
E.By using Elastic Load Balancers (ELBs), you can distribute traffic to multiple instances of the web tier, increasing scalability and availability. Controlling access through security groups allows for fine-grained control and ensures only authorized traffic reaches each layer.
F.
Deploying an Amazon RDS database in a Multi-AZ configuration provides high availability and automatic failover. Placing the database in private subnets enhances security. Allowing database access only from the application tier security groups limits exposure and follows the principle of least privilege.
upvoted 2 times

✉ **nonsense** 6 months, 2 weeks ago

Selected Answer: CEF

Only this valid for best practices and well architected
upvoted 4 times

A company is migrating its applications and databases to the AWS Cloud. The company will use Amazon Elastic Container Service (Amazon ECS), AWS Direct Connect, and Amazon RDS.

Which activities will be managed by the company's operational team? (Choose three.)

- A. Management of the Amazon RDS infrastructure layer, operating system, and platforms
- B. Creation of an Amazon RDS DB instance and configuring the scheduled maintenance window
- C. Configuration of additional software components on Amazon ECS for monitoring, patch management, log management, and host intrusion detection
- D. Installation of patches for all minor and major database versions for Amazon RDS
- E. Ensure the physical security of the Amazon RDS infrastructure in the data center
- F. Encryption of the data that moves in transit through Direct Connect

Correct Answer: BCF

Community vote distribution

BCF (90%) 10%

 **Guru4Cloud** 3 months ago

Selected Answer: BCF

B: Creating an RDS instance and configuring the maintenance window is done by the customer.

C: Adding monitoring, logging, etc on ECS is managed by the customer.

F: Encrypting Direct Connect traffic is handled by the customer.

upvoted 2 times

 **james2033** 4 months, 1 week ago

Selected Answer: BCF

In question has 3 keyword "Amazon ECS", "AWS Direct Connect", "Amazon RDS". With per Amazon services, choose 1 according answer. Has 6 items, need pick 3 items.

ECS --> choose C.

Direct Connect --> choose F.

RDS --> Exclude A (by keyword "infrastructure layer"), Choose B. Exclusive D (by keyword "patches for all minor and major database versions for Amazon RDS"). Exclusive E (by keyword "Ensure the physical security of the Amazon RDS"). Easy question.

upvoted 1 times

 **kapit** 5 months, 1 week ago

BC & F (no automatic encryption with direct connect

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: BF

Amazon ECS is a fully managed service, the ops team only focus on building their applications, not the environment.
Only option B and F makes sense.

upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: BCF

100% BCF.

upvoted 1 times

 **lucdt4** 6 months, 1 week ago

Selected Answer: BCF

BCF

B: Mentioned RDS

C: Mentioned ECS

F: Mentioned Direct connect

upvoted 2 times

 **hiroohiroo** 6 months, 1 week ago

Selected Answer: BCF

Yes BCF

upvoted 1 times

 **omoakin** 6 months, 2 weeks ago

I agree BCF

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: BCF

Bcf for me

upvoted 2 times

A company runs a Java-based job on an Amazon EC2 instance. The job runs every hour and takes 10 seconds to run. The job runs on a scheduled interval and consumes 1 GB of memory. The CPU utilization of the instance is low except for short surges during which the job uses the maximum CPU available. The company wants to optimize the costs to run the job.

Which solution will meet these requirements?

- A. Use AWS App2Container (A2C) to containerize the job. Run the job as an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate with 0.5 virtual CPU (vCPU) and 1 GB of memory.
- B. Copy the code into an AWS Lambda function that has 1 GB of memory. Create an Amazon EventBridge scheduled rule to run the code each hour.
- C. Use AWS App2Container (A2C) to containerize the job. Install the container in the existing Amazon Machine Image (AMI). Ensure that the schedule stops the container when the task finishes.
- D. Configure the existing schedule to stop the EC2 instance at the completion of the job and restart the EC2 instance when the next job starts.

Correct Answer: B

Community vote distribution

B (100%)

 **potomac** 3 weeks, 2 days ago

Selected Answer: B

Lambda allows you to allocate memory for your functions in increments of 1 MB, ranging from a minimum of 128 MB to a maximum of 10,240 MB (10 GB).

upvoted 1 times

 **Guru4Cloud** 3 months ago

Selected Answer: B

Remember - AWS Lambda function can go up to 10 GB of memory, instead of free tier only allow 512MB.

upvoted 3 times

 **james2033** 4 months, 1 week ago

Selected Answer: B

"AWS Batch jobs as EventBridge targets" at <https://docs.aws.amazon.com/batch/latest/userguide/batch-cwe-target.html>

AWS Batch + Amazon EventBridge <https://docs.aws.amazon.com/batch/latest/userguide/batch-cwe-target.html>.

AWS Lambda just for a point of time per period. Choose B.

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: B

10 seconds to run, optimize the costs, consumes 1 GB of memory = AWS Lambda function.

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: B

AWS Lambda automatically scales resources to handle the workload, so you don't have to worry about managing the underlying infrastructure. It provisions the necessary compute resources based on the configured memory size (1 GB in this case) and executes the job in a serverless environment.

By using Amazon EventBridge, you can create a scheduled rule to trigger the Lambda function every hour, ensuring that the job runs on the desired interval.

upvoted 1 times

 **Yadav_Sanjay** 6 months, 1 week ago

Selected Answer: B

B - Within 10 sec and 1 GB Memory (Lambda Memory 128MB to 10GB)

upvoted 2 times

 **Yadav_Sanjay** 6 months, 1 week ago

<https://docs.aws.amazon.com/lambda/latest/operatorguide/computing-power.html>

upvoted 1 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: B

Agreed, B Lambda

upvoted 2 times

A company wants to implement a backup strategy for Amazon EC2 data and multiple Amazon S3 buckets. Because of regulatory requirements, the company must retain backup files for a specific time period. The company must not alter the files for the duration of the retention period.

Which solution will meet these requirements?

- A. Use AWS Backup to create a backup vault that has a vault lock in governance mode. Create the required backup plan.
- B. Use Amazon Data Lifecycle Manager to create the required automated snapshot policy.
- C. Use Amazon S3 File Gateway to create the backup. Configure the appropriate S3 Lifecycle management.
- D. Use AWS Backup to create a backup vault that has a vault lock in compliance mode. Create the required backup plan.

Correct Answer: A

Community vote distribution

D (100%)

✉  **Efren**  6 months, 2 weeks ago

D, Governance is like the goverment, they can do things you cannot , like delete files or backups :D Compliance, nobody can!
upvoted 23 times

✉  **cmbt** 4 months, 3 weeks ago

Finally I understood!
upvoted 2 times

✉  **joshnort** 5 months ago

Great analogy
upvoted 6 times

✉  **Guru4Cloud**  3 months ago

Selected Answer: D

D. Use AWS Backup to create a backup vault that has a vault lock in compliance mode. Create the required backup plan
upvoted 1 times

✉  **Guru4Cloud** 3 months ago

Selected Answer: D

Use AWS Backup to create a backup vault that has a vault lock in compliance mode. Create the required backup plan
upvoted 1 times

✉  **ccat91** 4 months ago

Selected Answer: D
Compliance mode
upvoted 1 times

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

Selected Answer: D
Must not alter the files for the duration of the retention period = Compliance Mode
upvoted 1 times

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

Selected Answer: D
D for sure.
upvoted 1 times

✉  **dydzah** 6 months, 1 week ago

Selected Answer: D
<https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html>
upvoted 1 times

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

Selected Answer: D
compliance mode
upvoted 3 times

✉  **nonsense** 6 months, 2 weeks ago

Selected Answer: D

D bcs in governance we can delete backup
upvoted 3 times

A company has resources across multiple AWS Regions and accounts. A newly hired solutions architect discovers a previous employee did not provide details about the resources inventory. The solutions architect needs to build and map the relationship details of the various workloads across all accounts.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Use AWS Systems Manager Inventory to generate a map view from the detailed view report.
- B. Use AWS Step Functions to collect workload details. Build architecture diagrams of the workloads manually.
- C. Use Workload Discovery on AWS to generate architecture diagrams of the workloads.
- D. Use AWS X-Ray to view the workload details. Build architecture diagrams with relationships.

Correct Answer: A

Community vote distribution

C (93%) 7%

✉️  **potomac** 3 weeks, 2 days ago

Selected Answer: C

Workload Discovery on AWS (formerly called AWS Perspective) is a tool to visualize AWS Cloud workloads. Use Workload Discovery on AWS to build, customize, and share detailed architecture diagrams of your workloads based on live data from AWS.

upvoted 1 times

✉️  **TariqKipkemei** 4 weeks ago

Selected Answer: C

use Workload Discovery on AWS

upvoted 1 times

✉️  **Guru4Cloud** 3 months ago

Selected Answer: C

Workload Discovery is purpose-built to automatically generate visual mappings of architectures across accounts and Regions. This makes it the most operationally efficient way to meet the requirements.

upvoted 2 times

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

Selected Answer: C

Option A: AWS SSM offers "Software inventory": Collect software catalog and configuration for your instances.

Option C: Workload Discovery on AWS: is a tool for maintaining an inventory of the AWS resources across your accounts and various Regions and mapping relationships between them, and displaying them in a web UI.

upvoted 3 times

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

Selected Answer: A

<https://aws.amazon.com/blogs/mt/visualizing-resources-with-workload-discovery-on-aws/>

upvoted 1 times

✉️  **Abrar2022** 5 months, 3 weeks ago

Selected Answer: C

AWS Workload Discovery - create diagram, map and visualise AWS resources across AWS accounts and Regions

upvoted 2 times

✉️  **Abrar2022** 5 months, 3 weeks ago

Workload Discovery on AWS can map AWS resources across AWS accounts and Regions and visualize them in a UI provided on the website.

upvoted 1 times

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

Selected Answer: C

https://aws.amazon.com/jp/builders-flash/202209/workload-discovery-on-aws/?awsf.filter-name=*all

upvoted 2 times

✉️  **omoakin** 6 months, 2 weeks ago

Only C makes sense

upvoted 2 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: C

Workload Discovery on AWS is a service that helps visualize and understand the architecture of your workloads across multiple AWS accounts and Regions. It automatically discovers and maps the relationships between resources, providing an accurate representation of the architecture.

upvoted 2 times

 **Efren** 6 months, 2 weeks ago

Not sure here tbh

To efficiently build and map the relationship details of various workloads across multiple AWS Regions and accounts, you can use the AWS Systems Manager Inventory feature in combination with AWS Resource Groups. Here's a solution that can help you achieve this:

AWS Systems Manager Inventory:

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: C

only c mapping relationships

upvoted 1 times

A company uses AWS Organizations. The company wants to operate some of its AWS accounts with different budgets. The company wants to receive alerts and automatically prevent provisioning of additional resources on AWS accounts when the allocated budget threshold is met during a specific period.

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

- A. Use AWS Budgets to create a budget. Set the budget amount under the Cost and Usage Reports section of the required AWS accounts.
- B. Use AWS Budgets to create a budget. Set the budget amount under the Billing dashboards of the required AWS accounts.
- C. Create an IAM user for AWS Budgets to run budget actions with the required permissions.
- D. Create an IAM role for AWS Budgets to run budget actions with the required permissions.
- E. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the IAM identity created with the appropriate config rule to prevent provisioning of additional resources.
- F. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the IAM identity created with the appropriate service control policy (SCP) to prevent provisioning of additional resources.

Correct Answer: BDF

Community vote distribution

BDF (67%)	ADF (24%)	10%
-----------	-----------	-----

✉️  **vesen22** Highly Voted 6 months ago

Selected Answer: BDF

I don't see why adf has the most voted when almost everyone has chosen bdf, smh
https://acloudguru.com/videos/acg-fundamentals/how-to-set-up-an-aws-billing-and-budget-alert?utm_source=google&utm_medium=paid-search&utm_campaign=cloud-transformation&utm_term=ssi-global-acg-core-dsa&utm_content=free-trial&gclid=Cj0KCQjwmtGjBhDhARIsAEqfDEcDfXdLul2NxgSMxKraclTZimWOrDBRpsJPpx8IS9T4NndKhbUqPlaAlzhEALw_wcB
 upvoted 6 times

✉️  **udo2020** Highly Voted 6 months, 1 week ago

It is BDF because there is actually a Billing Dashboard available.
 upvoted 5 times

✉️  **TariqKipkemei** Most Recent 4 weeks ago

Selected Answer: DF

Its 11/Nov/2023. Options D&F are definitely required.
 As for the budget, right from the aws console, the only place to set this up is:
 AWS Billing > Cost Management > Budgets.
 upvoted 2 times

✉️  **Guru4Cloud** 3 months ago

Selected Answer: BDF

How to create a budget:
 Billing console > budget > create budget!
 upvoted 3 times

✉️  **Chris22usa** 5 months ago

ACF:
 Option B is incorrect because the budget amount should be set under the Cost and Usage Reports section, not the Billing dashboards.
 upvoted 1 times

✉️  **Abrar2022** 5 months, 3 weeks ago

Selected Answer: BDF

How to create a budget:
 Billing console > budget > create budget!
 upvoted 1 times

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

Selected Answer: BDF

https://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/view-billing-dashboard.html
 upvoted 4 times

✉️  **y0** 6 months, 1 week ago

BDF - Budgets can be set from the billing dashboard in AWS console
upvoted 2 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: ADF

Currently, AWS does not have a specific feature called "AWS Billing Dashboards."
upvoted 5 times

 **RainWhisper** 6 months, 1 week ago

<https://awslabs.github.io/scale-out-computing-on-aws/workshops/TKO-Scale-Out-Computing/modules/071-budgets/>
upvoted 1 times

 **Efren** 6 months, 2 weeks ago

if im not wrong, those are correct
upvoted 2 times

A company runs applications on Amazon EC2 instances in one AWS Region. The company wants to back up the EC2 instances to a second Region. The company also wants to provision EC2 resources in the second Region and manage the EC2 instances centrally from one AWS account.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a disaster recovery (DR) plan that has a similar number of EC2 instances in the second Region. Configure data replication.
- B. Create point-in-time Amazon Elastic Block Store (Amazon EBS) snapshots of the EC2 instances. Copy the snapshots to the second Region periodically.
- C. Create a backup plan by using AWS Backup. Configure cross-Region backup to the second Region for the EC2 instances.
- D. Deploy a similar number of EC2 instances in the second Region. Use AWS DataSync to transfer the data from the source Region to the second Region.

Correct Answer: C

Community vote distribution

C (89%) 11%

✉  **bogobob** 1 week, 5 days ago

Selected Answer: D

How does AWS Backup address that "The company also wants to provision EC2 resources in the second Region"?
upvoted 1 times

✉  **Guru4Cloud** 3 months ago

Selected Answer: C

C is the most cost-effective solution that meets all the requirements.

AWS Backup provides automated backups across Regions for EC2 instances. This handles the backup requirement.

AWS Backup is more cost-effective for cross-Region EC2 backups than using EBS snapshots manually or DataSync.
upvoted 3 times

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

Selected Answer: C

AWS backup
upvoted 1 times

✉  **omoakin** 6 months ago

CCCCC
. Create a backup plan by using AWS Backup. Configure cross-Region backup to the second Region for the EC2 instances.
upvoted 1 times

✉  **Blingy** 6 months ago

CCCCCC
upvoted 1 times

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

Selected Answer: C

Using AWS Backup, you can create backup plans that automate the backup process for your EC2 instances. By configuring cross-Region backup, you can ensure that backups are replicated to the second Region, providing a disaster recovery capability. This solution is cost-effective as it leverages AWS Backup's built-in features and eliminates the need for manual snapshot management or deploying and managing additional EC2 instances in the second Region.

upvoted 4 times

✉  **Efren** 6 months, 2 weeks ago

C, i would say same, always AWS Backup
upvoted 1 times

A company that uses AWS is building an application to transfer data to a product manufacturer. The company has its own identity provider (IdP). The company wants the IdP to authenticate application users while the users use the application to transfer data. The company must use Applicability Statement 2 (AS2) protocol.

Which solution will meet these requirements?

- A. Use AWS DataSync to transfer the data. Create an AWS Lambda function for IdP authentication.
- B. Use Amazon AppFlow flows to transfer the data. Create an Amazon Elastic Container Service (Amazon ECS) task for IdP authentication.
- C. Use AWS Transfer Family to transfer the data. Create an AWS Lambda function for IdP authentication.
- D. Use AWS Storage Gateway to transfer the data. Create an Amazon Cognito identity pool for IdP authentication.

Correct Answer: C

Community vote distribution

C (75%)

D (25%)

 **potomac** 3 weeks, 2 days ago

Selected Answer: C

To authenticate your users, you can use your existing identity provider with AWS Transfer Family. You integrate your identity provider using an AWS Lambda function, which authenticates and authorizes your users for access to Amazon S3 or Amazon Elastic File System (Amazon EFS).

upvoted 1 times

 **potomac** 3 weeks, 2 days ago

Selected Answer: C

Applicability Statement 2 (AS2) is a business-to-business (B2B) messaging protocol used to exchange Electronic Data Interchange (EDI) documents. With AWS Transfer Family's AS2 capabilities, you can securely exchange AS2 messages at scale while maintaining compliance and interoperability with your trading partners.

upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

D is ok

upvoted 1 times

 **hsinchang** 4 months ago

its own IdP -> Lambda

upvoted 2 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: C

Option C stands out stronger because AWS Transfer Family securely scales your recurring business-to-business file transfers to AWS Storage services using SFTP, FTPS, FTP, and AS2 protocols.

And AWS Lambda can be used to authenticate users with the company's IdP.

upvoted 4 times

 **baba365** 4 months, 3 weeks ago

Ans : C

To authenticate your users, you can use your existing identity provider with AWS Transfer Family. You integrate your identity provider using an AWS Lambda function, which authenticates and authorizes your users for access to Amazon S3 or Amazon Elastic File System (Amazon EFS).

<https://docs.aws.amazon.com/transfer/latest/userguide/custom-identity-provider-users.html>

upvoted 1 times

 **dydzah** 6 months ago

Selected Answer: C

<https://docs.aws.amazon.com/transfer/latest/userguide/custom-identity-provider-users.html>

upvoted 1 times

 **examtopictempacc** 6 months, 1 week ago

Selected Answer: C

C is correct. AWS Transfer Family supports the AS2 protocol, which is required by the company. Also, AWS Lambda can be used to authenticate users with the company's IdP, which meets the company's requirement.

upvoted 1 times

 EA100 6 months, 1 week ago

Answer - D

AS2 is a widely used protocol for secure and reliable data transfer. In this scenario, the company wants to transfer data using the AS2 protocol and authenticate application users using their own identity provider (IdP). AWS Storage Gateway provides a hybrid cloud storage solution that enables data transfer between on-premises environments and AWS.

By using AWS Storage Gateway, you can set up a gateway that supports the AS2 protocol for data transfer. Additionally, you can configure authentication using an Amazon Cognito identity pool. Amazon Cognito provides a comprehensive authentication and user management service that integrates with various identity providers, including your own IdP.

Therefore, Option D is the correct solution as it leverages AWS Storage Gateway for AS2 data transfer and allows authentication using an Amazon Cognito identity pool integrated with the company's IdP.

upvoted 1 times

 deecheon 2 months, 4 weeks ago

AWS Transfer Family also support AS2

upvoted 1 times

 hiroohiroo 6 months, 1 week ago

Selected Answer: C

<https://repost.aws/articles/ARo2ihKKThT2Cue5j6yVUgsQ/articles/ARo2ihKKThT2Cue5j6yVUgsQ/aws-transfer-family-announces-support-for-sending-as2-messages-over-https?>

upvoted 1 times

 omoakin 6 months, 2 weeks ago

C is correct

upvoted 1 times

 nosense 6 months, 1 week ago

Option D looks the better option because it is more secure, scalable, cost-effective, and easy to use than option C.

upvoted 1 times

 omoakin 6 months, 2 weeks ago

This is a new Qtn n AS2 is newly supported by AWS Transfer family.....good timing to know ur stuffs.

upvoted 1 times

 clouduenthusiast 6 months, 2 weeks ago

Selected Answer: D

AWS Storage Gateway supports the AS2 protocol for transferring data. By using AWS Storage Gateway, the company can integrate its own IdP authentication by creating an Amazon Cognito identity pool. Amazon Cognito provides user authentication and authorization capabilities, allowing the company to authenticate application users using its own IdP.

AWS Transfer Family does not currently support the AS2 protocol. AS2 is a specific protocol used for secure and reliable data transfer, often used in business-to-business (B2B) scenarios. In this case, option C, which suggests using AWS Transfer Family, would not meet the requirement of using the AS2 protocol.

upvoted 3 times

 omoakin 6 months, 2 weeks ago

AWS Transfer Family now supports the Applicability Statement 2 (AS2) protocol, complementing existing protocol support for SFTP, FTPS, and FTP

upvoted 1 times

 y0 6 months, 1 week ago

This is not a case for storage gateway which is more used for a hybrid like environment. Here, to transfer data, we can think or Datasync or Transfer family and considering AS2 protocol, transfer family looks good

upvoted 2 times

 Efren 6 months, 2 weeks ago

ChatGP

To meet the requirements of using an identity provider (IdP) for user authentication and the AS2 protocol for data transfer, you can implement the following solution:

AWS Transfer Family: Use AWS Transfer Family, specifically AWS Transfer for SFTP or FTPS, to handle the data transfer using the AS2 protocol. AWS Transfer for SFTP and FTPS provide fully managed, highly available SFTP and FTPS servers in the AWS Cloud.

Not sure about Lamdba tho

upvoted 2 times

 Efren 6 months, 2 weeks ago

Maybe yes

The Lambda authorizer authenticates the token with the third-party identity provider.

upvoted 1 times

 clouduenthusiast 6 months, 2 weeks ago

Also from ChatGPT

AWS Transfer Family supports multiple protocols, including AS2, and can be used for data transfer. By utilizing AWS Transfer Family, the company can integrate its own IdP authentication by creating an AWS Lambda function.

Both options D and C are valid solutions for the given requirements. The choice between them would depend on additional factors such as specific preferences, existing infrastructure, and overall architectural considerations.

upvoted 2 times

A solutions architect is designing a REST API in Amazon API Gateway for a cash payback service. The application requires 1 GB of memory and 2 GB of storage for its computation resources. The application will require that the data is in a relational format.

Which additional combination of AWS services will meet these requirements with the LEAST administrative effort? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon RDS
- D. Amazon DynamoDB
- E. Amazon Elastic Kubernetes Services (Amazon EKS)

Correct Answer: BC

Community vote distribution

BC (82%)

AC (18%)

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

Selected Answer: BC

"The application will require that the data is in a relational format" so DynamoDB is out. RDS is the choice. Lambda is serverless.
upvoted 10 times

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

Selected Answer: BC

AWS Lambda and Amazon RDS
upvoted 1 times

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

Selected Answer: AC

"2 GB of storage for its COMPUTATION resources" the maximum for Lambda is 512MB.
upvoted 3 times

✉  **PLN6302** 3 months ago

Lambda now supports upto 10GB of memory
upvoted 2 times

✉  **Kp88** 4 months ago

I thought the same but seems like you can go all the way to 10gb. 512mb is the free tier
<https://docs.aws.amazon.com/lambda/latest/dg/configuration-function-common.html#configuration-ephemeral-storage>
upvoted 2 times

✉  **r3mo** 5 months, 2 weeks ago

At first I was thinking the same. But the computation memory for the lambda function is 1gb not 2gb. Hence. if you go to basic settings when you create the lambda function you can select a in the memory settings the 1024 MB (1Gb) and that solve the problem.
upvoted 1 times

✉  **Efren** 6 months, 2 weeks ago

Selected Answer: BC

Relational Data RDS and computing for Lambda
upvoted 3 times

✉  **nonsense** 6 months, 2 weeks ago

bc for me
upvoted 2 times

A company uses AWS Organizations to run workloads within multiple AWS accounts. A tagging policy adds department tags to AWS resources when the company creates tags.

An accounting team needs to determine spending on Amazon EC2 consumption. The accounting team must determine which departments are responsible for the costs regardless of AWS account. The accounting team has access to AWS Cost Explorer for all AWS accounts within the organization and needs to access all reports from Cost Explorer.

Which solution meets these requirements in the MOST operationally efficient way?

- A. From the Organizations management account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.
- B. From the Organizations management account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.
- C. From the Organizations member account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by the tag name, and filter by EC2.
- D. From the Organizations member account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

Correct Answer: C

Community vote distribution

A (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: A

From the Organizations management account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

upvoted 2 times

 **TariqKipkemei** 5 months, 2 weeks ago

Selected Answer: A

From the Organizations management account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

upvoted 1 times

 **luisgu** 6 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

upvoted 4 times

 **hiroohiroo** 6 months, 1 week ago

Selected Answer: A

https://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/activating-tags.html

upvoted 2 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: A

By activating a user-defined cost allocation tag named "department" and creating a cost report in Cost Explorer that groups by the tag name and filters by EC2, the accounting team will be able to track and attribute costs to specific departments across all AWS accounts within the organization. This approach allows for consistent cost allocation and reporting regardless of the AWS account structure.

upvoted 4 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: A

a for me

upvoted 2 times

A company wants to securely exchange data between its software as a service (SaaS) application Salesforce account and Amazon S3. The company must encrypt the data at rest by using AWS Key Management Service (AWS KMS) customer managed keys (CMKs). The company must also encrypt the data in transit. The company has enabled API access for the Salesforce account.

- A. Create AWS Lambda functions to transfer the data securely from Salesforce to Amazon S3.
- B. Create an AWS Step Functions workflow. Define the task to transfer the data securely from Salesforce to Amazon S3.
- C. Create Amazon AppFlow flows to transfer the data securely from Salesforce to Amazon S3.
- D. Create a custom connector for Salesforce to transfer the data securely from Salesforce to Amazon S3.

Correct Answer: C*Community vote distribution*

C (100%)

cludenthusiast Highly Voted 6 months, 2 weeks ago**Selected Answer: C**

Amazon AppFlow is a fully managed integration service that allows you to securely transfer data between different SaaS applications and AWS services. It provides built-in encryption options and supports encryption in transit using SSL/TLS protocols. With AppFlow, you can configure the data transfer flow from Salesforce to Amazon S3, ensuring data encryption at rest by utilizing AWS KMS CMKs.

upvoted 6 times

Guru4Cloud Most Recent 3 months ago**Selected Answer: C**

- Amazon AppFlow can securely transfer data between Salesforce and Amazon S3.
- AppFlow supports encrypting data at rest in S3 using KMS CMKs.
- AppFlow supports encrypting data in transit using HTTPS/TLS.
- AppFlow provides built-in support and templates for Salesforce and S3, requiring less custom configuration than solutions like Lambda, Step Functions, or custom connectors.
- So Amazon AppFlow is the easiest way to meet all the requirements of securely transferring data between Salesforce and S3 with encryption at rest and in transit.

upvoted 3 times

hsinchang 4 months ago

securely transfer data between Software-as-a-Service (SaaS) applications and AWS -> AppFlow

upvoted 2 times

TariqKipkemei 5 months, 2 weeks ago**Selected Answer: C**

With Amazon AppFlow automate bi-directional data flows between SaaS applications and AWS services in just a few clicks

upvoted 1 times

DrWatson 5 months, 3 weeks ago**Selected Answer: C**

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

upvoted 1 times

Abrar2022 5 months, 3 weeks ago

All you need to know is that AWS AppFlow securely transfers data between different SaaS applications and AWS services

upvoted 1 times

hiroohiroo 6 months, 1 week ago**Selected Answer: C**

<https://docs.aws.amazon.com/appflow/latest/userguide/salesforce.html>

upvoted 2 times

Efren 6 months, 2 weeks ago**Selected Answer: C**

Saas with another service, AppFlow

upvoted 1 times

A company is developing a mobile gaming app in a single AWS Region. The app runs on multiple Amazon EC2 instances in an Auto Scaling group. The company stores the app data in Amazon DynamoDB. The app communicates by using TCP traffic and UDP traffic between the users and the servers. The application will be used globally. The company wants to ensure the lowest possible latency for all users.

Which solution will meet these requirements?

- A. Use AWS Global Accelerator to create an accelerator. Create an Application Load Balancer (ALB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB.
- B. Use AWS Global Accelerator to create an accelerator. Create a Network Load Balancer (NLB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB.
- C. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create a Network Load Balancer (NLB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB. Update CloudFront to use the NLB as the origin.
- D. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create an Application Load Balancer (ALB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB. Update CloudFront to use the ALB as the origin.

Correct Answer: A

Community vote distribution

B (100%)

 **Guru4Cloud** 3 months ago

Selected Answer: B

Use AWS Global Accelerator to create an accelerator. Create a Network Load Balancer (NLB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB
upvoted 2 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: B

TCP and UDP = global accelerator and Network Load Balancer
upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: B

Clearly B.
upvoted 1 times

 **eddie5049** 6 months, 1 week ago

Selected Answer: B

NLB + Accelerator
upvoted 3 times

 **hiroohiroo** 6 months, 1 week ago

Selected Answer: B

AWS Global Accelerator+NLB
upvoted 3 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: B

UDP, Global Accelerator plus NLB
upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

AWS Global Accelerator is a better solution for the mobile gaming app than CloudFront
upvoted 3 times

A company has an application that processes customer orders. The company hosts the application on an Amazon EC2 instance that saves the orders to an Amazon Aurora database. Occasionally when traffic is high the workload does not process orders fast enough.

What should a solutions architect do to write the orders reliably to the database as quickly as possible?

- A. Increase the instance size of the EC2 instance when traffic is high. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic.
- B. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.
- C. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SNS topic.
- D. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue when the EC2 instance reaches CPU threshold limits. Use scheduled scaling of EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.

Correct Answer: B

Community vote distribution

B (100%)

 **clouduenthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: B

By decoupling the write operation from the processing operation using SQS, you ensure that the orders are reliably stored in the queue, regardless of the processing capacity of the EC2 instances. This allows the processing to be performed at a scalable rate based on the available EC2 instances, improving the overall reliability and speed of order processing.

upvoted 7 times

 **Guru4Cloud** Most Recent 3 months ago

Selected Answer: B

Decoupling the order processing from the application using Amazon SQS and leveraging Auto Scaling to handle the processing of orders based on the workload in the SQS queue is indeed the most efficient and scalable approach. This architecture addresses both reliability and performance concerns during traffic spikes.

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: B

Write orders to an Amazon Simple Queue Service (Amazon SQS) queue. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.

upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: B

100% B.

upvoted 1 times

 **omoakin** 6 months ago

BBBBBBBBBB

upvoted 1 times

An IoT company is releasing a mattress that has sensors to collect data about a user's sleep. The sensors will send data to an Amazon S3 bucket. The sensors collect approximately 2 MB of data every night for each mattress. The company must process and summarize the data for each mattress. The results need to be available as soon as possible. Data processing will require 1 GB of memory and will finish within 30 seconds.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Glue with a Scala job
- B. Use Amazon EMR with an Apache Spark script
- C. Use AWS Lambda with a Python script
- D. Use AWS Glue with a PySpark job

Correct Answer: C

Community vote distribution

C (100%)

✉️ **Chiquitabandita** 3 weeks, 4 days ago

I understand C is a common answer "throw Lambda" seems to be a common theme for questions that need processing under 15 minutes for the test. but in reality, can the other solutions be viable options as well?

upvoted 2 times

✉️ **TariqKipkemei** 3 weeks, 6 days ago

Selected Answer: C

"processing will require 1 GB of memory and will finish within 30 seconds", perfect for AWS Lambda.

upvoted 1 times

✉️ **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

The data processing is lightweight, only requiring 1 GB memory and finishing in under 30 seconds. Lambda is designed for short, transient workloads like this.

Lambda scales automatically, invoking the function as needed when new data arrives. No servers to manage.

Lambda has a very low cost. You only pay for the compute time used to run the function, billed in 100ms increments. Much cheaper than provisioning EMR or Glue.

Processing can begin as soon as new data hits the S3 bucket by triggering the Lambda function. Provides low latency.

upvoted 2 times

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

Selected Answer: C

I reckon C, but I would consider other well founded options.

upvoted 1 times

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

Selected Answer: C

AWS Lambda charges you based on the number of invocations and the execution time of your function. Since the data processing job is relatively small (2 MB of data), Lambda is a cost-effective choice. You only pay for the actual usage without the need to provision and maintain infrastructure.

upvoted 4 times

✉️ **joechen2023** 5 months, 1 week ago

but the question states "Data processing will require 1 GB of memory and will finish within 30 seconds." so it can't be C as Lambda support maximum 512M

upvoted 1 times

✉️ **nilandd44gg** 4 months ago

C is valid.

Lambda quotas:

Memory - 128 MB to 10,240 MB, in 1-MB increments.

Note: Lambda allocates CPU power in proportion to the amount of memory configured. You can increase or decrease the memory and CPU power allocated to your function using the Memory (MB) setting. At 1,769 MB, a function has the equivalent of one vCPU.

Function timeout 900 seconds (15 minutes)

4 KB, for all environment variables associated with the function, in aggregate

<https://docs.aws.amazon.com/lambda/latest/dg/gettingstarted-limits.html>

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: C

c anyway the MOST cost-effectively

upvoted 2 times

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.

Which solution meets these requirements?

- A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
- B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
- C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.
- D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option
upvoted 2 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: A

Eliminate single points of failure = Multi-AZ deployment
upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: A

A) <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html#Concepts.MultiAZ.Migrating>
upvoted 1 times

 **Abrar2022** 5 months, 3 weeks ago

"minimize database downtime" so why create a new DB just modify the existing one so no time is wasted.
upvoted 3 times

 **clouduenthusiast** 6 months, 2 weeks ago

Selected Answer: A

Compared to other solutions that involve creating new instances, restoring snapshots, or setting up replication manually, converting to a Multi-AZ deployment is a simpler and more streamlined approach with lower overhead.

Overall, option A offers a cost-effective and efficient way to minimize database downtime without requiring significant changes or additional complexities.

upvoted 2 times

 **Efren** 6 months, 2 weeks ago

A for HA, but also read replica can convert itself to master if the master is down... so not sure if C?

upvoted 1 times

 **Efren** 6 months, 2 weeks ago

Sorry, the Route 53 doesn't make sense to send requests to RR, what if it's a write?

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: A

i guess aa

upvoted 3 times

A company is developing an application to support customer demands. The company wants to deploy the application on multiple Amazon EC2 Nitro-based instances within the same Availability Zone. The company also wants to give the application the ability to write to multiple block storage volumes in multiple EC2 Nitro-based instances simultaneously to achieve higher application availability.

Which solution will meet these requirements?

- A. Use General Purpose SSD (gp3) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- B. Use Throughput Optimized HDD (st1) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- D. Use General Purpose SSD (gp2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach

Correct Answer: C

Community vote distribution

C (83%) Other

 **potomac** 3 weeks, 2 days ago

Selected Answer: C

Multi-Attach is supported exclusively on Provisioned IOPS SSD (io1 and io2) volumes.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach

upvoted 2 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: C

Multi-Attach is supported exclusively on Provisioned IOPS SSD (io1 and io2) volumes.

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#:~:text=Multi%2DAttach%20is%20supported%20exclusively%20on%20Provisioned%20IOPS%20SSD%20\(io1%20and%20io2\)%20volume](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#:~:text=Multi%2DAttach%20is%20supported%20exclusively%20on%20Provisioned%20IOPS%20SSD%20(io1%20and%20io2)%20volume)

upvoted 1 times

 **Axeashes** 5 months, 2 weeks ago

Multi-Attach is supported exclusively on Provisioned IOPS SSD (io1 and io2) volumes.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html>

upvoted 1 times

 **Uzi_m** 5 months, 3 weeks ago

The correct answer is A.

Currently, Multi Attach EBS feature is supported by gp3 volumes also.

Multi-Attach is supported for certain EBS volume types, including io1, io2, gp3, st1, and sc1 volumes.

upvoted 1 times

 **Kp88** 4 months ago

No , Read this --> <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#considerations>

upvoted 1 times

 **AshishRocks** 5 months, 3 weeks ago

Answer should be D

upvoted 1 times

 **Kp88** 4 months ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#considerations>

upvoted 1 times

 **AshishRocks** 5 months, 3 weeks ago

By ChatGPT - Create General Purpose SSD (gp2) volumes: Provision multiple gp2 volumes with the required capacity for your application.

upvoted 1 times

 **Kp88** 4 months ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#considerations>

upvoted 1 times

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

Multi-Attach does not support Provisioned IOPS SSD (io2) volumes. Multi-Attach is currently available only for General Purpose SSD (gp2), Throughput Optimized HDD (st1), and Cold HDD (sc1) EBS volumes.

upvoted 1 times

✉ **Abrar2022** 5 months, 3 weeks ago

Multi-Attach is supported exclusively on Provisioned IOPS SSD (io1 or io2) volumes.

upvoted 1 times

✉ **elmogy** 6 months ago

Selected Answer: C

only io1/io2 supports Multi-Attach

upvoted 2 times

✉ **Uzi_m** 5 months, 3 weeks ago

Multi-Attach is supported for certain EBS volume types, including io1, io2, gp3, st1, and sc1 volumes.

upvoted 1 times

✉ **Kp88** 4 months ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#considerations>

upvoted 1 times

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

Selected Answer: C

only io1/io2 supports Multi-Attach

upvoted 2 times

✉ **Vlad** 6 months, 1 week ago

Selected Answer: A

Option D suggests using General Purpose SSD (gp2) EBS volumes with Amazon EBS Multi-Attach. While gp2 volumes support multi-attach, gp3 volumes offer a more cost-effective solution with enhanced performance characteristics.

upvoted 1 times

✉ **Vlad** 6 months, 1 week ago

I'm sorry :

Multi-Attach enabled volumes can be attached to up to 16 instances built on the Nitro System that are in the same Availability Zone. Multi-Attach is supported exclusively on Provisioned IOPS SSD (io1 or io2) volumes.

upvoted 2 times

✉ **Vlad** 6 months, 1 week ago

The answer is C:

upvoted 1 times

✉ **EA100** 6 months, 1 week ago

Answer - C

C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach.

While both option C and option D can support Amazon EBS Multi-Attach, using Provisioned IOPS SSD (io2) EBS volumes provides higher performance and lower latency compared to General Purpose SSD (gp2) volumes. This makes io2 volumes better suited for demanding and mission-critical applications where performance is crucial.

If the goal is to achieve higher application availability and ensure optimal performance, using Provisioned IOPS SSD (io2) EBS volumes with Multi-Attach will provide the best results.

upvoted 1 times

✉ **nonsense** 6 months, 1 week ago

Selected Answer: C

c is right

Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple instances that are in the same Availability Zone.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html>

nothing about gp

upvoted 2 times

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

Selected Answer: D

Given that the scenario does not mention any specific requirements for high-performance or specific IOPS needs, using General Purpose SSD (gp2) EBS volumes with Amazon EBS Multi-Attach (option D) is typically the more cost-effective and suitable choice. General Purpose SSD (gp2) volumes provide a good balance of performance and cost, making them well-suited for general-purpose workloads.

upvoted 1 times

✉ **elmogy** 6 months ago

the question has not mentioned anything about cost-effective solution.
only io1/io2 supports Multi-Attach

plus fyi, gp3 is the one gives a good balance of performance and cost. so gp2 is wrong in every way
upvoted 1 times

✉ **omoakin** 6 months, 2 weeks ago

I agree

General Purpose SSD (gp2) volumes are the most common volume type. They were designed to be a cost-effective storage option for a wide variety of workloads. Gp2 volumes cover system volumes, dev and test environments, and various low-latency apps.

upvoted 1 times

✉ **y0** 6 months, 1 week ago

gp2 - IOPS 16000

Nitro - IOPS 64000 - supported by io2. C is correct

upvoted 1 times

Question #466

Topic 1

A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.

What should a solutions architect do to meet this requirement?

- A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer
- B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region
- C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application
- D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer

Correct Answer: A

Community vote distribution

A (100%)

✉ **nonsense**  6 months, 2 weeks ago

Selected Answer: A

it's A

upvoted 5 times

✉ **Guru4Cloud**  3 months, 1 week ago

Selected Answer: A

A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer

upvoted 1 times

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

Selected Answer: A

Highly available = Multi-AZ EC2 Auto Scaling and Application Load Balancer.

upvoted 1 times

✉ **antropaws** 5 months, 3 weeks ago

Selected Answer: A

Most likely A.

upvoted 1 times

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

Selected Answer: A

By combining Multi-AZ EC2 Auto Scaling and an Application Load Balancer, you achieve high availability for the EC2 instances hosting your stateless two-tier application.

upvoted 4 times

A company uses AWS Organizations. A member account has purchased a Compute Savings Plan. Because of changes in the workloads inside the member account, the account no longer receives the full benefit of the Compute Savings Plan commitment. The company uses less than 50% of its purchased compute power.

- A. Turn on discount sharing from the Billing Preferences section of the account console in the member account that purchased the Compute Savings Plan.
- B. Turn on discount sharing from the Billing Preferences section of the account console in the company's Organizations management account.
- C. Migrate additional compute workloads from another AWS account to the account that has the Compute Savings Plan.
- D. Sell the excess Savings Plan commitment in the Reserved Instance Marketplace.

Correct Answer: B*Community vote distribution*

B (72%)

D (28%)

✉  **norris81**  6 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

Sign in to the AWS Management Console and open the AWS Billing console at <https://console.aws.amazon.com/billing/>

Note

Ensure you're logged in to the management account of your AWS Organizations.

upvoted 8 times

✉  **baba365**  2 months ago

So what exactly is the question?

upvoted 2 times

✉  **michalf84** 2 months, 1 week ago

Selected Answer: D

I saw similar question in older exam one can sell on the market unused capacity

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

B. Turn on discount sharing from the Billing Preferences section of the account console in the company's Organizations management account
upvoted 2 times

✉  **Lx016** 3 months ago

Bro, no need to copy paste the answer that is already written. Need an explanation, I see that you just copy pasting the potential answers without any explanation in each discussion.

upvoted 12 times

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

Selected Answer: D

"For example, you might want to sell Reserved Instances after moving instances to a new AWS Region, changing to a new instance type, ending projects before the term expiration, when your business needs change, or if you have unneeded capacity."

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market-general.html>

upvoted 1 times

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

Selected Answer: B

answer is B.

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html#:~:text=choose%20Save.-,Turning%20on%20shared%20reserved%20instances%20and%20Savings%20Plans%20discounts,-You%20can%20use>

upvoted 1 times

✉  **Felix_br** 5 months, 3 weeks ago

Selected Answer: D

The company uses less than 50% of its purchased compute power.

For this reason i believe D is the best solution : <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market-general.html>

upvoted 3 times

 **Abrar2022** 5 months, 3 weeks ago

The company Organization's management account can turn on/off shared reserved instances.

upvoted 1 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: B

To summarize, option C (Migrate additional compute workloads from another AWS account to the account that has the Compute Savings Plan) is a valid solution to address the underutilization of the Compute Savings Plan. However, it involves workload migration and may require careful planning and coordination. Consider the feasibility and impact of migrating workloads before implementing this solution.

upvoted 2 times

 **EA100** 6 months, 2 weeks ago

Answer - C

If a member account within AWS Organizations has purchased a Compute Savings Plan

upvoted 1 times

 **EA100** 6 months, 2 weeks ago

Asnwer - C

upvoted 1 times

A company is developing a microservices application that will provide a search catalog for customers. The company must use REST APIs to present the frontend of the application to users. The REST APIs must access the backend services that the company hosts in containers in private VPC subnets.

Which solution will meet these requirements?

- A. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS.
- B. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS.
- C. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.
- D. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

To allow the REST APIs to securely access the backend, a private VPC link should be created from API Gateway to the ECS containers. A private VPC link provides private connectivity between API Gateway and the VPC without using public IP addresses or requiring an internet gateway/NAT

upvoted 2 times

 **MNotABot** 4 months, 3 weeks ago

Question itself says: "The company must use REST APIs", hence WebSocket APIs are not applicable and such options are eliminated straight away.

upvoted 3 times

 **Axeashes** 5 months, 1 week ago

Selected Answer: B

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

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: B

A VPC link is a resource in Amazon API Gateway that allows for connecting API routes to private resources inside a VPC.

upvoted 1 times

 **samehpalass** 5 months, 1 week ago

B is the right choice

upvoted 1 times

 **Yadav_Sanjay** 5 months, 2 weeks ago

Why Not D

upvoted 3 times

 **potomac** 3 weeks, 2 days ago

A security group acts as a firewall for associated EC2 instances, controlling both inbound and outbound traffic at the instance level.

upvoted 1 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: B

REST API with Amazon API Gateway: REST APIs are the appropriate choice for providing the frontend of the microservices application. Amazon API Gateway allows you to design, deploy, and manage REST APIs at scale.

Amazon ECS in a Private Subnet: Hosting the application in Amazon ECS in a private subnet ensures that the containers are securely deployed within the VPC and not directly exposed to the public internet.

Private VPC Link: To enable the REST API in API Gateway to access the backend services hosted in Amazon ECS, you can create a private VPC link. This establishes a private network connection between the API Gateway and ECS containers, allowing secure communication without traversing the public internet.

upvoted 4 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

b is right, bcs vpc link provided security connection

upvoted 3 times

Question #469

Topic 1

A company stores raw collected data in an Amazon S3 bucket. The data is used for several types of analytics on behalf of the company's customers. The type of analytics requested determines the access pattern on the S3 objects.

The company cannot predict or control the access pattern. The company wants to reduce its S3 costs.

Which solution will meet these requirements?

- A. Use S3 replication to transition infrequently accessed objects to S3 Standard-Infrequent Access (S3 Standard-IA)
- B. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-IA)
- C. Use S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering
- D. Use S3 Inventory to identify and transition objects that have not been accessed from S3 Standard to S3 Intelligent-Tiering

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C. Use S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: C

Cannot predict access pattern = S3 Intelligent-Tiering.

upvoted 2 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: C

Not known patterns, Intelligent Tier

upvoted 3 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: C

S3 Inventory can't move files to another class

upvoted 4 times

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However the company's security policy states that any external service cannot initiate a connection to the EC2 instances.

What should a solutions architect recommend to resolve this issue?

- A. Create a NAT gateway and make it the destination of the subnet's route table
- B. Create an internet gateway and make it the destination of the subnet's route table
- C. Create a virtual private gateway and make it the destination of the subnet's route table
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table

Correct Answer: D

Community vote distribution

D (100%)

 **wRhlH** Highly Voted 5 months ago

For exam,
egress-only internet gateway: IPv6
NAT gateway: IPv4
upvoted 14 times

 **RDM10** 2 months, 1 week ago

thanks a lot
upvoted 1 times

 **cloudenthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: D

An egress-only internet gateway (EIGW) is specifically designed for IPv6-only VPCs and provides outbound IPv6 internet access while blocking inbound IPv6 traffic. It satisfies the requirement of preventing external services from initiating connections to the EC2 instances while allowing the instances to initiate outbound communications.

upvoted 6 times

 **RainWhisper** 5 months, 3 weeks ago

Enable outbound IPv6 traffic using an egress-only internet gateway
<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>
upvoted 2 times

 **cloudenthusiast** 6 months, 2 weeks ago

Since the company's security policy explicitly states that external services cannot initiate connections to the EC2 instances, using a NAT gateway (option A) would not be suitable. A NAT gateway allows outbound connections from private subnets to the internet, but it does not restrict inbound connections from external sources.

upvoted 5 times

 **Guru4Cloud** Most Recent 3 months, 1 week ago

Selected Answer: D

D. Create an egress-only internet gateway and make it the destination of the subnet's route table
upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: D

Outbound traffic only = Create an egress-only internet gateway and make it the destination of the subnet's route table
upvoted 1 times

 **radev** 6 months, 2 weeks ago

Selected Answer: D

Egress-Only internet Gateway
upvoted 3 times

A company is creating an application that runs on containers in a VPC. The application stores and accesses data in an Amazon S3 bucket. During the development phase, the application will store and access 1 TB of data in Amazon S3 each day. The company wants to minimize costs and wants to prevent traffic from traversing the internet whenever possible.

Which solution will meet these requirements?

- A. Enable S3 Intelligent-Tiering for the S3 bucket
- B. Enable S3 Transfer Acceleration for the S3 bucket
- C. Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC
- D. Create an interface endpoint for Amazon S3 in the VPC. Associate this endpoint with all route tables in the VPC

Correct Answer: C

Community vote distribution

C (100%)

✉️  **cloudepthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: C

Gateway VPC Endpoint: A gateway VPC endpoint enables private connectivity between a VPC and Amazon S3. It allows direct access to Amazon S3 without the need for internet gateways, NAT devices, VPN connections, or AWS Direct Connect.

Minimize Internet Traffic: By creating a gateway VPC endpoint for Amazon S3 and associating it with all route tables in the VPC, the traffic between the VPC and Amazon S3 will be kept within the AWS network. This helps in minimizing data transfer costs and prevents the need for traffic to traverse the internet.

Cost-Effective: With a gateway VPC endpoint, the data transfer between the application running in the VPC and the S3 bucket stays within the AWS network, reducing the need for data transfer across the internet. This can result in cost savings, especially when dealing with large amounts of data.
upvoted 5 times

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

Option B (Enable S3 Transfer Acceleration for the S3 bucket) is a feature that uses the CloudFront global network to accelerate data transfers to and from Amazon S3. While it can improve data transfer speed, it still involves traffic traversing the internet and doesn't directly address the goal of minimizing costs and preventing internet traffic whenever possible.

upvoted 1 times

✉️  **litos168** Highly Voted 4 months, 2 weeks ago

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

upvoted 5 times

✉️  **bsbs1234** Most Recent 1 month, 4 weeks ago

I think both C&D will work.
But D will have extra cost. So C is correct.
upvoted 1 times

✉️  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C. Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC
upvoted 1 times

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

Selected Answer: C

Prevent traffic from traversing the internet = Gateway VPC endpoint for S3.
upvoted 1 times

✉️  **Anmol_1010** 6 months, 1 week ago

Key word transversing to internet
upvoted 1 times

✉️  **Efren** 6 months, 2 weeks ago

Selected Answer: C

Gateway endpoint for S3

upvoted 2 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: C

vpc endpoint for s3

upvoted 4 times

A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.

Which method should the solutions architect select?

- A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
- B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
- C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
- D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Correct Answer: A

Community vote distribution

A (100%)

✉  **danielmakita** 1 month ago

Would go for A.
Minimal application changes != No application changes
upvoted 1 times

✉  **thanhnv142** 1 month, 1 week ago

"requires minimal application changes" - Do not choose A because it requires updates of codes.
upvoted 1 times

✉  **thanhnv142** 1 month, 1 week ago

C is correct
A, B and D all require code changes to the app.
upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
upvoted 1 times

✉  **haoAWS** 5 months ago

Selected Answer: A

Read replica does improve the read speed, but it cannot improve the latency because there is always latency between replicas. So A works and B not work.
upvoted 1 times

✉  **mattcl** 5 months, 1 week ago

C , "requires minimal application changes"
upvoted 1 times

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

Selected Answer: A

little latency = Amazon DynamoDB Accelerator (DAX) .
upvoted 1 times

✉  **DrWatson** 5 months, 3 weeks ago

Selected Answer: A

I go with A <https://aws.amazon.com/blogs/mobile/building-a-full-stack-chat-application-with-aws-and-nextjs/> but I have some doubts about this <https://aws.amazon.com/blogs/database/how-to-build-a-chat-application-with-amazon-elasticache-for-redis/>
upvoted 1 times

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

Selected Answer: A

Amazon DynamoDB Accelerator (DAX): DAX is an in-memory cache for DynamoDB that provides low-latency access to frequently accessed data. By configuring DAX for the new messages table, read requests for the table will be served from the DAX cache, significantly reducing the latency.

Minimal Application Changes: With DAX, the application code can be updated to use the DAX endpoint instead of the standard DynamoDB endpoint. This change is relatively minimal and does not require extensive modifications to the application's data access logic.

Low Latency: DAX caches frequently accessed data in memory, allowing subsequent read requests for the same data to be served with minimal latency. This ensures that new messages can be read by users with minimal delay.

upvoted 2 times

 **clouduenthusiast** 6 months, 2 weeks ago

Option B (Add DynamoDB read replicas) involves creating read replicas to handle the increased read load, but it may not directly address the requirement of minimizing latency for new message reads.

upvoted 1 times

 **Efren** 6 months, 2 weeks ago

Tricky one, in doubt also with B, read replicas.

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: A

a is valid

upvoted 2 times

Question #473

Topic 1

A company hosts a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website serves static content. Website traffic is increasing, and the company is concerned about a potential increase in cost.

- A. Create an Amazon CloudFront distribution to cache static files at edge locations
- B. Create an Amazon ElastiCache cluster. Connect the ALB to the ElastiCache cluster to serve cached files
- C. Create an AWS WAF web ACL and associate it with the ALB. Add a rule to the web ACL to cache static files
- D. Create a second ALB in an alternative AWS Region. Route user traffic to the closest Region to minimize data transfer costs

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

A. Create an Amazon CloudFront distribution to cache static files at edge locations

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: A

Serves static content = Amazon CloudFront distribution.

upvoted 1 times

 **clouduenthusiast** 6 months, 2 weeks ago

Selected Answer: A

Amazon CloudFront: CloudFront is a content delivery network (CDN) service that caches content at edge locations worldwide. By creating a CloudFront distribution, static content from the website can be cached at edge locations, reducing the load on the EC2 instances and improving the overall performance.

Caching Static Files: Since the website serves static content, caching these files at CloudFront edge locations can significantly reduce the number of requests forwarded to the EC2 instances. This helps to lower the overall cost by offloading traffic from the instances and reducing the data transfer costs.

upvoted 3 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: A

a for me

upvoted 2 times

A company has multiple VPCs across AWS Regions to support and run workloads that are isolated from workloads in other Regions. Because of a recent application launch requirement, the company's VPCs must communicate with all other VPCs across all Regions.

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

- A. Use VPC peering to manage VPC communication in a single Region. Use VPC peering across Regions to manage VPC communications.
- B. Use AWS Direct Connect gateways across all Regions to connect VPCs across regions and manage VPC communications.
- C. Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications.
- D. Use AWS PrivateLink across all Regions to connect VPCs across Regions and manage VPC communications

Correct Answer: C

Community vote distribution

C (100%)

 **Felix_br** Highly Voted 5 months, 3 weeks ago

The correct answer is: C. Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications.

AWS Transit Gateway is a network hub that you can use to connect your VPCs and on-premises networks. It provides a single point of control for managing your network traffic, and it can help you to reduce the number of connections that you need to manage.

Transit Gateway peering allows you to connect two Transit Gateways in different Regions. This can help you to create a global network that spans multiple Regions.

To use Transit Gateway to manage VPC communication in a single Region, you would create a Transit Gateway in each Region. You would then attach your VPCs to the Transit Gateway.

To use Transit Gateway peering to manage VPC communication across Regions, you would create a Transit Gateway peering connection between the Transit Gateways in each Region.

upvoted 10 times

 **TariqKipkemei** 5 months, 1 week ago

thank you for this comprehensive explanation
upvoted 1 times

 **cloudenthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: C

AWS Transit Gateway: Transit Gateway is a highly scalable service that simplifies network connectivity between VPCs and on-premises networks. By using a Transit Gateway in a single Region, you can centralize VPC communication management and reduce administrative effort.

Transit Gateway Peering: Transit Gateway supports peering connections across AWS Regions, allowing you to establish connectivity between VPCs in different Regions without the need for complex VPC peering configurations. This simplifies the management of VPC communications across Regions.

upvoted 5 times

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

Selected Answer: C

multiple regions + multiple VPCs --> Transit Gateway
upvoted 2 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: C

Definitely C.
Very well explained by @Felix_br
upvoted 1 times

 **omoakin** 6 months, 2 weeks ago

Cccccccccccccccc
if you have services in multiple Regions, a Transit Gateway will allow you to access those services with a simpler network configuration.
upvoted 2 times

A company is designing a containerized application that will use Amazon Elastic Container Service (Amazon ECS). The application needs to access a shared file system that is highly durable and can recover data to another AWS Region with a recovery point objective (RPO) of 8 hours. The file system needs to provide a mount target in each Availability Zone within a Region.

A solutions architect wants to use AWS Backup to manage the replication to another Region.

Which solution will meet these requirements?

- A. Amazon FSx for Windows File Server with a Multi-AZ deployment
- B. Amazon FSx for NetApp ONTAP with a Multi-AZ deployment
- C. Amazon Elastic File System (Amazon EFS) with the Standard storage class
- D. Amazon FSx for OpenZFS

Correct Answer: C

Community vote distribution

C (80%) B (20%)

✉  **elmogy**  6 months ago

Selected Answer: C

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

Q: What is Amazon EFS Replication?

EFS Replication can replicate your file system data to another Region or within the same Region without requiring additional infrastructure or a custom process. Amazon EFS Replication automatically and transparently replicates your data to a second file system in a Region or AZ of your choice. You can use the Amazon EFS console, AWS CLI, and APIs to activate replication on an existing file system. EFS Replication is continual and provides a recovery point objective (RPO) and a recovery time objective (RTO) of minutes, helping you meet your compliance and business continuity goals.

upvoted 7 times

✉  **Goutham4981**  1 week, 3 days ago

Selected Answer: C

In the absence of this information, we can only make an assumption based on the provided requirements. The requirement for a shared file system that can recover data to another AWS Region with a recovery point objective (RPO) of 8 hours, and the need for a mount target in each Availability Zone within a Region, are all natively supported by Amazon EFS with the Standard storage class.

While Amazon FSx for NetApp ONTAP does provide shared file systems and supports both Windows and Linux, it does not natively support replication to another region through AWS Backup.

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C. Amazon Elastic File System (Amazon EFS) with the Standard storage class

upvoted 1 times

✉  **cd93** 3 months, 1 week ago

Selected Answer: B

B or C, but since question didn't mention operating system type, I guess we should go with B because it is more versatile (EFS supports Linux only), although ECS containers do support windows instances...

upvoted 1 times

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

Selected Answer: C

Both option B and C will support this requirement.

<https://aws.amazon.com/efs/faq/#:~:text=What%20is%20Amazon%20EFS%20Replication%3F>

<https://aws.amazon.com/fsx/netapp-ontap/faqs/#:~:text=How%20do%20I%20configure%20cross%2Dregion%20replication%20for%20the%20data%20in%20my%20file%20system%3F>

upvoted 1 times

✉  **omoakin** 6 months ago

BBBBBBBBBBBBBBB

upvoted 1 times

 **RainWhisper** 6 months, 1 week ago

Both B and C are feasible.

Amazon FSx for NetApp ONTAP is just way overpriced for a backup storage solution. The keyword to look out for is sub milli seconds latency
In real life env, Amazon Elastic File System (Amazon EFS) with the Standard storage class is good enough.

upvoted 3 times

 **Anmol_1010** 6 months, 1 week ago

Efs, can be mounted only in 1 region
So the answer is B
upvoted 3 times

 **Rob1L** 6 months, 1 week ago

Selected Answer: C

C: EFS

upvoted 2 times

 **y0** 6 months, 1 week ago

Selected Answer: C

AWS Backup can manage replication of EFS to another region as mentioned below

<https://docs.aws.amazon.com/efs/latest/ug/awsbackup.html>

upvoted 1 times

 **norris81** 6 months, 2 weeks ago

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

During a disaster or fault within an AZ affecting all copies of your data, you might experience loss of data that has not been replicated using Amazon EFS Replication. EFS Replication is designed to meet a recovery point objective (RPO) and recovery time objective (RTO) of minutes. You can use AWS Backup to store additional copies of your file system data and restore them to a new file system in an AZ or Region of your choice. Amazon EFS file system backup data created and managed by AWS Backup is replicated to three AZs and is designed for 99.999999999% (11 nines) durability.

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Amazon EFS is a scalable and durable elastic file system that can be used with Amazon ECS. However, it does not support replication to another AWS Region.

upvoted 1 times

 **elmogy** 6 months ago

it does support replication to another AWS Region

check the same link you are replying to :/

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

Q: What is Amazon EFS Replication?

EFS Replication can replicate your file system data to another Region or within the same Region without requiring additional infrastructure or a custom process. Amazon EFS Replication automatically and transparently replicates your data to a second file system in a Region or AZ of your choice. You can use the Amazon EFS console, AWS CLI, and APIs to activate replication on an existing file system. EFS Replication is continual and provides a recovery point objective (RPO) and a recovery time objective (RTO) of minutes, helping you meet your compliance and business continuity goals.

upvoted 1 times

 **fakrap** 6 months, 1 week ago

To use EFS replication in a Region that is disabled by default, you must first opt in to the Region, so it does support.

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

shared file system that is highly durable and can recover data

upvoted 2 times

 **Efren** 6 months, 2 weeks ago

Why not EFS?

upvoted 1 times

A company is expecting rapid growth in the near future. A solutions architect needs to configure existing users and grant permissions to new users on AWS. The solutions architect has decided to create IAM groups. The solutions architect will add the new users to IAM groups based on department.

Which additional action is the MOST secure way to grant permissions to the new users?

- A. Apply service control policies (SCPs) to manage access permissions
- B. Create IAM roles that have least privilege permission. Attach the roles to the IAM groups
- C. Create an IAM policy that grants least privilege permission. Attach the policy to the IAM groups
- D. Create IAM roles. Associate the roles with a permissions boundary that defines the maximum permissions

Correct Answer: C

Community vote distribution

C (88%) 13%

 **Rob1L** Highly Voted 6 months, 1 week ago

Selected Answer: C

Option B is incorrect because IAM roles are not directly attached to IAM groups.

upvoted 5 times

 **RoroJ** 6 months ago

IAM Roles can be attached to IAM Groups:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/assign_role.html

upvoted 2 times

 **antropaws** 5 months, 3 weeks ago

Read your own link: You can assign an existing IAM role to an AWS Directory Service user or group. Not to IAM groups.

upvoted 5 times

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

Selected Answer: C

A is wrong

SCPs are mainly used along with AWS Organizations organizational units (OUs). SCPs do not replace IAM Policies such that they do not provide actual permissions. To perform an action, you would still need to grant appropriate IAM Policy permissions.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

Create an IAM policy that grants least privilege permission. Attach the policy to the IAM groups

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: C

An IAM policy is an object in AWS that, when associated with an identity or resource, defines their permissions. Permissions in the policies determine whether a request is allowed or denied. You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources.

So, option B will also work.

But Since I can only choose one, C would be it.

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: C

You can attach up to 10 IAM policy for a 'user group'.

upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: C

C is the correct one.

upvoted 1 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: C

Agreed with C

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_manage_attach-policy.html

Attaching a policy to an IAM user group

upvoted 4 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

should be b

upvoted 2 times

 **imazsyed** 6 months, 2 weeks ago

it should be C

upvoted 3 times

 **nonsense** 6 months, 2 weeks ago

Option C is not as secure as option B because IAM policies are attached to individual users and cannot be used to manage permissions for groups of users.

upvoted 2 times

 **omoakin** 6 months, 1 week ago

IAM Roles manage who has access to your AWS resources, whereas IAM policies control their permissions. A Role with no Policy attached to it won't have to access any AWS resources. A Policy that is not attached to an IAM role is effectively unused.

upvoted 3 times

 **Clouddon** 2 months, 3 weeks ago

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

upvoted 1 times

A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "s3>ListBucket",  
                "s3>DeleteObject"  
            ],  
            "Resource": [  
                "arn:aws:s3:::bucket-name"  
            ],  
            "Effect": "Allow"  
        }  
    ]  
}
```

Which statement should a solutions architect add to the policy to correct bucket access?

- "Action": [
 "s3:*Object"
],
A. "Resource": [
 "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"

- "Action": [
 "s3:*"
],
B. "Resource": [
 "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"

- "Action": [
 "s3>DeleteObject"
],
C. "Resource": [
 "arn:aws:s3:::bucket-name*"
],
"Effect": "Allow"

- "Action": [
 "s3>DeleteObject"
],
D. "Resource": [
 "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"

Correct Answer: C

Community vote distribution

D (100%)

 Guru4Cloud 3 months, 1 week ago

Selected Answer: D

option B action is S3:*. this means all actions. The company follows least-privilege access rules. Hence option D
upvoted 2 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: D

D is the answer
upvoted 1 times

 **AncaZalog** 5 months, 2 weeks ago

what's the difference between B and D? on B the statements are just placed in another order
upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

option B action is S3:*. this means all actions. The company follows least-privilege access rules. Hence option D
upvoted 1 times

 **serepetru** 6 months ago

What is the difference between C and D?
upvoted 2 times

 **Ta_Les** 5 months, 2 weeks ago

the "/" at the end of the last line on D
upvoted 2 times

 **Rob1L** 6 months, 1 week ago

Selected Answer: D

D for sure
upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: D

d work
upvoted 4 times

 **Efren** 6 months, 2 weeks ago

Agreed
upvoted 1 times

A law firm needs to share information with the public. The information includes hundreds of files that must be publicly readable. Modifications or deletions of the files by anyone before a designated future date are prohibited.

Which solution will meet these requirements in the MOST secure way?

- A. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Grant read-only IAM permissions to any AWS principals that access the S3 bucket until the designated date.
- B. Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objects.
- C. Create a new Amazon S3 bucket with S3 Versioning enabled. Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda function to replace the objects with the original versions from a private S3 bucket.
- D. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only IAM permissions to any AWS principals that access the S3 bucket.

Correct Answer: B

Community vote distribution

B (100%)

 **potomac** 3 weeks, 2 days ago

Selected Answer: B

S3 bucket policy
upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

B is correct.
A does not have S3 object lock, but deletion is prohibited, which implies object lock
C does not have S3 as static web, but have to share the s3 with the public
D mentions files - but S3 manages objects, not file
upvoted 1 times

 **hydro143** 1 month, 3 weeks ago

D?
Its like B, but also with read-only access limitations for anyone with IAM permissions. Also versioning in B doesn't help with anything.
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objects.
upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: B

Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objects.
upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: B

Clearly B.
upvoted 1 times

 **dydzah** 6 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>
upvoted 3 times

 **nonsense** 6 months, 1 week ago

Selected Answer: B

Option A allows the files to be modified or deleted by anyone with read-only IAM permissions. Option C allows the files to be modified or deleted by anyone who can trigger the AWS Lambda function.

Option D allows the files to be modified or deleted by anyone with read-only IAM permissions to the S3 bucket

upvoted 3 times

A company is making a prototype of the infrastructure for its new website by manually provisioning the necessary infrastructure. This infrastructure includes an Auto Scaling group, an Application Load Balancer and an Amazon RDS database. After the configuration has been thoroughly validated, the company wants the capability to immediately deploy the infrastructure for development and production use in two Availability Zones in an automated fashion.

What should a solutions architect recommend to meet these requirements?

- A. Use AWS Systems Manager to replicate and provision the prototype infrastructure in two Availability Zones
- B. Define the infrastructure as a template by using the prototype infrastructure as a guide. Deploy the infrastructure with AWS CloudFormation.
- C. Use AWS Config to record the inventory of resources that are used in the prototype infrastructure. Use AWS Config to deploy the prototype infrastructure into two Availability Zones.
- D. Use AWS Elastic Beanstalk and configure it to use an automated reference to the prototype infrastructure to automatically deploy new environments in two Availability Zones.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 3 months, 1 week ago

Just Think Infrastructure as Code==== Cloud Formation
upvoted 2 times

 **capino** 3 months, 1 week ago

Selected Answer: B
Just Think Infrastructure as Code==== Cloud Formation
upvoted 2 times

 **haoAWS** 5 months, 1 week ago

Why D is not correct?
upvoted 2 times

 **Kiki_Pass** 4 months ago

I guess it's because Beanstalk is PaaS (platform as a service) while CloudFormation is IaC (infrastructure as code). The question emphasis more on infrastructure
upvoted 1 times

 **wRhlH** 5 months ago

I guess "TEMPLATE" leads to CloudFormation
upvoted 2 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: B
Infrastructure as code = AWS CloudFormation
upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: B
Clearly B.
upvoted 1 times

 **Felix_br** 5 months, 3 weeks ago

Selected Answer: B
AWS CloudFormation is a service that allows you to define and provision infrastructure as code. This means that you can create a template that describes the resources you want to create, and then use CloudFormation to deploy those resources in an automated fashion.

In this case, the solutions architect should define the infrastructure as a template by using the prototype infrastructure as a guide. The template should include resources for an Auto Scaling group, an Application Load Balancer, and an Amazon RDS database. Once the template is created, the solutions architect can use CloudFormation to deploy the infrastructure in two Availability Zones.

upvoted 1 times

 **omoakin** 6 months ago

B

Define the infrastructure as a template by using the prototype infrastructure as a guide. Deploy the infrastructure with AWS CloudFormation
upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

b obvious

upvoted 4 times

Question #480

Topic 1

A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.

Which capability should the solutions architect use to meet the compliance requirements?

- A. AWS Key Management Service (AWS KMS)
- B. VPC endpoint**
- C. Private subnet
- D. Virtual private gateway

Correct Answer: B

Community vote distribution

B (100%)

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: B

Prevent traffic from traversing the internet = VPC endpoint for S3.

upvoted 2 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: B

B until proven contrary.

upvoted 1 times

 **handsonlabsaws** 5 months, 4 weeks ago

Selected Answer: B

B for sure

upvoted 2 times

 **Blingy** 6 months ago

BBBBBBBBBB

upvoted 1 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: B

A VPC endpoint enables you to privately access AWS services without requiring internet gateways, NAT gateways, VPN connections, or AWS Direct Connect connections. It allows you to connect your VPC directly to supported AWS services, such as Amazon S3, over a private connection within the AWS network.

By creating a VPC endpoint for Amazon S3, the traffic between your EC2 instances and S3 will stay within the AWS network and won't traverse the public internet. This provides a more secure and compliant solution, as the data transfer remains within the private network boundaries.

upvoted 4 times

A company hosts a three-tier web application in the AWS Cloud. A Multi-AZ Amazon RDS for MySQL server forms the database layer. Amazon ElastiCache forms the cache layer. The company wants a caching strategy that adds or updates data in the cache when a customer adds an item to the database. The data in the cache must always match the data in the database.

Which solution will meet these requirements?

- A. Implement the lazy loading caching strategy
- B. Implement the write-through caching strategy
- C. Implement the adding TTL caching strategy
- D. Implement the AWS AppConfig caching strategy

Correct Answer: B

Community vote distribution

B (100%)

 **clouduenthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: B

In the write-through caching strategy, when a customer adds or updates an item in the database, the application first writes the data to the database and then updates the cache with the same data. This ensures that the cache is always synchronized with the database, as every write operation triggers an update to the cache.

upvoted 13 times

 **clouduenthusiast** 6 months, 2 weeks ago

Lazy loading caching strategy (option A) typically involves populating the cache only when data is requested, and it does not guarantee that the data in the cache always matches the data in the database.

Adding TTL (Time-to-Live) caching strategy (option C) involves setting an expiration time for cached data. It is useful for scenarios where the data can be considered valid for a specific period, but it does not guarantee that the data in the cache is always in sync with the database.

AWS AppConfig caching strategy (option D) is a service that helps you deploy and manage application configurations. It is not specifically designed for caching data synchronization between a database and cache layer.

upvoted 18 times

 **Kp88** 4 months ago

Great explanation , thanks

upvoted 2 times

 **Guru4Cloud** Most Recent 3 months, 1 week ago

Selected Answer: B

B. Implement the write-through caching strategy

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: B

The answer is definitely B.

I couldn't provide any more details than what has been shared by @clouduenthusiast.

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

write-through caching strategy updates the cache at the same time as the database

upvoted 2 times

A company wants to migrate 100 GB of historical data from an on-premises location to an Amazon S3 bucket. The company has a 100 megabits per second (Mbps) internet connection on premises. The company needs to encrypt the data in transit to the S3 bucket. The company will store new data directly in Amazon S3.

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

- A. Use the s3 sync command in the AWS CLI to move the data directly to an S3 bucket
- B. Use AWS DataSync to migrate the data from the on-premises location to an S3 bucket
- C. Use AWS Snowball to move the data to an S3 bucket
- D. Set up an IPsec VPN from the on-premises location to AWS. Use the s3 cp command in the AWS CLI to move the data directly to an S3 bucket

Correct Answer: B

Community vote distribution

B (78%)

A (22%)

 **cludenthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: B

AWS DataSync is a fully managed data transfer service that simplifies and automates the process of moving data between on-premises storage and Amazon S3. It provides secure and efficient data transfer with built-in encryption, ensuring that the data is encrypted in transit.

By using AWS DataSync, the company can easily migrate the 100 GB of historical data from their on-premises location to an S3 bucket. DataSync will handle the encryption of data in transit and ensure secure transfer.

upvoted 6 times

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

Selected Answer: B

storage data (including metadata) is encrypted in transit, but how it's encrypted throughout the transfer depends on your source and destination locations.

upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

B is correct to migrate

A is incorrect because is it only used to upload minor files (about a few GB) to AWS. 100 GB is not appropriate.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Use AWS DataSync to migrate the data from the on-premises location to an S3 bucket

upvoted 1 times

 **HectorLeon2099** 4 months, 2 weeks ago

Selected Answer: A

B is a good option but as the volume is not large and the speed is not bad, A requires less operational overhead

upvoted 2 times

 **VellaDevil** 4 months, 3 weeks ago

Selected Answer: B

Answer A and B both are correct and with least operational overhead. But since the question says from an "On-premise Location" hence I would go with DataSync.

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: B

AWS DataSync is a secure, online service that automates and accelerates moving data between on-premises and AWS Storage services.

upvoted 1 times

 **vrevkov** 5 months, 1 week ago

Why not A?

s3 is already encrypted in transit by TLS.

We need to have the LEAST operational overhead and DataSync implies the installation of Agent whereas AWS CLI is easier to use.

upvoted 2 times

 **Smart** 3 months ago

I can think of two reasons.

- S3 does have HTTP and HTTPS endpoints available.
- DataSync offers data compression - considering the question mentions of internet bandwidth is mentioned.

upvoted 1 times

 **Axeashes** 5 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-commands.html>

upvoted 2 times

 **luiscc** 6 months, 2 weeks ago

Selected Answer: B

Using DataSync, the company can easily migrate the 100 GB of historical data to an S3 bucket. DataSync will handle the encryption of data in transit, so the company does not need to set up a VPN or worry about managing encryption keys.

Option A, using the s3 sync command in the AWS CLI to move the data directly to an S3 bucket, would require more operational overhead as the company would need to manage the encryption of data in transit themselves. Option D, setting up an IPsec VPN from the on-premises location to AWS, would also require more operational overhead and would be overkill for this scenario. Option C, using AWS Snowball, could work but would require more time and resources to order and set up the physical device.

upvoted 4 times

 **EA100** 6 months, 2 weeks ago

Answer - A

Use the s3 sync command in the AWS CLI to move the data directly to an S3 bucket.

upvoted 4 times

A company containerized a Windows job that runs on .NET 6 Framework under a Windows container. The company wants to run this job in the AWS Cloud. The job runs every 10 minutes. The job's runtime varies between 1 minute and 3 minutes.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an AWS Lambda function based on the container image of the job. Configure Amazon EventBridge to invoke the function every 10 minutes.
- B. Use AWS Batch to create a job that uses AWS Fargate resources. Configure the job scheduling to run every 10 minutes.
- C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a scheduled task based on the container image of the job to run every 10 minutes.
- D. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a standalone task based on the container image of the job. Use Windows task scheduler to run the job every 10 minutes.

Correct Answer: A

Community vote distribution

C (50%) B (30%) A (20%)

 **baba365** Highly Voted 2 months ago

Lambda supports only Linux-based container images.

<https://docs.aws.amazon.com/lambda/latest/dg/images-create.html>
upvoted 6 times

 **kt7** Most Recent 2 weeks ago

Selected Answer: B
Batch supports fargate now
upvoted 1 times

 **ccmc** 3 weeks, 5 days ago

Selected Answer: B
aws batch supports fargate
upvoted 1 times

 **deecheon** 2 months, 4 weeks ago

Selected Answer: C
C works. For A, the lambda support container image, but the container image must implement the Lambda Runtime API.
upvoted 1 times

 **markoniz** 2 months, 2 weeks ago

Absolutely agree with this one ... Lambda does not support Windows container, on the other hand ECS is adequate solution
upvoted 2 times

 **Hades2231** 3 months ago

Selected Answer: B
As they support Batch on Fargate now (Aug 2023), the correct answer should be B?
upvoted 2 times

 **RDM10** 2 months, 1 week ago

that's exactly my question too.
In one of the discussions, they said lambda is for jobs up to 15 min. But for other questions, they said batch is the best. I do not understand why we can't use batch?
upvoted 1 times

 **Smart** 3 months ago

Selected Answer: A
<https://docs.aws.amazon.com/lambda/latest/dg/csharp-image.html#csharp-image-clients>
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C is the most cost-effective solution for running a short-lived Windows container job on a schedule.

Using Amazon ECS scheduled tasks on Fargate eliminates the need to provision EC2 resources. You pay only for the duration the task runs.

Scheduled tasks handle scheduling the jobs and scaling resources automatically. This is lower cost than managing your own scaling via Lambda or Batch.

ECS also supports Windows containers natively unlike Lambda (option A).

Option D still requires provisioning and paying for full time EC2 resources to run a task scheduler even when tasks are not running.
upvoted 1 times

✉  **cd93** 3 months, 1 week ago

August 2023, AWS Batch now support Windows container

<https://docs.aws.amazon.com/batch/latest/userguide/fargate.html#when-to-use-fargate>

upvoted 1 times

✉  **cd93** 3 months ago

<https://aws.amazon.com/blogs/containers/running-windows-containers-with-amazon-ecs-on-aws-fargate/>

upvoted 1 times

✉  **wRhlH** 5 months ago

For those wonder why not B

AWS Batch doesn't support Windows containers on either Fargate or EC2 resources.

<https://docs.aws.amazon.com/batch/latest/userguide/fargate.html#when-to-use-fargate:~:text=AWS%20Batch%20doesn%27t%20support%20Windows%20containers%20on%20either%20Fargate%20or%20EC2%20resources.>

upvoted 2 times

✉  **lemur88** 3 months ago

They have now added support, which now makes B true?

<https://aws.amazon.com/about-aws/whats-new/2023/07/aws-batch-fargate-linux-arm64-windows-x86-containers-cli-sdk/>

upvoted 1 times

✉  **cyber_bedouin** 1 month, 1 week ago

the actual exam is not up-to-date, it came out in August 30, 2022

upvoted 1 times

✉  **mattcl** 5 months, 1 week ago

A: Lambda supports containerized applications

upvoted 2 times

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

Selected Answer: C

AWS Fargate will bill you based on the amount of vCPU, RAM, OS, CPU architecture, and storage that your containerized apps consume while running on EKS or ECS. From the time you start downloading a container image until the ECS task or EKS pod ends.

Lambda is also an option but will involve some re-architecting, so why take the long route?

upvoted 1 times

✉  **TariqKipkemei** 3 weeks, 1 day ago

Also, Lambda does not support windows-based container images.

<https://docs.aws.amazon.com/lambda/latest/dg/images-create.html#:~:text=Lambda%20supports%20only-,Linux%2Dbased,-container%20images.>

upvoted 1 times

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

Selected Answer: A

The previous status for the company app is within containerization technology using .Net. Now the company wants to use one of AWS solution (should not be ECS), so one easy possibility is using Lambda with EventBridge as option "A" declared !

upvoted 1 times

✉  **Ale1973** 3 months, 2 weeks ago

But, scenario says "Create an AWS Lambda function based on the container image of the job", then, I must assume that it is exactly the same image, not a new image based on it...

upvoted 1 times

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

Furthermore, Lambda can create "Container Image" appropriate for the company containerized app.

upvoted 1 times

✉  **AnishGS** 5 months, 2 weeks ago

Selected Answer: C

By leveraging AWS Fargate and ECS, you can achieve cost-effective scaling and resource allocation for your containerized Windows job running on .NET 6 Framework in the AWS Cloud. The serverless nature of Fargate ensures that you only pay for the actual resources consumed by your containers, allowing for efficient cost management.

upvoted 1 times

✉  **Axeashes** 5 months, 2 weeks ago

Selected Answer: C

came across this study: <https://blogs.perficient.com/2021/06/17/aws-cost-analysis-comparing-lambda-ec2-fargate/>
Indicating Fargate as a lower cost than Lamda for little or no idle time - I believe that is the case. .NET6 seems supported on both Lamda and Fargate.

upvoted 2 times

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

By utilizing AWS Fargate to run the containerized Windows job on .NET 6 Framework, and scheduling it using CloudWatch Events, you can achieve cost-effective execution while meeting the job's requirements. C is the answer

upvoted 1 times

✉  **omoakin** 6 months ago

CCCCCCCCCC

upvoted 2 times

✉  **PRASAD180** 6 months ago

100% C crt

upvoted 2 times

A company wants to move from many standalone AWS accounts to a consolidated, multi-account architecture. The company plans to create many new AWS accounts for different business units. The company needs to authenticate access to these AWS accounts by using a centralized corporate directory service.

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

- A. Create a new organization in AWS Organizations with all features turned on. Create the new AWS accounts in the organization.
- B. Set up an Amazon Cognito identity pool. Configure AWS IAM Identity Center (AWS Single Sign-On) to accept Amazon Cognito authentication.
- C. Configure a service control policy (SCP) to manage the AWS accounts. Add AWS IAM Identity Center (AWS Single Sign-On) to AWS Directory Service.
- D. Create a new organization in AWS Organizations. Configure the organization's authentication mechanism to use AWS Directory Service directly.
- E. Set up AWS IAM Identity Center (AWS Single Sign-On) in the organization. Configure IAM Identity Center, and integrate it with the company's corporate directory service.

Correct Answer: AE

Community vote distribution

AE (100%)

 **cloudepthusiast**  6 months, 2 weeks ago

Selected Answer: AE

- A. By creating a new organization in AWS Organizations, you can establish a consolidated multi-account architecture. This allows you to create and manage multiple AWS accounts for different business units under a single organization.
- E. Setting up AWS IAM Identity Center (AWS Single Sign-On) within the organization enables you to integrate it with the company's corporate directory service. This integration allows for centralized authentication, where users can sign in using their corporate credentials and access the AWS accounts within the organization.

Together, these actions create a centralized, multi-account architecture that leverages AWS Organizations for account management and AWS IAM Identity Center (AWS Single Sign-On) for authentication and access control.

upvoted 8 times

 **Guru4Cloud**  3 months, 1 week ago

Selected Answer: AE

- A) Using AWS Organizations allows centralized management of multiple AWS accounts in a single organization. New accounts can easily be created within the organization.
- E) Integrating AWS IAM Identity Center (AWS SSO) with the company's corporate directory enables federated single sign-on. Users can log in once to access accounts and resources across AWS.

Together, Organizations and IAM Identity Center provide consolidated management and authentication for multiple accounts using existing corporate credentials.

upvoted 1 times

 **samehpalass** 5 months, 1 week ago

Selected Answer: AE

- A:AWS Organization
- E:Authentication because option C (SCP) for Authorization

upvoted 2 times

 **baba365** 4 months, 3 weeks ago

Ans: CD

'centralized corporate directory service' with new accounts in AWS Organizations

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

Selected Answer: AE

- Create a new organization in AWS Organizations with all features turned on. Create the new AWS accounts in the organization.
- Set up AWS IAM Identity Center (AWS Single Sign-On) in the organization. Configure IAM Identity Center, and integrate it with the company's corporate directory service.

AWS IAM Identity Center (successor to AWS Single Sign-On) helps you securely create or connect your workforce identities and manage their access centrally across AWS accounts and applications.

[https://aws.amazon.com/iam/identity-center/#:~:text=AWS%20IAM%20Identity%20Center%20\(successor%20to%20AWS%20Single%20Sign%20On\)%20helps%20you%20securely%20create%20or%20connect%20your%20workforce%20identities%20and%20manage%20their%20access%20centrally%20across%20AWS%20accounts%20and%20applications.](https://aws.amazon.com/iam/identity-center/#:~:text=AWS%20IAM%20Identity%20Center%20(successor%20to%20AWS%20Single%20Sign%20On)%20helps%20you%20securely%20create%20or%20connect%20your%20workforce%20identities%20and%20manage%20their%20access%20centrally%20across%20AWS%20accounts%20and%20applications.)

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

ae is right

upvoted 1 times

A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.

What is the MOST cost-effective solution?

- A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
- B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
- C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: C

Community vote distribution

A (100%)

✉  **clouduenthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: A

By choosing Expedited retrievals in Amazon S3 Glacier, you can reduce the retrieval time to minutes, making it suitable for scenarios where quick access is required. Expedited retrievals come with a higher cost per retrieval compared to standard retrievals but provide faster access to your archived data.

upvoted 7 times

✉  **ngo01214** Most Recent 1 month, 2 weeks ago

s3 expedited can only be applied on glacier flexible retrieval storage class and s3 intelligent tiering archive access tier. so the answer should be C
upvoted 1 times

✉  **Smart** 3 months ago

Selected Answer: A

I am going with option A, but it is a poorly written question. "For all but the largest archives (more than 250 MB), data accessed by using Expedited retrievals is typically made available within 1–5 minutes."

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

Answer - A

Fast availability: Although retrieval times for objects stored in Amazon S3 Glacier typically range from minutes to hours, you can use the Expedited retrievals option to expedite access to your archives. By using Expedited retrievals, the files can be made available in a maximum of five minutes when needed. However, Expedited retrievals do incur higher costs compared to standard retrievals.

upvoted 1 times

✉  **hsinchang** 4 months ago

Selected Answer: A

Expedited retrievals are designed for urgent requests and can provide access to data in as little as 1-5 minutes for most archive objects. Standard retrievals typically finish within 3-5 hours for objects stored in the S3 Glacier Flexible Retrieval storage class or S3 Intelligent-Tiering Archive Access tier. These retrievals typically finish within 12 hours for objects stored in the S3 Glacier Deep Archive storage class or S3 Intelligent-Tiering Deep Archive Access tier. So A.

upvoted 2 times

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

Selected Answer: A

Expedited retrievals allow you to quickly access your data that's stored in the S3 Glacier Flexible Retrieval storage class or the S3 Intelligent-Tiering Archive Access tier when occasional urgent requests for restoring archives are required. Data accessed by using Expedited retrievals is typically made available within 1–5 minutes.

upvoted 1 times

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

Selected Answer: A

A for sure!

upvoted 1 times

✉  **Doyin8807** 6 months ago

C because A is not the most cost effective

upvoted 1 times

 **luiscc** 6 months, 2 weeks ago

Selected Answer: A

Expedited retrieval typically takes 1-5 minutes to retrieve data, making it suitable for the company's requirement of having the files available in a maximum of five minutes.

upvoted 4 times

 **Efren** 6 months, 2 weeks ago

Selected Answer: A

Glacier expedite

upvoted 2 times

 **EA100** 6 months, 2 weeks ago

Answer - A

Fast availability: Although retrieval times for objects stored in Amazon S3 Glacier typically range from minutes to hours, you can use the Expedited retrievals option to expedite access to your archives. By using Expedited retrievals, the files can be made available in a maximum of five minutes when needed. However, Expedited retrievals do incur higher costs compared to standard retrievals.

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

glacier expedited retrieval times of typically 1-5 minutes.

upvoted 4 times

 **wsdasdasdqwdaw** 1 month ago

Fully agree. Check here for evidences: <https://aws.amazon.com/s3/storage-classes/glacier/#:~:text=S3%20Glacier%20Flexible%20Retrieval%20provides,amounts%20of%20data%20typically%20in>

upvoted 1 times

A company is building a three-tier application on AWS. The presentation tier will serve a static website. The logic tier is a containerized application. This application will store data in a relational database. The company wants to simplify deployment and to reduce operational costs.

Which solution will meet these requirements?

- A. Use Amazon S3 to host static content. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.
- B. Use Amazon CloudFront to host static content. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.
- C. Use Amazon S3 to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.
- D. Use Amazon EC2 Reserved Instances to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

ECS is slightly cheaper than EKS

upvoted 6 times

✉  **wsdasdasdqwdaw**  1 month ago

Why not B ?

upvoted 1 times

✉  **wsdasdasdqwdaw** 1 month ago

Aaa I got it. With CF we are adding additional cost => A.

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

Use Amazon S3 to host static content. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.

upvoted 1 times

✉  **jaydesai8** 4 months, 2 weeks ago

Selected Answer: A

S3= hosting static contents

Ecs = Little cheaper than EKS

RDS = Database

upvoted 1 times

✉  **TariqKipkemei** 5 months ago

Selected Answer: A

Use Amazon S3 to host static content. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database

upvoted 1 times

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

Selected Answer: A

Amazon S3 is a highly scalable and cost-effective storage service that can be used to host static website content. It provides durability, high availability, and low latency access to the static files.

Amazon ECS with AWS Fargate eliminates the need to manage the underlying infrastructure. It allows you to run containerized applications without provisioning or managing EC2 instances. This reduces operational overhead and provides scalability.

By using a managed Amazon RDS cluster for the database, you can offload the management tasks such as backups, patching, and monitoring to AWS. This reduces the operational burden and ensures high availability and durability of the database.

upvoted 4 times

A company seeks a storage solution for its application. The solution must be highly available and scalable. The solution also must function as a file system be mountable by multiple Linux instances in AWS and on premises through native protocols, and have no minimum size requirements. The company has set up a Site-to-Site VPN for access from its on-premises network to its VPC.

Which storage solution meets these requirements?

- A. Amazon FSx Multi-AZ deployments
- B. Amazon Elastic Block Store (Amazon EBS) Multi-Attach volumes
- C. Amazon Elastic File System (Amazon EFS) with multiple mount targets
- D. Amazon Elastic File System (Amazon EFS) with a single mount target and multiple access points

Correct Answer: C

Community vote distribution

C (100%)

✉  **Felix_br** Highly Voted 5 months, 3 weeks ago

Selected Answer: C

The other options are incorrect for the following reasons:

- A. Amazon FSx Multi-AZ deployments Amazon FSx is a managed file system service that provides access to file systems that are hosted on Amazon EC2 instances. Amazon FSx does not support native protocols, such as NFS.
- B. Amazon Elastic Block Store (Amazon EBS) Multi-Attach volumes Amazon EBS is a block storage service that provides durable, block-level storage volumes for use with Amazon EC2 instances. Amazon EBS Multi-Attach volumes can be attached to multiple EC2 instances at the same time, but they cannot be mounted by multiple Linux instances through native protocols, such as NFS.
- D. Amazon Elastic File System (Amazon EFS) with a single mount target and multiple access points A single mount target can only be used to mount the file system on a single EC2 instance. Multiple access points are used to provide access to the file system from different VPCs.

upvoted 6 times

✉  **unbendable** 1 month ago

Amazon FSx ONTAP supports clients mounting it with NFS. <https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/attach-linux-client.html>. Though A is not clear about which FSx product is used

upvoted 1 times

✉  **cloudenthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: C

Amazon EFS is a fully managed file system service that provides scalable, shared storage for Amazon EC2 instances. It supports the Network File System version 4 (NFSv4) protocol, which is a native protocol for Linux-based systems. EFS is designed to be highly available, durable, and scalable.

upvoted 6 times

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

EFS POSIX LINUX

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

- C. Amazon Elastic File System (Amazon EFS) with multiple mount targets

upvoted 2 times

✉  **boubie44** 6 months, 1 week ago

i don't understand why not D?

upvoted 1 times

✉  **lucdt4** 6 months ago

the requirement is mountable by multiple Linux
-> C (multiple mount targets)

upvoted 2 times

A 4-year-old media company is using the AWS Organizations all features feature set to organize its AWS accounts. According to the company's finance team, the billing information on the member accounts must not be accessible to anyone, including the root user of the member accounts.

Which solution will meet these requirements?

- A. Add all finance team users to an IAM group. Attach an AWS managed policy named Billing to the group.
- B. Attach an identity-based policy to deny access to the billing information to all users, including the root user.
- C. Create a service control policy (SCP) to deny access to the billing information. Attach the SCP to the root organizational unit (OU).
- D. Convert from the Organizations all features feature set to the Organizations consolidated billing feature set.

Correct Answer: C

Community vote distribution

C (100%)

 **potomac** 3 weeks, 2 days ago

Selected Answer: C

SCP is for authorization

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C. Create a service control policy (SCP) to deny access to the billing information. Attach the SCP to the root organizational unit (OU)

upvoted 1 times

 **Kiki_Pass** 4 months ago

but SCP do not apply to the management account (full admin power)?

upvoted 1 times

 **PRASAD180** 5 months ago

C Crt 100%

upvoted 1 times

 **TariqKipkemei** 5 months ago

Selected Answer: C

Service control policy are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization. SCPs help you to ensure your accounts stay within your organization's access control guidelines. SCPs are available only in an organization that has all features enabled.

upvoted 1 times

 **Abrar2022** 5 months, 3 weeks ago

By denying access to billing information at the root OU, you can ensure that no member accounts, including root users, have access to the billing information.

upvoted 1 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: C

Service Control Policies (SCP): SCPs are an integral part of AWS Organizations and allow you to set fine-grained permissions on the organizational units (OUs) within your AWS Organization. SCPs provide central control over the maximum permissions that can be granted to member accounts, including the root user.

Denying Access to Billing Information: By creating an SCP and attaching it to the root OU, you can explicitly deny access to billing information for all accounts within the organization. SCPs can be used to restrict access to various AWS services and actions, including billing-related services.

Granular Control: SCPs enable you to define specific permissions and restrictions at the organizational unit level. By denying access to billing information at the root OU, you can ensure that no member accounts, including root users, have access to the billing information.

upvoted 3 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: C

c for me

upvoted 1 times

An ecommerce company runs an application in the AWS Cloud that is integrated with an on-premises warehouse solution. The company uses Amazon Simple Notification Service (Amazon SNS) to send order messages to an on-premises HTTPS endpoint so the warehouse application can process the orders. The local data center team has detected that some of the order messages were not received.

A solutions architect needs to retain messages that are not delivered and analyze the messages for up to 14 days.

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

- A. Configure an Amazon SNS dead letter queue that has an Amazon Kinesis Data Stream target with a retention period of 14 days.
- B. Add an Amazon Simple Queue Service (Amazon SQS) queue with a retention period of 14 days between the application and Amazon SNS.
- C. Configure an Amazon SNS dead letter queue that has an Amazon Simple Queue Service (Amazon SQS) target with a retention period of 14 days.
- D. Configure an Amazon SNS dead letter queue that has an Amazon DynamoDB target with a TTL attribute set for a retention period of 14 days.

Correct Answer: C

Community vote distribution

C (52%) B (48%)

✉  **daniel1** 1 month ago

Selected Answer: C

GPT4 to the rescue:

The most appropriate solution would be to configure an Amazon SNS dead letter queue with an Amazon Simple Queue Service (Amazon SQS) target with a retention period of 14 days (Option C). This setup would ensure that any undelivered messages are retained in the SQS queue for up to 14 days for analysis, with minimal development effort required.

upvoted 1 times

✉  **Wayne23Fang** 1 month, 1 week ago

Selected Answer: B

I like (B) since it is put SQS before SNS so we could prepare for retention. (C) dead letter Queue is kind of "rescue" effort. Also (C) should mention reprocessing dead letter.

upvoted 1 times

✉  **thanhnv142** 1 month, 1 week ago

C is correct. It used a combination of SNS and SQS so it better than B.

upvoted 1 times

✉  **iwannabeawsgod** 1 month, 1 week ago

Selected Answer: C

C is the answer

upvoted 1 times

✉  **Devsin2000** 2 months, 1 week ago

B is correct Answer. SQS Retain messages in queues for up to 14 days

C is incorrect because there is nothing called Amazon SNS dead letter queue

upvoted 2 times

✉  **RDM10** 2 months, 1 week ago

<https://docs.aws.amazon.com/sns/latest/dg/sns-configure-dead-letter-queue.html>

upvoted 3 times

✉  **lemur88** 3 months ago

Selected Answer: C

<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C. Configure an Amazon SNS dead letter queue that has an Amazon Simple Queue Service (Amazon SQS) target with a retention period of 14 days. By using an Amazon SQS queue as the target for the dead letter queue, you ensure that the undelivered messages are reliably stored in a queue for up to 14 days. Amazon SQS allows you to specify a retention period for messages, which meets the retention requirement without additional development effort.

upvoted 1 times

✉  **mtmayer** 3 months, 2 weeks ago

Selected Answer: B

Dead Letter is a SQS feature not SNS.

A dead-letter queue is an Amazon SQS queue that an Amazon SNS subscription can target for messages that can't be delivered to subscribers successfully. Messages that can't be delivered due to client errors or server errors are held in the dead-letter queue for further analysis or reprocessing. For more information, see Configuring an Amazon SNS dead-letter queue for a subscription and Amazon SNS message delivery retries.

<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>

upvoted 3 times

✉  **xyb** 3 months, 3 weeks ago

Selected Answer: B

In SNS, DLQs store the messages that failed to be delivered to subscribed endpoints. For more information, see Amazon SNS Dead-Letter Queues.

In SQS, DLQs store the messages that failed to be processed by your consumer application. This failure mode can happen when producers and consumers fail to interpret aspects of the protocol that they use to communicate. In that case, the consumer receives the message from the queue, but fails to process it, as the message doesn't have the structure or content that the consumer expects. The consumer can't delete the message from the queue either. After exhausting the receive count in the redrive policy, SQS can sideline the message to the DLQ. For more information, see Amazon SQS Dead-Letter Queues.

<https://aws.amazon.com/blogs/compute/designing-durable-serverless-apps-with-dlqs-for-amazon-sns-amazon-sqs-aws-lambda/>

upvoted 2 times

✉  **TariqKipkemei** 5 months ago

C is best to handle this requirement. Although good to note that dead-letter queue is an SQS queue.

"A dead-letter queue is an Amazon SQS queue that an Amazon SNS subscription can target for messages that can't be delivered to subscribers successfully. Messages that can't be delivered due to client errors or server errors are held in the dead-letter queue for further analysis or reprocessing."

<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html#:~:text=A%20dead%2Dletter%20queue%20is%20an%20Amazon%20SQS%20queue>

upvoted 1 times

✉  **Felix_br** 5 months, 3 weeks ago

C - Amazon SNS dead letter queues are used to handle messages that are not delivered to their intended recipients. When a message is sent to an Amazon SNS topic, it is first delivered to the topic's subscribers. If a message is not delivered to any of the subscribers, it is sent to the topic's dead letter queue.

Amazon SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Amazon SQS queues can be configured to have a retention period, which is the amount of time that messages will be kept in the queue before they are deleted.

To meet the requirements of the company, you can configure an Amazon SNS dead letter queue that has an Amazon SQS target with a retention period of 14 days. This will ensure that any messages that are not delivered to the on-premises warehouse application will be stored in the Amazon SQS queue for up to 14 days. The company can then analyze the messages in the Amazon SQS queue to determine why they were not delivered.

upvoted 2 times

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

Selected Answer: C

<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>

upvoted 2 times

✉  **Rob1L** 6 months, 1 week ago

Selected Answer: C

The message retention period in Amazon SQS can be set between 1 minute and 14 days (the default is 4 days). Therefore, you can configure your SQS DLQ to retain undelivered SNS messages for 14 days. This will enable you to analyze undelivered messages with the least development effort.

upvoted 4 times

✉  **nonsense** 6 months, 2 weeks ago

Selected Answer: C

A is a good solution, but it requires to modify the application. The application would need to be modified to send messages to the Amazon Kinesis Data Stream instead of the on-premises HTTPS endpoint.

Option B is not a good solution. The application would need to be modified to send messages to the Amazon SQS queue instead of the on-premises HTTPS endpoint.

Option D is not a good solution because Amazon DynamoDB is not designed for storing messages for long periods of time.

Option C is the best solution because it does not require any changes to the application

upvoted 1 times

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

Selected Answer: B

By adding an Amazon SQS queue as an intermediary between the application and Amazon SNS, you can retain undelivered messages for analysis. Amazon SQS provides a built-in retention period that allows you to specify how long messages should be retained in the queue. By setting the retention period to 14 days, you can ensure that the undelivered messages are available for analysis within that timeframe. This solution requires minimal development effort as it leverages Amazon SQS's capabilities without the need for custom code development.

upvoted 4 times

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

Amazon Simple Notification Service (Amazon SNS) does not directly support dead letter queues. The dead letter queue feature is available in services like Amazon Simple Queue Service (Amazon SQS) and AWS Lambda, but not in Amazon SNS.

upvoted 2 times

✉  **Efren** 6 months, 1 week ago

Agree with you

A dead-letter queue is an Amazon SQS queue that an Amazon SNS subscription can target for messages that can't be delivered to subscribers successfully.

upvoted 1 times

✉  **Efren** 6 months, 2 weeks ago

ChatGP says is SQS.. not sure

upvoted 1 times

✉  **Efren** 6 months, 2 weeks ago

D for me. you send to SQS and then what? needs to send it to some service where can be readed, if im not wrong

upvoted 1 times

A gaming company uses Amazon DynamoDB to store user information such as geographic location, player data, and leaderboards. The company needs to configure continuous backups to an Amazon S3 bucket with a minimal amount of coding. The backups must not affect availability of the application and must not affect the read capacity units (RCUs) that are defined for the table.

Which solution meets these requirements?

- A. Use an Amazon EMR cluster. Create an Apache Hive job to back up the data to Amazon S3.
- B. Export the data directly from DynamoDB to Amazon S3 with continuous backups. Turn on point-in-time recovery for the table.
- C. Configure Amazon DynamoDB Streams. Create an AWS Lambda function to consume the stream and export the data to an Amazon S3 bucket.
- D. Create an AWS Lambda function to export the data from the database tables to Amazon S3 on a regular basis. Turn on point-in-time recovery for the table.

Correct Answer: B

Community vote distribution

B (79%)

C (21%)

✉  **elmogy**  6 months ago

Selected Answer: B

Continuous backups is a native feature of DynamoDB, it works at any scale without having to manage servers or clusters and allows you to export data across AWS Regions and accounts to any point-in-time in the last 35 days at a per-second granularity. Plus, it doesn't affect the read capacity or the availability of your production tables.

<https://aws.amazon.com/blogs/aws/new-export-amazon-dynamodb-table-data-to-data-lake-amazon-s3/>
upvoted 5 times

✉  **potomac**  3 weeks, 2 days ago

Selected Answer: B

DynamoDB export to S3 is a fully managed solution for exporting DynamoDB data to an Amazon S3 bucket at scale.
upvoted 1 times

✉  **baba365** 2 months ago

A DynamoDB stream is an ordered flow of information about changes to items in a DynamoDB table... for C.U.D events (Create, Update, Delete) and its logs are retained for only 24hrs .
upvoted 2 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Export the data directly from DynamoDB to Amazon S3 with continuous backups. Turn on point-in-time recovery for the table.
upvoted 1 times

✉  **ukivanlampli** 3 months, 3 weeks ago

Selected Answer: C

continous backup, no impact to availability ==> DynamoDB stream
B. export is one off, noy continuous and demand on read capacity
upvoted 4 times

✉  **hsinchang** 4 months ago

minimal amount of coding rules out Lambda
upvoted 2 times

✉  **Chris22usa** 5 months ago

ChatGpt answer is C and it indicates continuous backup process uses DynamoDB stream actually
upvoted 2 times

✉  **TariqKipkemei** 5 months ago

Selected Answer: B

Using DynamoDB table export, you can export data from an Amazon DynamoDB table from any time within your point-in-time recovery window to an Amazon S3 bucket. Exporting a table does not consume read capacity on the table, and has no impact on table performance and availability.
upvoted 1 times

✉  **norris81** 6 months ago

Selected Answer: B

<https://repost.aws/knowledge-center/back-up-dynamodb-s3>

<https://aws.amazon.com/blogs/aws/new-amazon-dynamodb-continuous-backups-and-point-in-time-recovery-pitr/>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html>

There is no edit

upvoted 2 times

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

Selected Answer: B

Continuous Backups: DynamoDB provides a feature called continuous backups, which automatically backs up your table data. Enabling continuous backups ensures that your table data is continuously backed up without the need for additional coding or manual interventions.

Export to Amazon S3: With continuous backups enabled, DynamoDB can directly export the backups to an Amazon S3 bucket. This eliminates the need for custom coding to export the data.

Minimal Coding: Option B requires the least amount of coding effort as continuous backups and the export to Amazon S3 functionality are built-in features of DynamoDB.

No Impact on Availability and RCUs: Enabling continuous backups and exporting data to Amazon S3 does not affect the availability of your application or the read capacity units (RCUs) defined for the table. These operations happen in the background and do not impact the table's performance or consume additional RCUs.

upvoted 3 times

✉ **Efren** 6 months, 2 weeks ago

Selected Answer: B

DynamoDB Export to S3 feature

Using this feature, you can export data from an Amazon DynamoDB table anytime within your point-in-time recovery window to an Amazon S3 bucket.

upvoted 2 times

✉ **Efren** 6 months, 2 weeks ago

B also for me

upvoted 2 times

✉ **norris81** 6 months, 2 weeks ago

<https://repost.aws/knowledge-center/back-up-dynamodb-s3>

<https://aws.amazon.com/blogs/aws/new-amazon-dynamodb-continuous-backups-and-point-in-time-recovery-pitr/>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html>

upvoted 1 times

✉ **Efren** 6 months, 2 weeks ago

you could mention what is the best answer from you :)

upvoted 1 times

A solutions architect is designing an asynchronous application to process credit card data validation requests for a bank. The application must be secure and be able to process each request at least once.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS Key Management Service (SSE-KMS) for encryption. Add the kms:Decrypt permission for the Lambda execution role.
- B. Use AWS Lambda event source mapping. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use SQS managed encryption keys (SSE-SQS) for encryption. Add the encryption key invocation permission for the Lambda function.
- C. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use AWS KMS keys (SSE-KMS). Add the kms:Decrypt permission for the Lambda execution role.
- D. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS KMS keys (SSE-KMS) for encryption. Add the encryption key invocation permission for the Lambda function.

Correct Answer: A

Community vote distribution

A (62%)	B (35%)	4%
---------	---------	----

✉  **Guru4Cloud**  3 months, 1 week ago

Selected Answer: B

Using SQS FIFO queues ensures each message is processed at least once in order. SSE-SQS provides encryption that is handled entirely by SQS without needing decrypt permissions.

Standard SQS queues (Options A and D) do not guarantee order.

Using KMS keys (Options C and D) requires providing the Lambda role with decrypt permissions, adding complexity.

SQS FIFO queues with SSE-SQS encryption provide orderly, secure, server-side message processing that Lambda can consume without needing to manage decryption. This is the most efficient and cost-effective approach.

upvoted 5 times

✉  **Clouddon** 2 months, 1 week ago

Amazon SQS offers standard as the default queue type. Standard queues support a nearly unlimited number of API calls per second, per API action (SendMessage, ReceiveMessage, or DeleteMessage). Standard queues support at-least-once message delivery. However, occasionally (because of the highly distributed architecture that allows nearly unlimited throughput), more than one copy of a message might be delivered out of order. Standard queues provide best-effort ordering which ensures that messages are generally delivered in the same order as they're sent. Whereas, FIFO (First-In-First-Out) queues have all the capabilities of the standard queues, but are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated. (is correct)

upvoted 2 times

✉  **EdenWang**  1 week, 6 days ago

Selected Answer: B

With the SSE-SQS encryption type, you do not need to create, manage, or pay for SQS-managed encryption keys.

upvoted 1 times

✉  **wsdasdasdqwdaw** 1 month ago

Initially though it is B, but it is said that the messages should be processed at least once, not the same order, and Standard SQS is "almost" FIFO, which changed my opinion and I would go with A as correct.

upvoted 2 times

✉  **BrijMohan08** 2 months, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/standard-queues.html>

upvoted 3 times

✉  **hsinchang** 4 months ago

Least Privilege Policy leads to A over D.

upvoted 1 times

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

Selected Answer: B

Considering this is credit card validation process, there needs to be a strict 'process exactly once' policy offered by the SQS FIFO, and also SQS already supports server-side encryption with customer-provided encryption keys using the AWS Key Management Service (SSE-KMS) or using SQS-

owned encryption keys (SSE-SQS). Both encryption options greatly reduce the operational burden and complexity involved in protecting data. Additionally, with the SSE-SQS encryption type, you do not need to create, manage, or pay for SQS-managed encryption keys. Therefore option B stands out for me.

upvoted 1 times

✉ **TariqKipkemei** 3 weeks ago

I retract my answer and change it to A, there is a requirement to process each request 'at least once'. Only standard queues can deliver messages at least once.

There is also a requirement for the most 'cost-effective' option. Standard queues are the cheaper option.

<https://aws.amazon.com/sqs/pricing/#:~:text=SQS%20requests%20priced%3F>

upvoted 1 times

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

Selected Answer: A

https://docs.aws.amazon.com/zh_tw/AWSSimpleQueueService/latest/SQSDriverGuide/sqs-least-privilege-policy.html

upvoted 1 times

✉ **Abrar2022** 5 months, 3 weeks ago

Selected Answer: A

at least once and cost effective suggests SQS standard

upvoted 1 times

✉ **Felix_br** 5 months, 3 weeks ago

Selected Answer: B

Solution B is the most cost-effective solution to meet the requirements of the application.

Amazon Simple Queue Service (SQS) FIFO queues are a good choice for this application because they guarantee that messages are processed in the order in which they are received. This is important for credit card data validation because it ensures that fraudulent transactions are not processed before legitimate transactions.

SQS managed encryption keys (SSE-SQS) are a good choice for encrypting the messages in the SQS queue because they are free to use. AWS Key Management Service (KMS) keys (SSE-KMS) are also a good choice for encrypting the messages, but they do incur a cost.

upvoted 2 times

✉ **omoakin** 6 months ago

AAAAAAA

upvoted 1 times

✉ **elmogy** 6 months ago

Selected Answer: A

SQS FIFO is slightly more expensive than standard queue

<https://calculator.aws/#/addService/SQS>

I would still go with the standard because of the keyword "at least once" because FIFO process "exactly once". That leaves us with A and D, I believe that lambda function only needs to decrypt so I would choose A

upvoted 4 times

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

Selected Answer: A

should be A. Key word - at least once and cost effective suggests SQS standard

upvoted 2 times

✉ **Efren** 6 months, 1 week ago

It has to be default, no FIFO. It doesn't say just one, it says at least once, so that is default queue that is cheaper than FIFO. Between the default options, not sure to be honest

upvoted 2 times

✉ **jayce5** 6 months ago

No, when it comes to "credit card data validation," it should be FIFO. If you use the standard approach, there is a chance that people who come after will get processed before those who come first.

upvoted 1 times

✉ **awwass** 6 months, 1 week ago

Selected Answer: A

I guess A

upvoted 1 times

✉ **awwass** 6 months, 1 week ago

This solution uses standard queues in Amazon SQS, which are less expensive than FIFO queues. It also uses AWS Key Management Service (SSE-KMS) for encryption, which is a cost-effective way to encrypt data at rest and in transit. The kms:Decrypt permission is added to the Lambda execution role to allow it to decrypt messages from the queue

upvoted 1 times

✉ **Rob1L** 6 months, 1 week ago

Selected Answer: A

Options B, C and D involve using SQS FIFO queues, which guarantee exactly once processing, which is more expensive and more than necessary for the requirement of at least once processing.

upvoted 4 times

 **Efren** 6 months, 2 weeks ago

For me its b, kms:decrypt is an action

upvoted 3 times

 **nonsense** 6 months, 2 weeks ago

not add the kms:Decrypt permission for the Lambda execution role, which means that Lambda will have to decrypt the data on each invocation

upvoted 2 times

 **Efren** 6 months, 1 week ago

ID say then A

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: C

I guess c

upvoted 1 times

A company has multiple AWS accounts for development work. Some staff consistently use oversized Amazon EC2 instances, which causes the company to exceed the yearly budget for the development accounts. The company wants to centrally restrict the creation of AWS resources in these accounts.

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

- A. Develop AWS Systems Manager templates that use an approved EC2 creation process. Use the approved Systems Manager templates to provision EC2 instances.
- B. Use AWS Organizations to organize the accounts into organizational units (OUs). Define and attach a service control policy (SCP) to control the usage of EC2 instance types.
- C. Configure an Amazon EventBridge rule that invokes an AWS Lambda function when an EC2 instance is created. Stop disallowed EC2 instance types.
- D. Set up AWS Service Catalog products for the staff to create the allowed EC2 instance types. Ensure that staff can deploy EC2 instances only by using the Service Catalog products.

Correct Answer: B

Community vote distribution

B (92%) 8%

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Use AWS Organizations to organize the accounts into organizational units (OUs). Define and attach a service control policy (SCP) to control the usage of EC2 instance types.

upvoted 1 times

 **Ale1973** 3 months, 2 weeks ago

Selected Answer: D

I have a question regarding this answer, what do they mean by "development effort":

If they mean the work it takes to implement the solution (using develop as implement), option B achieves the constraint with little administrative overhead (there is less to do to configure this option).

If by "development effort", they mean less effort for the development team, when development team try to deploy instances and gets errors because they are not allowed, this generates overhead. In this case the best option is D.

What did you think?

upvoted 1 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: B

Use AWS Organizations to organize the accounts into organizational units (OUs). Define and attach a service control policy (SCP) to control the usage of EC2 instance types

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: B

Anytime you see Multiple AWS Accounts, and needs to consolidate is AWS Organization. Also anytime we need to restrict anything in an organization, it is SCP policies.

upvoted 3 times

 **Blingy** 6 months ago

BBBBBBBBBB

upvoted 1 times

 **elmogy** 6 months ago

Selected Answer: B

I would choose B

The other options would require some level of programming or custom resource creation:

- A. Developing Systems Manager templates requires development effort
- C. Configuring EventBridge rules and Lambda functions requires development effort
- D. Creating Service Catalog products requires development effort to define the allowed EC2 configurations.

Option B - Using Organizations service control policies - requires no custom development. It involves:

Organizing accounts into OUs

Creating an SCP that defines allowed/disallowed EC2 instance types

Attaching the SCP to the appropriate OUs

This is a native AWS service with a simple UI for defining and managing policies. No coding or resource creation is needed. So option B, using Organizations service control policies, will meet the requirements with the least development effort.

upvoted 3 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: B

AWS Organizations: AWS Organizations is a service that helps you centrally manage multiple AWS accounts. It enables you to group accounts into organizational units (OUs) and apply policies across those accounts.

Service Control Policies (SCPs): SCPs in AWS Organizations allow you to define fine-grained permissions and restrictions at the account or OU level. By attaching an SCP to the development accounts, you can control the creation and usage of EC2 instance types.

Least Development Effort: Option B requires minimal development effort as it leverages the built-in features of AWS Organizations and SCPs. You can define the SCP to restrict the use of oversized EC2 instance types and apply it to the appropriate OUs or accounts.

upvoted 3 times

 **Efren** 6 months, 2 weeks ago

B for me as well

upvoted 1 times

A company wants to use artificial intelligence (AI) to determine the quality of its customer service calls. The company currently manages calls in four different languages, including English. The company will offer new languages in the future. The company does not have the resources to regularly maintain machine learning (ML) models.

The company needs to create written sentiment analysis reports from the customer service call recordings. The customer service call recording text must be translated into English.

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

- A. Use Amazon Comprehend to translate the audio recordings into English.
- B. Use Amazon Lex to create the written sentiment analysis reports.
- C. Use Amazon Polly to convert the audio recordings into text.
- D. Use Amazon Transcribe to convert the audio recordings in any language into text.
- E. Use Amazon Translate to translate text in any language to English.
- F. Use Amazon Comprehend to create the sentiment analysis reports.

Correct Answer: DEF

Community vote distribution

DEF (100%)

 **wsdasdasdqwdaw** 1 month ago

It is: DEF

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: DEF

D. Use Amazon Transcribe to convert the audio recordings in any language into text.

E. Use Amazon Translate to translate text in any language to English.

F. Use Amazon Comprehend to create the sentiment analysis reports.

upvoted 1 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: DEF

Amazon Transcribe to convert speech to text. Amazon Translate to translate text to english. Amazon Comprehend to perform sentiment analysis on translated text.

upvoted 1 times

 **HareshPrajapati** 6 months ago

afree with DEF

upvoted 1 times

 **Blingy** 6 months ago

I'd go with DEF too

upvoted 2 times

 **elmogy** 6 months ago

Selected Answer: DEF

agree with DEF

upvoted 2 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: DEF

Amazon Transcribe will convert the audio recordings into text, Amazon Translate will translate the text into English, and Amazon Comprehend will perform sentiment analysis on the translated text to generate sentiment analysis reports.

upvoted 4 times

 **Efren** 6 months, 2 weeks ago

agreed as well, weird

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

@efren - It is not weird - This need to know the services for it
upvoted 1 times

A company uses Amazon EC2 instances to host its internal systems. As part of a deployment operation, an administrator tries to use the AWS CLI to terminate an EC2 instance. However, the administrator receives a 403 (Access Denied) error message.

The administrator is using an IAM role that has the following IAM policy attached:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["ec2:TerminateInstances"],  
            "Resource": ["*"]  
        },  
        {  
            "Effect": "Deny",  
            "Action": ["ec2:TerminateInstances"],  
            "Condition": {  
                "NotIpAddress": {  
                    "aws:SourceIp": [  
                        "192.0.2.0/24",  
                        "203.0.113.0/24"  
                    ]  
                }  
            },  
            "Resource": ["*"]  
        }  
    ]  
}
```

What is the cause of the unsuccessful request?

- A. The EC2 instance has a resource-based policy with a Deny statement.
- B. The principal has not been specified in the policy statement.
- C. The "Action" field does not grant the actions that are required to terminate the EC2 instance.
- D. The request to terminate the EC2 instance does not originate from the CIDR blocks 192.0.2.0/24 or 203.0.113.0/24.

Correct Answer: D

Community vote distribution

D (100%)

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

Selected Answer: D

the command is coming from a source IP which is not in the allowed range.

upvoted 3 times

✉  **elmogy** 6 months ago

Selected Answer: D

" aws:SourceIP " indicates the IP address that is trying to perform the action.

upvoted 1 times

✉  **nosense** 6 months, 1 week ago

Selected Answer: D

d for sure

upvoted 2 times

A company is conducting an internal audit. The company wants to ensure that the data in an Amazon S3 bucket that is associated with the company's AWS Lake Formation data lake does not contain sensitive customer or employee data. The company wants to discover personally identifiable information (PII) or financial information, including passport numbers and credit card numbers.

Which solution will meet these requirements?

- A. Configure AWS Audit Manager on the account. Select the Payment Card Industry Data Security Standards (PCI DSS) for auditing.
- B. Configure Amazon S3 Inventory on the S3 bucket. Configure Amazon Athena to query the inventory.
- C. Configure Amazon Macie to run a data discovery job that uses managed identifiers for the required data types.
- D. Use Amazon S3 Select to run a report across the S3 bucket.

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

Configure Amazon Macie to run a data discovery job that uses managed identifiers for the required data types.

upvoted 1 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: C

Amazon Macie is a data security service that uses machine learning (ML) and pattern matching to discover and help protect your sensitive data.

upvoted 1 times

 **Blingy** 6 months ago

Macie = Sensitive PII

upvoted 3 times

 **elmogy** 6 months ago

Selected Answer: C

agree with C

upvoted 3 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: C

Amazon Macie is a service that helps discover, classify, and protect sensitive data stored in AWS. It uses machine learning algorithms and managed identifiers to detect various types of sensitive information, including personally identifiable information (PII) and financial information. By configuring Amazon Macie to run a data discovery job with the appropriate managed identifiers for the required data types (such as passport numbers and credit card numbers), the company can identify and classify any sensitive data present in the S3 bucket.

upvoted 3 times

A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.

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

- A. Mount Amazon S3 as a file system to the on-premises servers.
- B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
- C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
- D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
- E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.

Correct Answer: BD

Community vote distribution

BD (100%)

 **thanhnv142** 1 month, 1 week ago

DE

B is not correct because NFS is a file system while storage gw is a storage. To replace a file system, need another file system which is EFS.
upvoted 2 times

 **Tekk97** 1 week ago

That's what I thought. but I think B is work too.

upvoted 1 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: BD

Deploy an AWS Storage Gateway file gateway to replace NFS storage

Deploy an AWS Storage Gateway volume gateway to replace the block storage

upvoted 1 times

 **elmogy** 6 months ago

Selected Answer: BD

local caching is a key feature of AWS Storage Gateway solution

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

<https://aws.amazon.com/blogs/storage/aws-storage-gateway-increases-cache-4x-and-enhances-bandwidth-throttling/#:~:text=AWS%20Storage%20Gateway%20increases%20cache%204x%20and%20enhances,for%20Volume%20Gateway%20customers%20...%20Conclusion%20>

upvoted 2 times

 **cloudenthusiast** 6 months, 2 weeks ago

Selected Answer: BD

By combining the deployment of an AWS Storage Gateway file gateway and an AWS Storage Gateway volume gateway, the company can address both its block storage and NFS storage needs, while leveraging local caching capabilities for improved performance.

upvoted 4 times

 **Piccalo** 6 months, 2 weeks ago

Selected Answer: BD

B and D is the correct answer

upvoted 1 times

A company has a service that reads and writes large amounts of data from an Amazon S3 bucket in the same AWS Region. The service is deployed on Amazon EC2 instances within the private subnet of a VPC. The service communicates with Amazon S3 over a NAT gateway in the public subnet. However, the company wants a solution that will reduce the data output costs.

Which solution will meet these requirements MOST cost-effectively?

- A. Provision a dedicated EC2 NAT instance in the public subnet. Configure the route table for the private subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
- B. Provision a dedicated EC2 NAT instance in the private subnet. Configure the route table for the public subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
- C. Provision a VPC gateway endpoint. Configure the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic.
- D. Provision a second NAT gateway. Configure the route table for the private subnet to use this NAT gateway as the destination for all S3 traffic.

Correct Answer: C

Community vote distribution

C (100%)

 **cloudenthusiast** Highly Voted 6 months, 2 weeks ago

Selected Answer: C

A VPC gateway endpoint allows you to privately access Amazon S3 from within your VPC without using a NAT gateway or NAT instance. By provisioning a VPC gateway endpoint for S3, the service in the private subnet can directly communicate with S3 without incurring data transfer costs for traffic going through a NAT gateway.

upvoted 5 times

 **Guru4Cloud** Most Recent 3 months, 1 week ago

Selected Answer: C

Using a VPC endpoint for S3 allows the EC2 instances to access S3 directly over the Amazon network without traversing the internet. This significantly reduces data output charges.

upvoted 1 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: C

use VPC gateway endpoint to route traffic internally and save on costs.

upvoted 1 times

 **elmogy** 6 months ago

Selected Answer: C

private subnet needs to communicate with S3 --> VPC endpoint right away

upvoted 2 times

A company uses Amazon S3 to store high-resolution pictures in an S3 bucket. To minimize application changes, the company stores the pictures as the latest version of an S3 object. The company needs to retain only the two most recent versions of the pictures.

The company wants to reduce costs. The company has identified the S3 bucket as a large expense.

Which solution will reduce the S3 costs with the LEAST operational overhead?

- A. Use S3 Lifecycle to delete expired object versions and retain the two most recent versions.
- B. Use an AWS Lambda function to check for older versions and delete all but the two most recent versions.
- C. Use S3 Batch Operations to delete noncurrent object versions and retain only the two most recent versions.
- D. Deactivate versioning on the S3 bucket and retain the two most recent versions.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

Use S3 Lifecycle to delete expired object versions and retain the two most recent versions.

upvoted 1 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: A

S3 Lifecycle to the rescue...whoooosh

upvoted 1 times

 **VellaDevil** 4 months, 3 weeks ago

Selected Answer: A

A --> "you can also provide a maximum number of noncurrent versions to retain."
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/intro-lifecycle-rules.html>

upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: A

A is correct.

upvoted 1 times

 **Konb** 6 months, 1 week ago

Selected Answer: A

Agree with LONGMEN

upvoted 3 times

 **cloudeuthusiast** 6 months, 2 weeks ago

Selected Answer: A

S3 Lifecycle policies allow you to define rules that automatically transition or expire objects based on their age or other criteria. By configuring an S3 Lifecycle policy to delete expired object versions and retain only the two most recent versions, you can effectively manage the storage costs while maintaining the desired retention policy. This solution is highly automated and requires minimal operational overhead as the lifecycle management is handled by S3 itself.

upvoted 4 times

A company needs to minimize the cost of its 1 Gbps AWS Direct Connect connection. The company's average connection utilization is less than 10%. A solutions architect must recommend a solution that will reduce the cost without compromising security.

Which solution will meet these requirements?

- A. Set up a new 1 Gbps Direct Connect connection. Share the connection with another AWS account.
- B. Set up a new 200 Mbps Direct Connect connection in the AWS Management Console.
- C. Contact an AWS Direct Connect Partner to order a 1 Gbps connection. Share the connection with another AWS account.
- D. Contact an AWS Direct Connect Partner to order a 200 Mbps hosted connection for an existing AWS account.

Correct Answer: B

Community vote distribution

D (71%) B (29%)

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

If you already have an existing AWS Direct Connect connection configured at 1 Gbps, and you wish to reduce the connection bandwidth to 200 Mbps to minimize costs, you should indeed contact your AWS Direct Connect Partner and request to lower the connection speed to 200 Mbps.
upvoted 3 times

✉  **Guru4Cloud** 3 months, 1 week ago

I meant D.. DDDDDDDDDDD

upvoted 4 times

✉  **Abrar2022** 5 months, 3 weeks ago

Selected Answer: D

Hosted Connection 50 Mbps, 100 Mbps, 200 Mbps,
Dedicated Connection 1 Gbps, 10 Gbps, and 100 Gbps
upvoted 4 times

✉  **omoakin** 6 months ago

BBBBBBBBBBBBBBB

upvoted 1 times

✉  **elmogy** 6 months ago

Selected Answer: D

company need to setup a cheaper connection (200 M) but B is incorrect because you can only order port speeds of 1, 10, or 100 Gbps for more flexibility you can go with hosted connection, You can order port speeds between 50 Mbps and 10 Gbps.

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect.html>

upvoted 3 times

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

Selected Answer: B

By opting for a lower capacity 200 Mbps connection instead of the 1 Gbps connection, the company can significantly reduce costs. This solution ensures a dedicated and secure connection while aligning with the company's low utilization, resulting in cost savings.
upvoted 3 times

✉  **norris81** 6 months, 2 weeks ago

Selected Answer: D

D

For Dedicated Connections, 1 Gbps, 10 Gbps, and 100 Gbps ports are available. For Hosted Connections, connection speeds of 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps and 10 Gbps may be ordered from approved AWS Direct Connect Partners. See AWS Direct Connect Partners for more information.

upvoted 4 times

✉  **nonsense** 6 months, 2 weeks ago

Selected Answer: D

A hosted connection is a lower-cost option that is offered by AWS Direct Connect Partners

upvoted 4 times

✉  **Efren** 6 months, 2 weeks ago

Also, there are not 200 MBps direct connection speed.

upvoted 1 times

 **nonsense** 6 months, 2 weeks ago

Hosted Connection 50 Mbps, 100 Mbps, 200 Mbps,
Dedicated Connection 1 Gbps, 10 Gbps, and 100 Gbps
B would require the company to purchase additional hardware or software

upvoted 2 times

A company has multiple Windows file servers on premises. The company wants to migrate and consolidate its files into an Amazon FSx for Windows File Server file system. File permissions must be preserved to ensure that access rights do not change.

Which solutions will meet these requirements? (Choose two.)

- A. Deploy AWS DataSync agents on premises. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.
- B. Copy the shares on each file server into Amazon S3 buckets by using the AWS CLI. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
- C. Remove the drives from each file server. Ship the drives to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
- D. Order an AWS Snowcone device. Connect the device to the on-premises network. Launch AWS DataSync agents on the device. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.
- E. Order an AWS Snowball Edge Storage Optimized device. Connect the device to the on-premises network. Copy data to the device by using the AWS CLI. Ship the device back to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.

Correct Answer: AD

Community vote distribution

AD (91%)	9%
----------	----

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

Selected Answer: AD

A This option involves deploying DataSync agents on your on-premises file servers and using DataSync to transfer the data directly to the FSx for Windows File Server. DataSync ensures that file permissions are preserved during the migration process.

D

This option involves using an AWS Snowcone device, a portable data transfer device. You would connect the Snowcone device to your on-premises network, launch DataSync agents on the device, and schedule DataSync tasks to transfer the data to FSx for Windows File Server. DataSync handles the migration process while preserving file permissions.

upvoted 5 times

✉️  **Guru4Cloud**  3 months, 1 week ago

Selected Answer: BD

Why not - BD?

upvoted 1 times

✉️  **Guru4Cloud** 3 months, 1 week ago

- ° This option uses S3 as an intermediary, ensuring that file permissions are preserved during the initial data copy. DataSync can then transfer the data from S3 to FSx while maintaining the permissions.
- ° This option uses a Snowcone device with DataSync agents to replicate the on-premises permission structure directly to FSx. This approach is suitable for maintaining file permissions during migration.

upvoted 1 times

✉️  **elmogy** 6 months ago

Selected Answer: AD

the key is file permissions are preserved during the migration process. only datasync supports that

upvoted 3 times

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

Bro,all 5 answers mentioned Datasync.....

upvoted 2 times

✉️  **Devsin2000** 2 months, 1 week ago

Yes but AD have only DataSync, whereas others have AWS CLI used.

upvoted 1 times

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

Selected Answer: AD

Option B would require copy the data to Amazon S3 before transferring it to Amazon FSx for Windows File Server
Option C would require the company to remove the drives from each file server and ship them to AWS

upvoted 2 times

 **barracouto** 3 months, 2 weeks ago

Also, S3 doesn't retain permissions because it isn't a file system.

upvoted 1 times

A company wants to ingest customer payment data into the company's data lake in Amazon S3. The company receives payment data every minute on average. The company wants to analyze the payment data in real time. Then the company wants to ingest the data into the data lake.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Use Amazon Kinesis Data Streams to ingest data. Use AWS Lambda to analyze the data in real time.
- B. Use AWS Glue to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.
- C. Use Amazon Kinesis Data Firehose to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.
- D. Use Amazon API Gateway to ingest data. Use AWS Lambda to analyze the data in real time.

Correct Answer: A

Community vote distribution

C (100%)

✉  **clouduenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: C

By leveraging the combination of Amazon Kinesis Data Firehose and Amazon Kinesis Data Analytics, you can efficiently ingest and analyze the payment data in real time without the need for manual processing or additional infrastructure management. This solution provides a streamlined and scalable approach to handle continuous data ingestion and analysis requirements.

upvoted 7 times

✉  **Axeashes** Highly Voted 5 months, 2 weeks ago

Kinesis Data Firehose is near real time (min. 60 sec). - The question is focusing on real time processing/analysis + efficiency -> Kinesis Data Stream is real time ingestion.

<https://www.amazonaws.cn/en/kinesis/data-firehose/#:~:text=Near%20real%2Dtime,is%20sent%20to%20the%20service>.

upvoted 7 times

✉  **Axeashes** 5 months, 2 weeks ago

Unless the intention is real time analytics not real time ingestion !

upvoted 2 times

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

Firehose has a 60 sec delay so real time analytics should be without real time data isn't that problematic? Why would you have then real time analytics then in the first place?

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

Kinesis Data Streams focuses on ingesting and storing data streams while Kinesis Data Firehose focuses on delivering data streams to select destinations, as the motive of the question is to do analytics, the answer should be C.

upvoted 2 times

✉  **hsinchang** 4 months ago

Selected Answer: C

Kinesis Data Streams focuses on ingesting and storing data streams while Kinesis Data Firehose focuses on delivering data streams to select destinations, as the motive of the question is to do analytics, the answer should be C.

upvoted 1 times

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

Selected Answer: C

Quote "Connect with 30+ fully integrated AWS services and streaming destinations such as Amazon Simple Storage Service (S3)" at <https://aws.amazon.com/kinesis/data-firehose/>. Amazon Kinesis Data Analytics <https://aws.amazon.com/kinesis/data-analytics/>

upvoted 1 times

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

Selected Answer: C

Use Kinesis Firehose to capture and deliver the data to Kinesis Analytics to perform analytics.

upvoted 1 times

✉  **Anmol_1010** 6 months, 1 week ago

Did anyone took tge exam recently,
How many questiona were there

upvoted 2 times

 **omoakin** 6 months, 1 week ago

Can we understand why admin's answers are mostly wrong? Or is this done on purpose?

upvoted 2 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: C

Amazon Kinesis Data Firehose the most optimal variant

upvoted 3 times

 **kailu** 6 months, 2 weeks ago

Shouldn't C be more appropriate?

upvoted 3 times

 **MostofMichelle** 5 months, 4 weeks ago

You're right. I believe the answers are wrong on purpose, so good thing votes can be made on answers and discussions are allowed.

upvoted 1 times

A company runs a website that uses a content management system (CMS) on Amazon EC2. The CMS runs on a single EC2 instance and uses an Amazon Aurora MySQL Multi-AZ DB instance for the data tier. Website images are stored on an Amazon Elastic Block Store (Amazon EBS) volume that is mounted inside the EC2 instance.

Which combination of actions should a solutions architect take to improve the performance and resilience of the website? (Choose two.)

- A. Move the website images into an Amazon S3 bucket that is mounted on every EC2 instance
- B. Share the website images by using an NFS share from the primary EC2 instance. Mount this share on the other EC2 instances.
- C. Move the website images onto an Amazon Elastic File System (Amazon EFS) file system that is mounted on every EC2 instance.
- D. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an accelerator in AWS Global Accelerator for the website
- E. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an Amazon CloudFront distribution for the website.

Correct Answer: DE

Community vote distribution

CE (62%)

AE (38%)

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

Selected Answer: CE

By combining the use of Amazon EFS for shared file storage and Amazon CloudFront for content delivery, you can achieve improved performance and resilience for the website.

upvoted 8 times

✉  **potomac**  3 weeks, 2 days ago

Selected Answer: CE

You can mount EFS file systems to multiple Amazon EC2 instances remotely and securely without having to log in to the instances by using the AWS Systems Manager Run Command.

upvoted 2 times

✉  **wsdasdasdqwdaw** 1 month ago

A is out of the game for sure. Mount S3 to EC2 ... madness. The question is CE or DE, but it is CE because of AWS Global Accelerator is match with NLB, not ALB as it is stated in option D, thus CE as many of all here noted.

upvoted 1 times

✉  **thanhnv142** 1 month ago

A and E is correct. We have a cloud front + S3 combo

upvoted 1 times

✉  **wsdasdasdqwdaw** 1 month ago

S3 can't be mounted on EC2 it is not A for sure!

upvoted 1 times

✉  **NickGordon** 2 weeks, 5 days ago

<https://aws.amazon.com/blogs/storage/mounting-amazon-s3-to-an-amazon-ec2-instance-using-a-private-connection-to-s3-file-gateway/>

upvoted 2 times

✉  **thanhnv142** 1 month, 1 week ago

A and E.

C is not correct because You don't mount a new EFS onto existing EC2. If you do that, you have to migrate all existing data in EBS into EFS. Then remove all the EBS. Should never do this.

upvoted 1 times

✉  **franbarberan** 2 months ago

Selected Answer: CE

<https://bluexp.netapp.com/blog/ebs-efs-amazons3-best-cloud-storage-system>

upvoted 2 times

✉  **Smart** 3 months ago

Selected Answer: CE

Not A - S3 cannot be mounted (up until few months ago). Exam does not test for the updates in last 6 months.
upvoted 3 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: AE

You have summarized the reasons why options A and E are the best choices very well.

Migrating static website assets like images to Amazon S3 enables high scalability, durability and shared access across instances. This improves performance.

Using Auto Scaling with load balancing provides elasticity and resilience. Adding a CloudFront distribution further boosts performance through caching and content delivery.

upvoted 2 times

 **Ale1973** 3 months, 3 weeks ago

Selected Answer: AE

Both options AE and CE would work, but I choose AE, because, on my opinion, S3 is best suited for performance and resilience.
upvoted 2 times

 **MickeyMouse** 3 months, 3 weeks ago

Selected Answer: CE

EFS, unlike EBS, can be mounted across multiple EC2 instances and hence C over A.
upvoted 1 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: AE

Technically both options AE and CE would work. But S3 is best suited for unstructured data, and the key benefit of mounting S3 on EC2 is that it provides a cost-effective alternative of using object storage for applications dealing with large files, as compared to expensive file or block storage. At the same time it provides more performant, scalable and highly available storage for these applications.

Even though there is no mention of 'cost efficient' in this question, in the real world cost is the no.1 factor.
In the exam I believe both options would be a pass.

<https://aws.amazon.com/blogs/storage/mounting-amazon-s3-to-an-amazon-ec2-instance-using-a-private-connection-to-s3-file-gateway/>
upvoted 4 times

 **AshutoshSingh1923** 4 months, 4 weeks ago

Selected Answer: CE

Option C provides moving the website images onto an Amazon EFS file system that is mounted on every EC2 instance. Amazon EFS provides a scalable and fully managed file storage solution that can be accessed concurrently from multiple EC2 instances. This ensures that the website images can be accessed efficiently and consistently by all instances, improving performance

In Option E The Auto Scaling group maintains a minimum of two instances, ensuring resilience by automatically replacing any unhealthy instances. Additionally, configuring an Amazon CloudFront distribution for the website further improves performance by caching content at edge locations closer to the end-users, reducing latency and improving content delivery.

Hence combining these actions, the website's performance is improved through efficient image storage and content delivery

upvoted 1 times

 **Vadbro7** 5 months ago

Which answe is correct?the most voted ones or the Suggested answers?

upvoted 1 times

 **mattcl** 5 months, 1 week ago

A and E: S3 is perfect for images. Besides is the perfect partner of cloudfront

upvoted 2 times

 **r3mo** 5 months, 2 weeks ago

C,E is the answer.

upvoted 1 times

 **Abrar2022** 5 months, 3 weeks ago

You don't mount S3

upvoted 3 times

 **omoakin** 6 months ago

answer is CD

upvoted 2 times

A company runs an infrastructure monitoring service. The company is building a new feature that will enable the service to monitor data in customer AWS accounts. The new feature will call AWS APIs in customer accounts to describe Amazon EC2 instances and read Amazon CloudWatch metrics.

What should the company do to obtain access to customer accounts in the MOST secure way?

- A. Ensure that the customers create an IAM role in their account with read-only EC2 and CloudWatch permissions and a trust policy to the company's account.
- B. Create a serverless API that implements a token vending machine to provide temporary AWS credentials for a role with read-only EC2 and CloudWatch permissions.
- C. Ensure that the customers create an IAM user in their account with read-only EC2 and CloudWatch permissions. Encrypt and store customer access and secret keys in a secrets management system.
- D. Ensure that the customers create an Amazon Cognito user in their account to use an IAM role with read-only EC2 and CloudWatch permissions. Encrypt and store the Amazon Cognito user and password in a secrets management system.

Correct Answer: A

Community vote distribution

A (100%)

 **cloudenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: A

By having customers create an IAM role with the necessary permissions in their own accounts, the company can use AWS Identity and Access Management (IAM) to establish cross-account access. The trust policy allows the company's AWS account to assume the customer's IAM role temporarily, granting access to the specified resources (EC2 instances and CloudWatch metrics) within the customer's account. This approach follows the principle of least privilege, as the company only requests the necessary permissions and does not require long-term access keys or user credentials from the customers.

upvoted 11 times

 **Piccalo** Highly Voted 6 months, 2 weeks ago

Selected Answer: A

A. Roles give temporary credentials

upvoted 6 times

 **Efren** 6 months, 2 weeks ago

Agreed . Role is the keyword

upvoted 1 times

 **Guru4Cloud** Most Recent 3 months, 1 week ago

Selected Answer: A

A is the most secure approach for accessing customer accounts.

Having customers create a cross-account IAM role with the appropriate permissions, and configuring the trust policy to allow the monitoring service principal account access, implements secure delegation and least privilege access.

upvoted 1 times

A company needs to connect several VPCs in the us-east-1 Region that span hundreds of AWS accounts. The company's networking team has its own AWS account to manage the cloud network.

What is the MOST operationally efficient solution to connect the VPCs?

- A. Set up VPC peering connections between each VPC. Update each associated subnet's route table
- B. Configure a NAT gateway and an internet gateway in each VPC to connect each VPC through the internet
- C. Create an AWS Transit Gateway in the networking team's AWS account. Configure static routes from each VPC.
- D. Deploy VPN gateways in each VPC. Create a transit VPC in the networking team's AWS account to connect to each VPC.

Correct Answer: C

Community vote distribution

C (100%)

✉  **clouduenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: C

AWS Transit Gateway is a highly scalable and centralized hub for connecting multiple VPCs, on-premises networks, and remote networks. It simplifies network connectivity by providing a single entry point and reducing the number of connections required. In this scenario, deploying an AWS Transit Gateway in the networking team's AWS account allows for efficient management and control over the network connectivity across multiple VPCs.

upvoted 6 times

✉  **hsinchang** Highly Voted 4 months ago

Selected Answer: C

The main difference between AWS Transit Gateway and VPC peering is that AWS Transit Gateway is designed to connect multiple VPCs together in a hub-and-spoke model, while VPC peering is designed to connect two VPCs together in a peer-to-peer model.

As we have several VPCs here, the answer should be C.

upvoted 6 times

✉  **TariqKipkemei** Most Recent 2 weeks, 6 days ago

Selected Answer: C

Connect, Monitor and Manage Multiple VPCs in one place = AWS Transit Gateway

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C is the most operationally efficient solution for connecting a large number of VPCs across accounts.

Using AWS Transit Gateway allows all the VPCs to connect to a central hub without needing to create a mesh of VPC peering connections between each VPC pair.

This significantly reduces the operational overhead of managing the network topology as new VPCs are added or changed.

The networking team can centrally manage the Transit Gateway routing and share it across accounts using Resource Access Manager.
upvoted 2 times

✉  **MirKhobaeb** 6 months ago

Answer is C

upvoted 1 times

✉  **MirKhobaeb** 6 months ago

A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks. As your cloud infrastructure expands globally, inter-Region peering connects transit gateways together using the AWS Global Infrastructure. Your data is automatically encrypted and never travels over the public internet.

upvoted 2 times

✉  **nonsense** 6 months, 1 week ago

Selected Answer: C

I voted for c

upvoted 2 times

✉  **nonsense** 6 months, 1 week ago

An AWS Transit Gateway is a highly scalable and secure way to connect VPCs in multiple AWS accounts. It is a central hub that routes traffic between VPCs, on-premises networks, and AWS services.

upvoted 3 times

A company has Amazon EC2 instances that run nightly batch jobs to process data. The EC2 instances run in an Auto Scaling group that uses On-Demand billing. If a job fails on one instance, another instance will reprocess the job. The batch jobs run between 12:00 AM and 06:00 AM local time every day.

Which solution will provide EC2 instances to meet these requirements MOST cost-effectively?

- A. Purchase a 1-year Savings Plan for Amazon EC2 that covers the instance family of the Auto Scaling group that the batch job uses.
- B. Purchase a 1-year Reserved Instance for the specific instance type and operating system of the instances in the Auto Scaling group that the batch job uses.
- C. Create a new launch template for the Auto Scaling group. Set the instances to Spot Instances. Set a policy to scale out based on CPU usage.
- D. Create a new launch template for the Auto Scaling group. Increase the instance size. Set a policy to scale out based on CPU usage.

Correct Answer: C

Community vote distribution

C (100%)

 **cludenthusiast**  6 months, 1 week ago

Selected Answer: C

Purchasing a 1-year Savings Plan (option A) or a 1-year Reserved Instance (option B) may provide cost savings, but they are more suitable for long-running, steady-state workloads. Since your batch jobs run for a specific period each day, using Spot Instances with the ability to scale out based on CPU usage is a more cost-effective choice.

upvoted 7 times

 **Guru4Cloud**  3 months, 1 week ago

Selected Answer: C

C is the most cost-effective solution in this scenario.

Using Spot Instances allows EC2 capacity to be purchased at significant discounts compared to On-Demand prices. The auto scaling group can scale out to add Spot Instances when needed for the batch jobs.

If Spot Instances become unavailable, regular On-Demand Instances will be launched instead to maintain capacity. The potential for interruptions is acceptable since failed jobs can be re-run.

upvoted 3 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: C

Spot Instances to the rescue....whooosh

upvoted 1 times

 **wRhlH** 5 months ago

" If a job fails on one instance, another instance will reprocess the job". This ensures Spot Instances are enough for this case

upvoted 1 times

 **Abrar2022** 5 months, 3 weeks ago

Selected Answer: C

Since your batch jobs run for a specific period each day, using Spot Instances with the ability to scale out based on CPU usage is a more cost-effective choice.

upvoted 1 times

 **Blingy** 6 months ago

C FOR ME COS OF SPOT INSTACES

upvoted 2 times

 **udo2020** 6 months, 1 week ago

First I think it is B but because of cost saving I think it should be C spot instances.

upvoted 1 times

 **nonsense** 6 months, 1 week ago

Selected Answer: C

c for me

upvoted 1 times

A social media company is building a feature for its website. The feature will give users the ability to upload photos. The company expects significant increases in demand during large events and must ensure that the website can handle the upload traffic from users.

Which solution meets these requirements with the MOST scalability?

- A. Upload files from the user's browser to the application servers. Transfer the files to an Amazon S3 bucket.
- B. Provision an AWS Storage Gateway file gateway. Upload files directly from the user's browser to the file gateway.
- C. Generate Amazon S3 presigned URLs in the application. Upload files directly from the user's browser into an S3 bucket.
- D. Provision an Amazon Elastic File System (Amazon EFS) file system. Upload files directly from the user's browser to the file system.

Correct Answer: C

Community vote distribution

C (95%) 5%

✉ **clouduenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: C

This approach allows users to upload files directly to S3 without passing through the application servers, reducing the load on the application and improving scalability. It leverages the client-side capabilities to handle the file uploads and offloads the processing to S3.

upvoted 12 times

✉ **Goutham4981** Most Recent 5 days, 5 hours ago

Selected Answer: A

S3 presigned url is used for sharing objects from an s3 bucket and not for uploading to an s3 bucket

upvoted 1 times

✉ **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C is the best solution to meet the scalability requirements.

Generating S3 presigned URLs allows users to upload directly to S3 instead of application servers. This removes the application servers as a bottleneck for upload traffic.

S3 can scale to handle very high volumes of uploads with no limits on storage or throughput. Using presigned URLs leverages this scalability.

upvoted 3 times

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

Selected Answer: C

You may use presigned URLs to allow someone to upload an object to your Amazon S3 bucket. Using a presigned URL will allow an upload without requiring another party to have AWS security credentials or permissions.

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

upvoted 1 times

✉ **baba365** 4 months, 3 weeks ago

Hello Moderator. This question and answer should be rephrased because:

1. S3 pre-signed URLs are used to share objects FROM S3 buckets
2. How scalable are pre-signed URLs when they are time constrained?

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

upvoted 2 times

✉ **nonsense** 6 months, 1 week ago

Selected Answer: C

the most scalable because it allows users to upload files directly to Amazon S3,

upvoted 3 times

A company has a web application for travel ticketing. The application is based on a database that runs in a single data center in North America. The company wants to expand the application to serve a global user base. The company needs to deploy the application to multiple AWS Regions. Average latency must be less than 1 second on updates to the reservation database.

The company wants to have separate deployments of its web platform across multiple Regions. However, the company must maintain a single primary reservation database that is globally consistent.

Which solution should a solutions architect recommend to meet these requirements?

- A. Convert the application to use Amazon DynamoDB. Use a global table for the central reservation table. Use the correct Regional endpoint in each Regional deployment.
- B. Migrate the database to an Amazon Aurora MySQL database. Deploy Aurora Read Replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.
- C. Migrate the database to an Amazon RDS for MySQL database. Deploy MySQL read replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.
- D. Migrate the application to an Amazon Aurora Serverless database. Deploy instances of the database to each Region. Use the correct Regional endpoint in each Regional deployment to access the database. Use AWS Lambda functions to process event streams in each Region to synchronize the databases.

Correct Answer: B

Community vote distribution

A (55%)

B (45%)

✉️  **cloudenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: A

Using DynamoDB's global tables feature, you can achieve a globally consistent reservation database with low latency on updates, making it suitable for serving a global user base. The automatic replication provided by DynamoDB eliminates the need for manual synchronization between Regions.
upvoted 9 times

✉️  **numark** Most Recent 2 days, 15 hours ago

"a web application for travel ticketing". This would be a transaction, so DynamoDB is not the answer.

upvoted 1 times

✉️  **Goutham4981** 5 days, 5 hours ago

Selected Answer: A

Dynamo DB global table acts as a single table. It does not consist of primary and standby databases. It is one single global table which is synchronously updated. Users can write to any of the regional endpoints and the write will be automatically updated across regions. To have a single primary database that is consistent does not align with dynamo db global tables.
Option B is even more dumb compared to A since read replicas does not provide failover capability or fast updates from the primary database.
The answer almost close to the requirement is Option A even though it is a misfit

upvoted 1 times

✉️  **Goutham4981** 1 week, 3 days ago

Selected Answer: A

The question mentions that the average latency on updates to the regional reservation databases should be less than 1sec. Read replicas provide asynchronous replication and hence the update times will be higher. Hence we can easily scrap all the options containing read replicas from the options. Moreover, a globally consistent database with millisecond latencies screams dynamo db global
upvoted 1 times

✉️  **DDongi** 1 month, 1 week ago

Selected Answer: B

I think the real difference is that DynamoDB is by default only eventually consistent however it has to be consistent. So it's B.
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadConsistency.html>

upvoted 4 times

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

Selected Answer: B

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Replication.CrossRegion.html> " average latency less than 1 second."

upvoted 2 times

 **kwang312** 2 months ago

This is for Cluster
upvoted 1 times

 **ibu007** 2 months, 3 weeks ago

Selected Answer: A

Amazon DynamoDB global tables is a fully managed, serverless, multi-Region, and multi-active database. Global tables provide you 99.999% availability, increased application resiliency, and improved business continuity. As global tables replicate your Amazon DynamoDB tables automatically across your choice of AWS Regions, you can achieve fast, local read and write performance.

upvoted 1 times

 **Bennyboy789** 3 months ago

Selected Answer: B

Amazon Aurora provides global databases that replicate your data with low latency to multiple regions. By using Aurora Read Replicas in each Region, the company can achieve low-latency access to the data while maintaining global consistency. The use of regional endpoints ensures that each deployment accesses the appropriate local replica, reducing latency. This solution allows the company to meet the requirement of serving a global user base while keeping average latency less than 1 second.

upvoted 1 times

 **Bennyboy789** 3 months ago

While Amazon DynamoDB is a highly scalable NoSQL database, using a global table might introduce latency and might not be suitable for maintaining a single primary reservation database with globally consistent data.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Aurora Global DB provides native multi-master replication and automatic failover for high availability across regions. Read replicas in each region ensure low read latency by promoting a local replica to handle reads.

A single Aurora primary region handles all writes to maintain data consistency.

Data replication and sync is managed automatically by Aurora Global DB.

Regional endpoints minimize cross-region latency.

Automatic failover promotes a replica to be the new primary if the current primary region goes down.

upvoted 1 times

 **cd93** 3 months, 1 week ago

Selected Answer: B

"the company must maintain a single primary reservation database that is globally consistent." --> Relational database, because it only allow writes from one regional endpoint

DynamoDB global table allow BOTH reads and writes on all regions ("last writer wins"), so it is not single point of entry. You can set up IAM identity based policy to restrict write access for global tables that are not in NA but it is not mentioned.

upvoted 1 times

 **ralfj** 3 months, 3 weeks ago

Selected Answer: B

Advantages of Amazon Aurora global databases

By using Aurora global databases, you can get the following advantages:

Global reads with local latency – If you have offices around the world, you can use an Aurora global database to keep your main sources of information updated in the primary AWS Region. Offices in your other Regions can access the information in their own Region, with local latency.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

D. although D is also using Aurora Global Database, there is no need for Lambda function to sync data.

upvoted 1 times

 **bjexamprep** 3 months, 4 weeks ago

Selected Answer: A

In real life, I would use Aurora Global Database. Because 1. it achieve less than 1 sec latency, 2. And ticketing system is a very typical traditional relational system.

While, in the exam I would vote for A. Because Option B isn't using global database which means you have to provide the endpoint of primary region to a remote region for update and even the typical back and forth latency is 400ms but you have to have a lot of professional network setup to guarantee it, which option B doesn't mention.

upvoted 3 times

 **BlueAlBird** 3 months, 4 weeks ago

ANs; B

Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS Regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each Region, and provides disaster recovery from Region-wide outages.

Ref: <https://aws.amazon.com/rds/aurora/global-database/>

upvoted 1 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: B

Latency experienced in both DynamoDB and Aurora MySQL can be influenced by factors such as your chosen AWS region, the network connectivity between your application and the database, and the performance optimizations you have implemented in your application code.

This is the type of requirement where both DBs will serve the purpose. In the real world it would be determined by whether the existing DB is SQL/NoSQL .

But for this case personally I prefer option B.

upvoted 2 times

✉ **EEK2k** 4 months, 2 weeks ago

Typical latency of Dynamo DB is 10 to 20 seconds and Aurora DB is less than 1 second. Thus correct Answer is B.

upvoted 2 times

✉ **manuelemg2007** 3 months, 1 week ago

DynamoDB is designed for single-digit millisecond latency

upvoted 2 times

✉ **Iragmt** 4 months, 3 weeks ago

Selected Answer: B

B

Key words here are

- Average latency must be less than 1 second on updates to the reservation database.

- single primary reservation database that is globally consistent

DynamoDB - multi-region,multi-master

Aurora Global database - multi-region,single-master

upvoted 2 times

✉ **baba365** 4 months, 3 weeks ago

option B. specifies Aurora MySQL database, not Aurora Global Database.

upvoted 3 times

✉ **mattcl** 5 months, 1 week ago

B "An Aurora Global Database uses storage-based replication to replicate a database across multiple Regions, with typical latency of less than one second"

upvoted 2 times

A company has migrated multiple Microsoft Windows Server workloads to Amazon EC2 instances that run in the us-west-1 Region. The company manually backs up the workloads to create an image as needed.

In the event of a natural disaster in the us-west-1 Region, the company wants to recover workloads quickly in the us-west-2 Region. The company wants no more than 24 hours of data loss on the EC2 instances. The company also wants to automate any backups of the EC2 instances.

Which solutions will meet these requirements with the LEAST administrative effort? (Choose two.)

- A. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Copy the image on demand.
- B. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Configure the copy to the us-west-2 Region.
- C. Create backup vaults in us-west-1 and in us-west-2 by using AWS Backup. Create a backup plan for the EC2 instances based on tag values. Create an AWS Lambda function to run as a scheduled job to copy the backup data to us-west-2.
- D. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Define the destination for the copy as us-west-2. Specify the backup schedule to run twice daily.
- E. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Specify the backup schedule to run twice daily. Copy on demand to us-west-2.

Correct Answer: BC

Community vote distribution

BD (100%)

 **pmlabs** 1 month, 3 weeks ago

B D seems to meet the requiremnts fully
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: BD
B and D are the options that meet the requirements with the least administrative effort.

B uses EC2 image lifecycle policies to automatically create AMIs of the instances twice daily and copy them to the us-west-2 region. This automates regional backups.

D leverages AWS Backup to define a backup plan that runs twice daily and copies backups to us-west-2. AWS Backup automates EC2 instance backups.

Together, these options provide automated, regional EC2 backup capabilities with minimal administrative overhead.
upvoted 1 times

 **TariqKipkemei** 4 months, 2 weeks ago

Selected Answer: BD
options B and D will provide least administrative effort.
upvoted 1 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: BD
I also vote B and D.
upvoted 1 times

 **cloudenthusiast** 6 months, 1 week ago

Selected Answer: BD
Option B suggests using an EC2-backed Amazon Machine Image (AMI) lifecycle policy to automate the backup process. By configuring the policy to run twice daily and specifying the copy to the us-west-2 Region, the company can ensure regular backups are created and copied to the alternate region.

Option D proposes using AWS Backup, which provides a centralized backup management solution. By creating a backup vault and backup plan based on tag values, the company can automate the backup process for the EC2 instances. The backup schedule can be set to run twice daily, and the destination for the copy can be defined as the us-west-2 Region.

upvoted 4 times

 **cloudenthusiast** 6 months, 1 week ago

Both options automate the backup process and include copying the backups to the us-west-2 Region, ensuring data resilience in the event of a disaster. These solutions minimize administrative effort by leveraging automated backup and copy mechanisms provided by AWS services.

upvoted 3 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: BD

solutions are both automated and require no manual intervention to create or copy backups

upvoted 4 times

A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet. An Application Load Balancer (ALB) for the web tier uses the public subnets. Amazon EC2 instances for the application tier use the private subnets.

Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution.

What should the solutions architect recommend to meet this requirement?

- A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.
- B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.
- C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.
- D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

Correct Answer: B

Community vote distribution

B (82%) A (18%)

 **lucdt4** Highly Voted 6 months ago

Selected Answer: B

A wrong because security group can't deny (only allow)
upvoted 9 times

 **cloudenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: B

In this scenario, the security audit reveals that the application is receiving millions of illegitimate requests from a small number of IP addresses. To address this issue, it is recommended to modify the network ACL (Access Control List) for the web tier subnets.

By adding an inbound deny rule specifically targeting the IP addresses that are consuming resources, the network ACL can block the illegitimate traffic at the subnet level before it reaches the web servers. This will help alleviate the excessive load on the web tier and improve the application's performance.

upvoted 5 times

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

Selected Answer: B

Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.
upvoted 1 times

 **potomac** 3 weeks, 2 days ago

Selected Answer: B

A is wrong
Security groups act at the network interface level, not the subnet level, and they support Allow rules only.
upvoted 1 times

 **Devsin2000** 2 months ago

Selected Answer: A

The security Group can be applied to an ALB at web tier.
upvoted 1 times

 **Goutham4981** 1 week, 3 days ago

Security group can't deny.
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Since the bad requests are targeting the web tier, adding ACL deny rules for those IP addresses on the web subnets will block the traffic before it reaches the instances.

Security group changes (Options A and C) would not be effective since the requests are not even reaching those resources.

Modifying the application tier ACL (Option D) would not stop the bad traffic from hitting the web tier.

upvoted 1 times

✉  **fakrap** 6 months, 1 week ago

Selected Answer: B

A is wrong because you cannot put any deny in security group

upvoted 2 times

✉  **Rob1L** 6 months, 1 week ago

Selected Answer: B

You cannot Deny on SG, so it's B

upvoted 4 times

✉  **nonsense** 6 months, 2 weeks ago

Selected Answer: A

Option B is not as effective as option A

upvoted 4 times

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

A and C out due to the fact that SG does not have deny on allow rules.

upvoted 2 times

✉  **y0** 6 months, 2 weeks ago

Security group only have allow rules

upvoted 1 times

✉  **nonsense** 6 months, 1 week ago

yeah, my mistake. B should be

upvoted 1 times

A global marketing company has applications that run in the ap-southeast-2 Region and the eu-west-1 Region. Applications that run in a VPC in eu-west-1 need to communicate securely with databases that run in a VPC in ap-southeast-2.

Which network design will meet these requirements?

- A. Create a VPC peering connection between the eu-west-1 VPC and the ap-southeast-2 VPC. Create an inbound rule in the eu-west-1 application security group that allows traffic from the database server IP addresses in the ap-southeast-2 security group.
- B. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPC. Update the subnet route tables. Create an inbound rule in the ap-southeast-2 database security group that references the security group ID of the application servers in eu-west-1.
- C. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPC. Update the subnet route tables. Create an inbound rule in the ap-southeast-2 database security group that allows traffic from the eu-west-1 application server IP addresses.
- D. Create a transit gateway with a peering attachment between the eu-west-1 VPC and the ap-southeast-2 VPC. After the transit gateways are properly peered and routing is configured, create an inbound rule in the database security group that references the security group ID of the application servers in eu-west-1.

Correct Answer: B

Community vote distribution

C (81%)

B (19%)

 **VellaDevil** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

Answer: C --> "You cannot reference the security group of a peer VPC that's in a different Region. Instead, use the CIDR block of the peer VPC." <https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html>

upvoted 16 times

 **hsinchang** 4 months ago

Thanks for this clarification!

upvoted 1 times

 **Axeashes** Highly Voted 5 months, 2 weeks ago

Selected Answer: C

"You cannot reference the security group of a peer VPC that's in a different Region. Instead, use the CIDR block of the peer VPC." <https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html>

upvoted 6 times

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

Selected Answer: C

After establishing the VPC peering connection, the subnet route tables need to be updated in both VPCs to route traffic to the other VPC's CIDR blocks through the peering connection.

upvoted 2 times

 **Bennyboy789** 3 months ago

Selected Answer: C

VPC Peering Connection: This allows communication between instances in different VPCs as if they are on the same network. It's a straightforward approach to connect the two VPCs.

Subnet Route Tables: After establishing the VPC peering connection, the subnet route tables need to be updated in both VPCs to route traffic to the other VPC's CIDR blocks through the peering connection.

Inbound Rule in Database Security Group: By creating an inbound rule in the ap-southeast-2 database security group that allows traffic from the eu-west-1 application server IP addresses, you ensure that only the specified application servers from the eu-west-1 VPC can access the database servers in the ap-southeast-2 VPC.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

B) Configure VPC peering between ap-southeast-2 and eu-west-1 VPCs. Update routes. Allow traffic in ap-southeast-2 database SG from eu-west-1 application server SG.

This option establishes the correct network connectivity for the applications in eu-west-1 to reach the databases in ap-southeast-2:

VPC peering connects the two VPCs across regions - <https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html#:~:text=You%20can%20create%20a%20VPC,%2DRegion%20VPC%20peering%20connection>.

Updating route tables enables routing between the VPCs
Security group rule allowing traffic from eu-west-1 application server SG to ap-southeast-2 database SG secures connectivity
upvoted 1 times

✉ **Guru4Cloud** 3 months, 1 week ago

Options A, C, D have flaws:
Option A peer direction is wrong
Option C opens databases to application server IP addresses rather than SG
Option D uses transit gateway which is unnecessary for just two VPCs
upvoted 1 times

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

Selected Answer: C
Selected C but B can also work
upvoted 1 times

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

I just tried from the the console, You can specify the name or ID of another security group in the same region. To specify a security group in another AWS account (EC2-Classic only), prefix it with the account ID and a forward slash, for example: 111122223333/OtherSecurityGroup. You can Specify a single IP address, or an IP address range in CIDR notation in the same/other region.

In the exam both option B and C would be a pass. In the real world both option will work.

upvoted 2 times

✉ **TariqKipkemei** 2 weeks, 6 days ago

Correction, You cannot reference the security group of a peer VPC that's in a different Region. Instead, use the CIDR block of the peer VPC. The C is the only option here.

<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html#:~:text>You%20cannot-,reference,-the%20security%20group>

upvoted 1 times

✉ **Chris22usa** 5 months ago

I realize D is right as ChatGpt indicates.Because here is not a problem just one application in a VPC connection to another in different region. Actually there many applications in different VPCs in a region which need to connect any other application crossingly in other region. So two transit gateway need to installed in two regions for multiple to multiple VPCs connections.

upvoted 1 times

✉ **Iragmt** 4 months, 3 weeks ago

However, there was also a part of "create an inbound rule in the database security group that references the security group ID of the application servers in eu-west-1"

therefore, still C because we cannot reference SG ID of diff VPC, we should use the CIDR block

upvoted 1 times

✉ **Chris22usa** 5 months ago

post it on ChaptGpt and it give me answer D. what heck with this?

upvoted 1 times

✉ **haoAWS** 5 months ago

Selected Answer: C

B is wrong because It is in a different region, so reference to the security group ID will not work. A is wrong because you need to update the route table. The answer should be C.

upvoted 1 times

✉ **mattcl** 5 months, 1 week ago

is B. what happens if application server IP addresses changes (Option C). You must change manually the IP in the security group again.
upvoted 1 times

✉ **antropaws** 5 months, 1 week ago

Selected Answer: C

I thought B, but I vote C after checking Axeashes response.

upvoted 1 times

✉ **HelioNeto** 6 months ago

Selected Answer: C

I think the answer is C because the security groups are in different VPCs. When the question wants to allow traffic from app vpc to database vpc i think using peering connection you will be able to add the security groups rules using private ip addresses of app servers. I don't think the database VPC will identify the security group id of another VPC.

upvoted 1 times

✉ **REzirezi** 6 months, 1 week ago

D You cannot create a VPC peering connection between VPCs in different regions.

upvoted 3 times

 **fakrap** 6 months, 1 week ago

You can peer any two VPCs in different Regions, as long as they have distinct, non-overlapping CIDR blocks. This ensures that all of the private IP addresses are unique, and it allows all of the resources in the VPCs to address each other without the need for any form of network address translation (NAT).

upvoted 1 times

 **RainWhisper** 6 months, 1 week ago

You can peer any two VPCs in different Regions, as long as they have distinct, non-overlapping CIDR blocks
<https://docs.aws.amazon.com/devicefarm/latest/developerguide/amazon-vpc-cross-region.html>

upvoted 2 times

 **nonsense** 6 months, 1 week ago

Selected Answer: B

b for me. bcs correct inbound rule, and not overhead

upvoted 2 times

 **cloudenthusiast** 6 months, 1 week ago

Selected Answer: B

Option B suggests configuring a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPC. By establishing this peering connection, the VPCs can communicate with each other over their private IP addresses.

Additionally, updating the subnet route tables is necessary to ensure that the traffic destined for the remote VPC is correctly routed through the VPC peering connection.

To secure the communication, an inbound rule is created in the ap-southeast-2 database security group. This rule references the security group ID of the application servers in the eu-west-1 VPC, allowing traffic only from those instances. This approach ensures that only the authorized application servers can access the databases in the ap-southeast-2 VPC.

upvoted 4 times

A company is developing software that uses a PostgreSQL database schema. The company needs to configure multiple development environments and databases for the company's developers. On average, each development environment is used for half of the 8-hour workday.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure each development environment with its own Amazon Aurora PostgreSQL database
- B. Configure each development environment with its own Amazon RDS for PostgreSQL Single-AZ DB instances
- C. Configure each development environment with its own Amazon Aurora On-Demand PostgreSQL-Compatible database
- D. Configure each development environment with its own Amazon S3 bucket by using Amazon S3 Object Select

Correct Answer: B

Community vote distribution

C (60%)

B (40%)

✉  **clouenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: C

Option C suggests using Amazon Aurora On-Demand PostgreSQL-Compatible databases for each development environment. This option provides the benefits of Amazon Aurora, which is a high-performance and scalable database engine, while allowing you to pay for usage on an on-demand basis. Amazon Aurora On-Demand instances are typically more cost-effective for individual development environments compared to the provisioned capacity options.

upvoted 7 times

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

Option B suggests using Amazon RDS for PostgreSQL Single-AZ DB instances for each development environment. While Amazon RDS is a reliable and cost-effective option, it may have slightly higher costs compared to Amazon Aurora On-Demand instances.

upvoted 6 times

✉  **Iragmt** 4 months, 3 weeks ago

I'm thinking that it should be B, since question does not mention any requirement only cost effective and this is just an development environment I guess we can leverage the use of RDS free tier also

upvoted 1 times

✉  **Wayne23Fang** Most Recent 1 month, 1 week ago

Selected Answer: B

Aurora instances will cost you ~20% more than RDS MySQL Given the running hours the same.
Also Aurora is HA.

upvoted 1 times

✉  **baba365** 2 months ago

... just trying to trick you. Aurora on demand is Aurora Serverless.

upvoted 2 times

✉  **Anmol_1010** 1 month, 1 week ago

that is good piece of infroamtion
upvoted 1 times

✉  **deechean** 2 months, 4 weeks ago

Selected Answer: C

Aurora allows you to pay for the hours used. 4 hour every day, you only need 1/6 cost of 24 hours per day. You can check the Aurora pricing calculator.

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

The key factors:

RDS Single-AZ instances only run the DB instance when in use, minimizing costs for dev environments not used full-time
RDS charges by the hour for DB instance hours used, versus Aurora clusters that have hourly uptime charges
PostgreSQL is natively supported by RDS so no compatibility issues
S3 Object Select (Option D) does not provide full database functionality
Aurora (Options A and C) has higher minimum costs than RDS even when not fully utilized

upvoted 2 times

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

Selected Answer: C

Putting into consideration that the environments will only run 4 hours everyday and the need to save on costs, then Amazon Aurora would be suitable because it supports auto-scaling configuration where the database automatically starts up, shuts down, and scales capacity up or down based on your application's needs. So for the rest of the 4 hours everyday when not in use the database shuts down automatically when there is no activity.

Option C would be best, as this is the name of the service from the aws console.

upvoted 2 times

 **dddwwwwwwww12** 4 months, 2 weeks ago

is A not the serverless ?

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: C

C, more specific "Aurora Serverless V2", check the link: <https://aws.amazon.com/rds/aurora/serverless/>

upvoted 1 times

 **nuri92** 5 months, 2 weeks ago

Selected Answer: B

Answer is B.

upvoted 2 times

 **Bill1000** 5 months, 3 weeks ago

Selected Answer: C

With Aurora Serverless, you create a database, specify the desired database capacity range, and connect your applications. You pay on a per-second basis for the database capacity that you use when the database is active, and migrate between standard and serverless configurations with a few steps in the Amazon Relational Database Service (Amazon RDS) console.

upvoted 1 times

 **Felix_br** 5 months, 3 weeks ago

Selected Answer: C

Amazon Aurora On-Demand is a pay-per-use deployment option for Amazon Aurora that allows you to create and destroy database instances as needed. This is ideal for development environments that are only used for part of the day, as you only pay for the database instance when it is in use.

The other options are not as cost-effective. Option A, configuring each development environment with its own Amazon Aurora PostgreSQL database, would require you to pay for the database instance even when it is not in use. Option B, configuring each development environment with its own Amazon RDS for PostgreSQL Single-AZ DB instance, would also require you to pay for the database instance even when it is not in use. Option D, configuring each development environment with its own Amazon S3 bucket by using Amazon S3 Object Select, is not a viable option as Amazon S3 is not a database.

upvoted 1 times

 **elmogy** 6 months ago

Selected Answer: B

Option B would be the most cost-effective solution for configuring development environments. Amazon RDS for PostgreSQL Single-AZ DB instances would provide a cost-effective solution for a development environment. Amazon Aurora has higher cost than RDS (20% more)

upvoted 2 times

 **Rob1L** 6 months, 1 week ago

Selected Answer: B

Amazon Aurora, whether On-Demand or not (Option A and C), provides higher performance and is more intended for production environments. It also typically has a higher cost compared to RDS,

upvoted 3 times

 **Anmol_1010** 6 months, 1 week ago

Its B the most cost effective if it was preformance then it would be option A

upvoted 1 times

 **nosense** 6 months, 2 weeks ago

Selected Answer: C

c cost effectively

upvoted 2 times

A company uses AWS Organizations with resources tagged by account. The company also uses AWS Backup to back up its AWS infrastructure resources. The company needs to back up all AWS resources.

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

- A. Use AWS Config to identify all untagged resources. Tag the identified resources programmatically. Use tags in the backup plan.
- B. Use AWS Config to identify all resources that are not running. Add those resources to the backup vault.
- C. Require all AWS account owners to review their resources to identify the resources that need to be backed up.
- D. Use Amazon Inspector to identify all noncompliant resources.

Correct Answer: A

Community vote distribution

A (100%)

 **TariqKipkemei** 2 weeks, 5 days ago

Selected Answer: A

Use AWS config to deploy the tag rule and remediate resources that are not compliant.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

This option has the least operational overhead:

AWS Config continuously evaluates resource configurations and can identify untagged resources

Resources can be programmatically tagged via the AWS SDK based on Config data

Backup plans can use tag criteria to automatically back up newly tagged resources

No manual review or resource discovery needed

upvoted 1 times

 **Bill1000** 5 months, 3 weeks ago

Selected Answer: A

Vote A

upvoted 1 times

 **nonsense** 6 months, 1 week ago

Selected Answer: A

a valid for me

upvoted 3 times

 **clouduenthusiast** 6 months, 1 week ago

Selected Answer: A

This solution allows you to leverage AWS Config to identify any untagged resources within your AWS Organizations accounts. Once identified, you can programmatically apply the necessary tags to indicate the backup requirements for each resource. By using tags in the backup plan configuration, you can ensure that only the tagged resources are included in the backup process, reducing operational overhead and ensuring all necessary resources are backed up.

upvoted 3 times

A social media company wants to allow its users to upload images in an application that is hosted in the AWS Cloud. The company needs a solution that automatically resizes the images so that the images can be displayed on multiple device types. The application experiences unpredictable traffic patterns throughout the day. The company is seeking a highly available solution that maximizes scalability.

What should a solutions architect do to meet these requirements?

- A. Create a static website hosted in Amazon S3 that invokes AWS Lambda functions to resize the images and store the images in an Amazon S3 bucket.
- B. Create a static website hosted in Amazon CloudFront that invokes AWS Step Functions to resize the images and store the images in an Amazon RDS database.
- C. Create a dynamic website hosted on a web server that runs on an Amazon EC2 instance. Configure a process that runs on the EC2 instance to resize the images and store the images in an Amazon S3 bucket.
- D. Create a dynamic website hosted on an automatically scaling Amazon Elastic Container Service (Amazon ECS) cluster that creates a resize job in Amazon Simple Queue Service (Amazon SQS). Set up an image-resizing program that runs on an Amazon EC2 instance to process the resize jobs.

Correct Answer: A

Community vote distribution

A (100%)

 **clouduenthusiast**  6 months, 1 week ago

Selected Answer: A

By using Amazon S3 and AWS Lambda together, you can create a serverless architecture that provides highly scalable and available image resizing capabilities. Here's how the solution would work:

Set up an Amazon S3 bucket to store the original images uploaded by users.

Configure an event trigger on the S3 bucket to invoke an AWS Lambda function whenever a new image is uploaded.

The Lambda function can be designed to retrieve the uploaded image, perform the necessary resizing operations based on device requirements, and store the resized images back in the S3 bucket or a different bucket designated for resized images.

Configure the Amazon S3 bucket to make the resized images publicly accessible for serving to users.

upvoted 13 times

 **Guru4Cloud**  3 months, 1 week ago

Selected Answer: A

This meets all the key requirements:

S3 static website provides high availability and auto scaling to handle unpredictable traffic

Lambda functions invoked from the S3 site can resize images on the fly

Storing images in S3 buckets provides durability, scalability and high throughput

Serverless approach with S3 and Lambda maximizes scalability and availability

upvoted 1 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: A

Scalability = S3, Lamda

automatically resize images = Lambda

upvoted 2 times

A company is running a microservices application on Amazon EC2 instances. The company wants to migrate the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for scalability. The company must configure the Amazon EKS control plane with endpoint private access set to true and endpoint public access set to false to maintain security compliance. The company must also put the data plane in private subnets. However, the company has received error notifications because the node cannot join the cluster.

Which solution will allow the node to join the cluster?

- A. Grant the required permission in AWS Identity and Access Management (IAM) to the AmazonEKSNodeRole IAM role.
- B. Create interface VPC endpoints to allow nodes to access the control plane.
- C. Recreate nodes in the public subnet. Restrict security groups for EC2 nodes.
- D. Allow outbound traffic in the security group of the nodes.

Correct Answer: B

Community vote distribution

B (55%)

A (45%)

 **cludenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: B

By creating interface VPC endpoints, you can enable the necessary communication between the Amazon EKS control plane and the nodes in private subnets. This solution ensures that the control plane maintains endpoint private access (set to true) and endpoint public access (set to false) for security compliance.

upvoted 10 times

 **y0** Highly Voted 6 months, 1 week ago

Selected Answer: A

Check this : <https://docs.aws.amazon.com/eks/latest/userguide/create-node-role.html>

Also, EKS does not require VPC endpoints. This is not the right use case for EKS

upvoted 7 times

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

Selected Answer: A

Before can launch nodes and register nodes into a EKS cluster, must create an IAM role for those nodes to use when they are launched.

upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

A is correct:

To deploy a new EKS cluster:

1. Need to have a VPC and at least 2 subnets
2. An IAM role that have permission to create and describe EKS cluster

upvoted 2 times

 **thanhnv142** 1 month, 1 week ago

A is good to go. B is not correct because they already setup connection to control plane.

upvoted 2 times

 **Bennyboy789** 3 months ago

Selected Answer: B

In Amazon EKS, nodes need to communicate with the EKS control plane. When the Amazon EKS control plane endpoint access is set to private, you need to create interface VPC endpoints in the VPC where your nodes are running. This allows the nodes to access the control plane privately without needing public internet access.

upvoted 2 times

 **Smart** 3 months ago

Selected Answer: A

This should be an associate-level question.

<https://repost.aws/knowledge-center/eks-worker-nodes-cluster>
<https://docs.aws.amazon.com/eks/latest/userguide/create-node-role.html>

upvoted 1 times

 **Smart** 3 months ago

This should NOT be an associate-level question

upvoted 2 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Since the EKS control plane has public access disabled and is in private subnets, the EKS nodes in the private subnets need interface VPC endpoints to reach the control plane API.

Creating these interface endpoints allows the EKS nodes to communicate with the control plane privately within the VPC to join the cluster.
upvoted 2 times

✉  **Guru4Cloud** 3 months, 1 week ago

Why B

Private Control Plane: You've configured the Amazon EKS control plane with private endpoint access, which means the control plane is not accessible over the public internet.

VPC Endpoints: When the control plane is set to private access, you need to set up VPC endpoints for the Amazon EKS service so that the nodes in your private subnets can communicate with the EKS control plane without going through the public internet. These are known as interface VPC endpoints.

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Reason why, not A

While security groups and IAM permissions are important considerations for networking and authentication, they alone won't resolve the issue of nodes not being able to join the cluster when the control plane is configured for private access.

upvoted 1 times

✉  **0628atv** 4 months, 2 weeks ago

Selected Answer: A

because the node cannot join the cluster.

upvoted 3 times

✉  **Iragmt** 4 months, 3 weeks ago

Selected Answer: A

A. When it comes to troubleshooting, First thing to do is to check the if the proper permissions are given to the roles. Since the question doesn't mention any procedure how they configure/created the eks cluster and nodes, you need to check on the policies and it is also a requirement on creating EKS

You can check this site <https://docs.aws.amazon.com/eks/latest/userguide/troubleshooting.html>
<https://docs.aws.amazon.com/eks/latest/userguide/create-node-role.html>

upvoted 2 times

✉  **jaydesai8** 4 months, 3 weeks ago

Selected Answer: B

As mention in the link below

Kubernetes API requests within your cluster's VPC (such as node to control plane communication) use the private VPC endpoint.
<https://docs.aws.amazon.com/eks/latest/userguide/cluster-endpoint.html>

Answer is B

upvoted 1 times

✉  **narddrer** 4 months, 3 weeks ago

Selected Answer: B

Question is more about Private and public endpoint for nodes, more about routing and registering than accessing.
as per the link <https://docs.aws.amazon.com/eks/latest/userguide/cluster-endpoint.html>

upvoted 1 times

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

Selected Answer: B

Going with B here:

--> <https://docs.aws.amazon.com/eks/latest/userguide/vpc-interface-endpoints.html>

upvoted 1 times

✉  **vrevkov** 5 months, 1 week ago

Selected Answer: A

This is A because the control plane and data plane nodes are in the same VPC and data plane nodes don't need any interface VPC endpoints, but they definitely need to have IAM role with correct permissions.

<https://docs.aws.amazon.com/eks/latest/userguide/create-node-role.html>

upvoted 2 times

✉  **CVliner** 5 months, 1 week ago

Please be noted, that A fits only for security for nodes (not cluster) For cluster we have to write IAM role name eksClusterRole.
https://docs.aws.amazon.com/eks/latest/userguide/service_IAM_role.html

upvoted 3 times

 **antropaws** 5 months, 3 weeks ago

Selected Answer: A

The question is:

Which solution will allow the node to join the cluster?

The answer is A:

Amazon EKS node IAM role

Nodes receive permissions for these API calls through an IAM instance profile and associated policies. Before you can launch nodes and register them into a cluster, you must create an IAM role for those nodes to use when they are launched. This requirement applies to nodes launched with the Amazon EKS optimized AMI provided by Amazon, or with any other node AMIs that you intend to use.

<https://docs.aws.amazon.com/eks/latest/userguide/create-node-role.html>

upvoted 4 times

 **elmogy** 6 months ago

Selected Answer: B

Kubernetes API requests within your cluster's VPC (such as node to control plane communication) use the private VPC endpoint.

<https://docs.aws.amazon.com/eks/latest/userguide/cluster-endpoint.html>

upvoted 4 times

 **nonsense** 6 months, 2 weeks ago

Selected Answer: B

b for me

upvoted 3 times

A company is migrating an on-premises application to AWS. The company wants to use Amazon Redshift as a solution.

Which use cases are suitable for Amazon Redshift in this scenario? (Choose three.)

- A. Supporting data APIs to access data with traditional, containerized, and event-driven applications
- B. Supporting client-side and server-side encryption
- C. Building analytics workloads during specified hours and when the application is not active
- D. Caching data to reduce the pressure on the backend database
- E. Scaling globally to support petabytes of data and tens of millions of requests per minute
- F. Creating a secondary replica of the cluster by using the AWS Management Console

Correct Answer: BCE

Community vote distribution

BCE (54%)	ACE (19%)	12%	Other
-----------	-----------	-----	-------

 **elmogy** Highly Voted 6 months ago

Selected Answer: BCE

Amazon Redshift is a data warehouse solution, so it is suitable for:

- Supporting encryption (client-side and server-side)
- Handling analytics workloads, especially during off-peak hours when the application is less active
- Scaling to large amounts of data and high query volumes for analytics purposes

The following options are incorrect because:

- A) Data APIs are not typically used with Redshift. It is more for running SQL queries and analytics.
- D) Redshift is not typically used for caching data. It is for analytics and data warehouse purposes.
- F) Redshift clusters do not create replicas in the management console. They are standalone clusters. you could create DR cluster from snapshot and restore to another region (automated or manual) but I do not think this what is meant in this option.

upvoted 8 times

 **TariqKipkemei** Most Recent 2 weeks, 5 days ago

Selected Answer: ACE

Technically both options A and B apply, this is from the links below:

A. You can access your Amazon Redshift database using the built-in Amazon Redshift Data API.

<https://docs.aws.amazon.com/redshift/latest/mgmt/data-api.html#:~:text=in%20Amazon%20Redshift-,Data%20API,-.%20Using%20this%20API>

B. You can encrypt data client-side and upload the encrypted data to Amazon Redshift. In this case, you manage the encryption process, the encryption keys, and related tools.

<https://docs.aws.amazon.com/redshift/latest/mgmt/security-encryption.html#:~:text=Use-,client%2Dside,-encryption%20E2%80%93%20You%20can>

upvoted 1 times

 **potomac** 3 weeks, 2 days ago

Selected Answer: ABC

Amazon Redshift provides a Data API that you can use to painlessly access data from Amazon Redshift with all types of traditional, cloud-native, and containerized, serverless web services-based and event-driven applications.

Amazon Redshift supports up to 500 concurrent queries per cluster, which may be expanded by adding more nodes to the cluster.

upvoted 2 times

 **potomac** 3 weeks, 2 days ago

change to ABD

To reduce query runtime and improve system performance, Amazon Redshift caches the results of certain types of queries in memory on the leader node. When a user submits a query, Amazon Redshift checks the results cache for a valid, cached copy of the query results. If a match is found in the result cache, Amazon Redshift uses the cached results and doesn't run the query. Result caching is transparent to the user.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: BCE

The key use cases for Amazon Redshift that fit this scenario are:

- B) Redshift supports both client-side and server-side encryption to protect sensitive data.

C) Redshift is well suited for running batch analytics workloads during off-peak times without affecting OLTP systems.

E) Redshift can scale to massive datasets and concurrent users to support large analytics workloads.

upvoted 1 times

✉ **cd93** 3 months, 1 week ago

Selected Answer: BCD

Why E lol? It's a data warehouse! it has no need to support millions of requests, it is not mentioned anywhere (<https://aws.amazon.com/redshift/features>)

In fact Redshift editor supports max 500 connections and workgroup support max 2000 connections at once, see it's quota page
Redshift has a cache layer, D is correct

upvoted 3 times

✉ **mrsoa** 4 months ago

Selected Answer: BCE

BCE, For B this is why

<https://docs.aws.amazon.com/redshift/latest/mgmt/security-encryption.html>

upvoted 1 times

✉ **james2033** 4 months, 2 weeks ago

Selected Answer: ACE

Quote: "The Data API enables you to seamlessly access data from Redshift Serverless with all types of traditional, cloud-native, and containerized serverless web service-based applications and event-driven applications." at <https://aws.amazon.com/blogs/big-data/use-the-amazon-redshift-data-api-to-interact-with-amazon-redshift-serverless/> (28/4/2023). Choose A, B and C are next chosen correct answers.

upvoted 2 times

✉ **james2033** 4 months, 2 weeks ago

Typo, I want said "C and E are next chosen correct answers."

upvoted 2 times

✉ **0628atv** 4 months, 2 weeks ago

Selected Answer: ACE

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

upvoted 2 times

✉ **Rob1L** 6 months, 1 week ago

Selected Answer: BCE

B. Supporting client-side and server-side encryption: Amazon Redshift supports both client-side and server-side encryption for improved data security.

C. Building analytics workloads during specified hours and when the application is not active: Amazon Redshift is optimized for running complex analytic queries against very large datasets, making it a good choice for this use case.

E. Scaling globally to support petabytes of data and tens of millions of requests per minute: Amazon Redshift is designed to handle petabytes of data, and to deliver fast query and I/O performance for virtually any size dataset.

upvoted 4 times

✉ **omoakin** 6 months, 1 week ago

CEF for me

upvoted 2 times

✉ **Efren** 6 months, 2 weeks ago

A seems correct

The Data API enables you to seamlessly access data from Redshift Serverless with all types of traditional, cloud-native, and containerized serverless web service-based applications and event-driven applications.

upvoted 1 times

✉ **Efren** 6 months, 2 weeks ago

BCE for me

upvoted 1 times

✉ **y0** 6 months, 2 weeks ago

U mean ACE rite?

upvoted 1 times

✉ **Efren** 6 months, 1 week ago

Yeah not sure, but i would say ACE

upvoted 1 times

✉ **nonsense** 6 months, 2 weeks ago

Selected Answer: ACF

b it's working, but not primary
upvoted 2 times

A company provides an API interface to customers so the customers can retrieve their financial information. The company expects a larger number of requests during peak usage times of the year.

The company requires the API to respond consistently with low latency to ensure customer satisfaction. The company needs to provide a compute host for the API.

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

- A. Use an Application Load Balancer and Amazon Elastic Container Service (Amazon ECS).
- B. Use Amazon API Gateway and AWS Lambda functions with provisioned concurrency.
- C. Use an Application Load Balancer and an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.
- D. Use Amazon API Gateway and AWS Lambda functions with reserved concurrency.

Correct Answer: B

Community vote distribution

B (100%)

 **cloudenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: B

In the context of the given scenario, where the company wants low latency and consistent performance for their API during peak usage times, it would be more suitable to use provisioned concurrency. By allocating a specific number of concurrent executions, the company can ensure that there are enough function instances available to handle the expected load and minimize the impact of cold starts. This will result in lower latency and improved performance for the API.

upvoted 7 times

 **Bennyboy789** Most Recent 3 months ago

Selected Answer: B

Provisioned - minimizing cold starts and providing low latency.

upvoted 4 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

This option provides the least operational overhead:

API Gateway handles the API requests and integration with Lambda
Lambda automatically scales compute without managing servers
Provisioned concurrency ensures consistent low latency by keeping functions initialized
No need to manage containers or orchestration platforms as with ECS/EKS

upvoted 1 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: B

The company requires the API to respond consistently with low latency to ensure customer satisfaction especially during high peak periods, there is no mention of cost efficient. Hence provisioned concurrency is the best option.
Provisioned concurrency is the number of pre-initialized execution environments you want to allocate to your function. These execution environments are prepared to respond immediately to incoming function requests. Configuring provisioned concurrency incurs charges to your AWS account.

<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html#:~:text=for%20a%20function.-,Provisioned%20concurrency,-%E2%80%93%20Provisioned%20concurrency%20is>

upvoted 1 times

 **MirKhobaeb** 6 months ago

Selected Answer: B

AWS Lambda provides a highly scalable and distributed infrastructure that automatically manages the underlying compute resources. It automatically scales your API based on the incoming request load, allowing it to respond consistently with low latency, even during peak times. AWS Lambda takes care of infrastructure provisioning, scaling, and resource management, allowing you to focus on writing the code for your API logic.

upvoted 3 times

A company wants to send all AWS Systems Manager Session Manager logs to an Amazon S3 bucket for archival purposes.

Which solution will meet this requirement with the MOST operational efficiency?

- A. Enable S3 logging in the Systems Manager console. Choose an S3 bucket to send the session data to.
- B. Install the Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Export the logs to an S3 bucket from the group for archival purposes.
- C. Create a Systems Manager document to upload all server logs to a central S3 bucket. Use Amazon EventBridge to run the Systems Manager document against all servers that are in the account daily.
- D. Install an Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Create a CloudWatch logs subscription that pushes any incoming log events to an Amazon Kinesis Data Firehose delivery stream. Set Amazon S3 as the destination.

Correct Answer: D

Community vote distribution

A (88%)

13%

 **potomac** 3 weeks, 2 days ago

Selected Answer: A

You can choose to store session log data in a specified Amazon Simple Storage Service (Amazon S3) bucket for debugging and troubleshooting purposes.

upvoted 1 times

 **deechean** 2 months, 4 weeks ago

Selected Answer: A

You can config the log archived to S3 in the Session Manager - > preference tab. Another option is CloudWatch log.

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging.html#session-manager-logging-s3>

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

°Simplicity - Enabling S3 logging requires just a simple configuration in the Systems Manager console to specify the destination S3 bucket. No other services need to be configured.

°Direct integration - Systems Manager has native support to send session logs to S3 through this feature. No need for intermediary services.

°Automated flow - Once S3 logging is enabled, the session logs automatically flow to the S3 bucket without manual intervention.

°Easy management - The S3 bucket can be managed independently for log storage and archival purposes without impacting Systems Manager.

°Cost-effectiveness - No charges for intermediate CloudWatch or Kinesis services. Just basic S3 storage costs.

°Minimal overhead - No ongoing management of complex pipeline of services. Direct logs to S3 minimizes overhead.

upvoted 1 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: A

With the MOST operational efficiency then option A is best.

Otherwise B is also an option with a little bit more ops than option A.

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

upvoted 1 times

 **Zox42** 4 months, 3 weeks ago

Selected Answer: A

Answer A. <https://aws-labs.net/winlab5-manageinfra/sessmgrlog.html>

upvoted 1 times

 **Zuit** 5 months ago

Selected Answer: A

GPT argued for D.

B could be an option, by installing a logging package on alle managed systems/ECs etc. <https://docs.aws.amazon.com/systems-manager/latest/userguide/distributor-working-with-packages-deploy.html>

However, as it mentions the "Session manager logs" I would tend towards A.

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: A

It should be "A".

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

upvoted 1 times

✉ **secdgs** 5 months, 2 weeks ago

Selected Answer: A

It have menu to Enable S3 Logging.

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging.html#session-manager-logging-s3>

upvoted 1 times

✉ **Markie999** 5 months, 3 weeks ago

Selected Answer: B

BBBBBBBBBB

upvoted 1 times

✉ **Bill1000** 5 months, 3 weeks ago

Selected Answer: B

The option 'A' says "Enable S3 logging in the Systems Manager console." This means that you will enable the logs !! FOR !! S3 events and its is not what the question asks. My vote is for Option B, based on this article: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 1 times

✉ **baba365** 4 months, 3 weeks ago

To log session data using Amazon S3 (console)

Open the AWS Systems Manager console at <https://console.aws.amazon.com/systems-manager/>.

In the navigation pane, choose Session Manager.

Choose the Preferences tab, and then choose Edit.

Select the check box next to Enable under S3 logging.

upvoted 2 times

✉ **vrevkov** 5 months, 1 week ago

But where do you want to install the Amazon CloudWatch agent in case of B?

upvoted 1 times

✉ **omoakin** 6 months ago

DDDDDD

upvoted 1 times

✉ **Anmol_1010** 6 months, 1 week ago

Option D is definitely not right,

Its option B

upvoted 1 times

✉ **omoakin** 6 months, 1 week ago

Chat GPT says option A is incorrect cos it requires enabling S3 logging in the system manager console only logs information about the systems manager service not the session logs

Says correct answer is B

upvoted 1 times

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

Question may not be very clear. A should be the answer. Below link is the documentation:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging.html#session-manager-logging-s3>

upvoted 3 times

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

Selected Answer: A

option A does not involve CloudWatch, while option D does. Therefore, in terms of operational overhead, option A would generally have less complexity and operational overhead compared to option D.

Option A simply enables S3 logging in the Systems Manager console, allowing you to directly send session logs to an S3 bucket. This approach is straightforward and requires minimal configuration.

On the other hand, option D involves installing and configuring the Amazon CloudWatch agent, creating a CloudWatch log group, setting up a CloudWatch Logs subscription, and configuring an Amazon Kinesis Data Firehose delivery stream to store logs in an S3 bucket. This requires additional setup and management compared to option A.

So, if minimizing operational overhead is a priority, option A would be a simpler and more straightforward choice.

upvoted 3 times

✉ **nonsense** 6 months, 2 weeks ago

Selected Answer: A

A MOST operational efficiency?

upvoted 3 times

An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime.

Which solution meets these requirements with the LEAST amount of effort?

- A. Enable storage autoscaling in RDS
- B. Increase the RDS database instance size
- C. Change the RDS database instance storage type to Provisioned IOPS
- D. Back up the RDS database, increase the storage capacity, restore the database, and stop the previous instance

Correct Answer: A

Community vote distribution

A (100%)

✉  **clouduenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: A

Enabling storage autoscaling allows RDS to automatically adjust the storage capacity based on the application's needs. When the storage usage exceeds a predefined threshold, RDS will automatically increase the allocated storage without requiring manual intervention or causing downtime. This ensures that the RDS database has sufficient disk space to handle the increasing storage requirements.

upvoted 8 times

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

Selected Answer: A

Amazon RDS for MariaDB, Amazon RDS for MySQL, Amazon RDS for PostgreSQL, Amazon RDS for SQL Server and Amazon RDS for Oracle support RDS Storage Auto Scaling. RDS Storage Auto Scaling automatically scales storage capacity in response to growing database workloads, with zero downtime.

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

This question is so obvious

upvoted 1 times

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

Selected Answer: A

RDS Storage Auto Scaling continuously monitors actual storage consumption, and scales capacity up automatically when actual utilization approaches provisioned storage capacity. Auto Scaling works with new and existing database instances. You can enable Auto Scaling with just a few clicks in the AWS Management Console. There is no additional cost for RDS Storage Auto Scaling. You pay only for the RDS resources needed to run your applications.

<https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/#:~:text=of%20the%20rest.-,RDS%20Storage%20Auto%20Scaling,-continuously%20monitors%20actual>

upvoted 1 times

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

Selected Answer: A

Quote "Amazon RDS now supports Storage Auto Scaling" and "... with zero downtime." (Jun 20th 2019) at <https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/>

upvoted 1 times

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

Hello moderator, please help me delete this discussion, I already add content before this comment.

upvoted 1 times

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

Selected Answer: A

See "Amazon RDS now supports Storage Auto Scaling. Posted On: Jun 20, 2019. Starting today, Amazon RDS for MariaDB, Amazon RDS for MySQL, Amazon RDS for PostgreSQL, Amazon RDS for SQL Server and Amazon RDS for Oracle support RDS Storage Auto Scaling. RDS Storage Auto Scaling automatically scales storage capacity in response to growing database workloads, with zero downtime." at <https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/>

upvoted 2 times

✉  **haoAWS** 5 months ago

Selected Answer: A

- A is the best answer.
- B will not work for increasing disk space, it only improve the IO performance.
- C will not work because it will cause downtime.
- D is too complicated and need much operational effort.

upvoted 1 times

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

<https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/>

upvoted 1 times

✉  **Anmol_1010** 6 months, 1 week ago

The key word is No Down time. A would be best option

upvoted 2 times

A consulting company provides professional services to customers worldwide. The company provides solutions and tools for customers to expedite gathering and analyzing data on AWS. The company needs to centrally manage and deploy a common set of solutions and tools for customers to use for self-service purposes.

Which solution will meet these requirements?

- A. Create AWS CloudFormation templates for the customers.
- B. Create AWS Service Catalog products for the customers.
- C. Create AWS Systems Manager templates for the customers.
- D. Create AWS Config items for the customers.

Correct Answer: B

Community vote distribution

B (100%)

 **cludenthusiast** Highly Voted 6 months, 1 week ago

Selected Answer: B

AWS Service Catalog allows you to create and manage catalogs of IT services that can be deployed within your organization. With Service Catalog, you can define a standardized set of products (solutions and tools in this case) that customers can self-service provision. By creating Service Catalog products, you can control and enforce the deployment of approved and validated solutions and tools.

upvoted 7 times

 **Oblako** 1 day, 16 hours ago

"within your organization" => not for customers

upvoted 1 times

 **Guru4Cloud** Most Recent 3 months, 1 week ago

Selected Answer: B

Some key advantages of using Service Catalog:

Centralized management - Products can be maintained in a single catalog for easy discovery and governance.

Self-service access - Customers can deploy the solutions on their own without manual intervention.

Standardization - Products provide pre-defined templates for consistent deployment.

Access control - Granular permissions can be applied to restrict product visibility and access.

Reporting - Service Catalog provides detailed analytics on product usage and deployments.

upvoted 2 times

 **hsinchang** 4 months ago

Selected Answer: B

CloudFormation: a code as infrastructure service

Systems Manager: management solution for resources

Config: assess, audit and evaluate configurations

Other options does not fit this scenario.

upvoted 1 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: B

AWS Service Catalog lets you centrally manage your cloud resources to achieve governance at scale of your infrastructure as code (IaC) templates, written in CloudFormation or Terraform. With AWS Service Catalog, you can meet your compliance requirements while making sure your customers can quickly deploy the cloud resources they need.

<https://aws.amazon.com/servicecatalog/#:~:text=How%20it%20works-,AWS%20Service%20Catalog,-lets%20you%20centrally>

upvoted 1 times

 **Yadav_Sanjay** 6 months ago

Selected Answer: B

<https://docs.aws.amazon.com/servicecatalog/latest/adminguide/introduction.html>

upvoted 2 times

A company is designing a new web application that will run on Amazon EC2 Instances. The application will use Amazon DynamoDB for backend data storage. The application traffic will be unpredictable. The company expects that the application read and write throughput to the database will be moderate to high. The company needs to scale in response to application traffic.

Which DynamoDB table configuration will meet these requirements MOST cost-effectively?

- A. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard table class. Set DynamoDB auto scaling to a maximum defined capacity.
- B. Configure DynamoDB in on-demand mode by using the DynamoDB Standard table class.
- C. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class. Set DynamoDB auto scaling to a maximum defined capacity.
- D. Configure DynamoDB in on-demand mode by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class.

Correct Answer: B

Community vote distribution

B (60%)	A (30%)	5%
---------	---------	----

✉  **Efren**  6 months, 2 weeks ago

B for me. Provisioned if we know how much traffic will come, but its unpredictable, so we have to go for on-demand upvoted 5 times

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

Spot On
upvoted 1 times

✉  **dilaaziz**  2 weeks ago

Selected Answer: D

Data storage: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithTables.tableclasses.html>
upvoted 1 times

✉  **potomac** 3 weeks, 2 days ago

Selected Answer: B

On-demand mode is great for unpredictable traffic
upvoted 1 times

✉  **bsbs1234** 1 month, 2 weeks ago

I choose B
I think the items stored in the table in this question has large size. So each read/write, a big chunk of data pass through. A capacity unit is used to describe data throughput. provision to the high capacity units will be a waste because unpredicted traffic pattern.
upvoted 1 times

✉  **Bennyboy789** 3 months ago

Selected Answer: B

Unpredictable= on demand
upvoted 2 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

The key factors are:

With On-Demand mode, you only pay for what you use instead of over-provisioning capacity. This avoids idle capacity costs.
DynamoDB Standard provides the fastest performance needed for moderate-high traffic apps vs Standard-IA which is for less frequent access.
Auto scaling with provisioned capacity can also work but requires more administrative effort to tune the scaling thresholds.
upvoted 1 times

✉  **msdnpro** 4 months ago

Selected Answer: B

Support for B from AWS:

On-demand mode is a good option if any of the following are true:

- You create new tables with unknown workloads.
- You have unpredictable application traffic.
- You prefer the ease of paying for only what you use.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>

upvoted 1 times

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

Selected Answer: B

Technically both options A and B will work. But this statement 'traffic will be unpredictable' rules out option A, because 'provisioned mode' was made for scenarios where traffic is predictable.

So I will stick with B, because 'on-demand mode' is made for unpredictable traffic and instantly accommodates workloads as they ramp up or down.

upvoted 1 times

✉ **0628atv** 4 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html>

upvoted 2 times

✉ **wRhlH** 5 months ago

Selected Answer: C

Not B for sure, "The company needs to scale in response to application traffic."

Between A and C, I would choose C. Because it's a new application, and the traffic will be from moderate to high. So by choosing C, it's both cost-effective and scalable

upvoted 1 times

✉ **live_reply_developers** 5 months ago

Selected Answer: A

"With provisioned capacity mode, you specify the number of reads and writes per second that you expect your application to require, and you are billed based on that. Furthermore if you can forecast your capacity requirements you can also reserve a portion of DynamoDB provisioned capacity and optimize your costs even further.

With provisioned capacity you can also use auto scaling to automatically adjust your table's capacity based on the specified utilization rate to ensure application performance, and also to potentially reduce costs. To configure auto scaling in DynamoDB, set the minimum and maximum levels of read and write capacity in addition to the target utilization percentage."

<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>

upvoted 2 times

✉ **F629** 5 months, 1 week ago

Selected Answer: A

I think it's A. B is on-demand, but it may not save money. If it's a not-busy application, on-demand may save money, but to a medium to high busy level application, I prefer a provisioned.

upvoted 1 times

✉ **Rob1L** 6 months, 1 week ago

Selected Answer: B

unpredictable = on-demand

upvoted 3 times

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

Selected Answer: B

AWS Service Catalog allows you to create and manage catalogs of IT services that can be deployed within your organization. With Service Catalog, you can define a standardized set of products (solutions and tools in this case) that customers can self-service provision. By creating Service Catalog products, you can control and enforce the deployment of approved and validated solutions and tools.

upvoted 3 times

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

On-Demand Mode: With on-demand mode, DynamoDB automatically scales its capacity to handle the application's traffic.

DynamoDB Standard Table Class: The DynamoDB Standard table class provides a balance between cost and performance.

Cost-Effectiveness: By using on-demand mode, the company only pays for the actual read and write requests made to the table, rather than provisioning and paying for a fixed amount of capacity units in advance.

upvoted 4 times

✉ **nonsense** 6 months, 2 weeks ago

Selected Answer: A

a for me

upvoted 1 times

✉ **nonsense** 6 months, 1 week ago

changed for C.

Option A: need to purchase more capacity than they actually need This would lead to unnecessary costs.

Option B: company's application is expected to have moderate to high read and write throughput, so this option would not be sufficient.

C Configure DynamoDB with provisioned read and write by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class. Set DynamoDB auto scaling to a maximum defined capacity.

upvoted 1 times

A retail company has several businesses. The IT team for each business manages its own AWS account. Each team account is part of an organization in AWS Organizations. Each team monitors its product inventory levels in an Amazon DynamoDB table in the team's own AWS account.

The company is deploying a central inventory reporting application into a shared AWS account. The application must be able to read items from all the teams' DynamoDB tables.

Which authentication option will meet these requirements MOST securely?

- A. Integrate DynamoDB with AWS Secrets Manager in the inventory application account. Configure the application to use the correct secret from Secrets Manager to authenticate and read the DynamoDB table. Schedule secret rotation for every 30 days.
- B. In every business account, create an IAM user that has programmatic access. Configure the application to use the correct IAM user access key ID and secret access key to authenticate and read the DynamoDB table. Manually rotate IAM access keys every 30 days.
- C. In every business account, create an IAM role named BU_ROLE with a policy that gives the role access to the DynamoDB table and a trust policy to trust a specific role in the inventory application account. In the inventory account, create a role named APP_ROLE that allows access to the STS AssumeRole API operation. Configure the application to use APP_ROLE and assume the crossaccount role BU_ROLE to read the DynamoDB table.
- D. Integrate DynamoDB with AWS Certificate Manager (ACM). Generate identity certificates to authenticate DynamoDB. Configure the application to use the correct certificate to authenticate and read the DynamoDB table.

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

IAM Roles: IAM roles provide a secure way to grant permissions to entities within AWS. By creating an IAM role in each business account named BU_ROLE with the necessary permissions to access the DynamoDB table, the access can be controlled at the IAM role level.

Cross-Account Access: By configuring a trust policy in the BU_ROLE that trusts a specific role in the inventory application account (APP_ROLE), you establish a trusted relationship between the two accounts.

Least Privilege: By creating a specific IAM role (BU_ROLE) in each business account and granting it access only to the required DynamoDB table, you can ensure that each team's table is accessed with the least privilege principle.

Security Token Service (STS): The use of STS AssumeRole API operation in the inventory application account allows the application to assume the cross-account role (BU_ROLE) in each business account.

upvoted 15 times

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

Well broken down..thank you :)

upvoted 2 times

✉  **Bennyboy789**  3 months ago

Selected Answer: C

Keyword: IAM ROLES

upvoted 2 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

C is the most secure option to meet the requirements.

Using cross-account IAM roles and role chaining allows the inventory application to securely access resources in other accounts. The roles provide temporary credentials and can be permissions controlled.

upvoted 1 times

✉  **hsinchang** 4 months ago

Selected Answer: C

Looks complex, but IAM role seems more probable, I go with C.

upvoted 3 times

✉  **mattcl** 5 months, 1 week ago

Why not A?

upvoted 3 times

✉  **antropaws** 5 months, 1 week ago

Selected Answer: C

It's complex, but looks C.

upvoted 1 times

✉  **eehhssaan** 6 months, 1 week ago

i'll go with C .. coming from two minds

upvoted 2 times

✉  **nonsense** 6 months, 1 week ago

a or c. C looks like a more secure

upvoted 1 times

✉  **omoakin** 6 months, 1 week ago

CCCCCCCCCC

upvoted 1 times

A company runs container applications by using Amazon Elastic Kubernetes Service (Amazon EKS). The company's workload is not consistent throughout the day. The company wants Amazon EKS to scale in and out according to the workload.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Use an AWS Lambda function to resize the EKS cluster.
- B. Use the Kubernetes Metrics Server to activate horizontal pod autoscaling.
- C. Use the Kubernetes Cluster Autoscaler to manage the number of nodes in the cluster.
- D. Use Amazon API Gateway and connect it to Amazon EKS.
- E. Use AWS App Mesh to observe network activity.

Correct Answer: BC

Community vote distribution

BC (100%)

 **wsdasdasdqwdaw** 1 month ago

K8S Metrics Server and Autoscaler => B and C

upvoted 2 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: BC

B and C are the correct options.

Using the Kubernetes Metrics Server (B) enables horizontal pod autoscaling to dynamically scale pods based on CPU/memory usage. This allows scaling at the application tier level.

The Kubernetes Cluster Autoscaler (C) automatically adjusts the number of nodes in the EKS cluster in response to pod resource requirements and events. This allows scaling at the infrastructure level.

upvoted 2 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: BC

This is pretty straight forward.

Use the Kubernetes Metrics Server to activate horizontal pod autoscaling.

Use the Kubernetes Cluster Autoscaler to manage the number of nodes in the cluster.

upvoted 2 times

 **james2033** 4 months, 2 weeks ago

Selected Answer: BC

Kubernetes Metrics Server <https://docs.aws.amazon.com/eks/latest/userguide/metrics-server.html>

AWS Autoscaler <https://docs.aws.amazon.com/eks/latest/userguide/autoscaling.html> and
<https://github.com/kubernetes/autoscaler/blob/master/cluster-autoscaler/cloudprovider/aws/README.md>

upvoted 2 times

 **cloudenthusiast** 6 months, 1 week ago

Selected Answer: BC

By combining the Kubernetes Cluster Autoscaler (option C) to manage the number of nodes in the cluster and enabling horizontal pod autoscaling (option B) with the Kubernetes Metrics Server, you can achieve automatic scaling of your EKS cluster and container applications based on workload demand. This approach minimizes operational overhead as it leverages built-in Kubernetes functionality and automation mechanisms.

upvoted 4 times

 **nonsense** 6 months, 1 week ago

Selected Answer: BC

b and c is right

upvoted 1 times

A company runs a microservice-based serverless web application. The application must be able to retrieve data from multiple Amazon DynamoDB tables. A solutions architect needs to give the application the ability to retrieve the data with no impact on the baseline performance of the application.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. AWS AppSync pipeline resolvers
- B. Amazon CloudFront with Lambda@Edge functions
- C. Edge-optimized Amazon API Gateway with AWS Lambda functions
- D. Amazon Athena Federated Query with a DynamoDB connector

Correct Answer: A

Community vote distribution

B (50%)	D (32%)	A (18%)
---------	---------	---------

✉  **omoakin**  6 months, 1 week ago

Great work made it to the last question. Goodluck to you all
upvoted 15 times

✉  **cyber_bedouin** 1 month, 1 week ago

Thanks. Do you think the questions after 500 are relevant, they seem to be above associate level (harder)
upvoted 1 times

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

good luck to you as well.
upvoted 4 times

✉  **elmogy**  6 months ago

just passed yesterday 30-05-23, around 75% of the exam came from here, some with light changes.
upvoted 13 times

✉  **hungta**  1 week, 6 days ago

Selected Answer: B

For an operationally efficient solution that minimizes impact on baseline performance in a microservice-based serverless web application retrieving data from multiple DynamoDB tables, Amazon CloudFront with Lambda@Edge functions (Option B) is often the most suitable choice
upvoted 1 times

✉  **thanhnv142** 1 month ago

D is correct. There is construction of how to retrieve data from DynamoDB with Athena
<https://docs.aws.amazon.com/athena/latest/ug/connect-to-a-data-source.html>
upvoted 1 times

✉  **pmlabs** 1 month, 3 weeks ago

The Answer is A. Some use case for AWS AppSync is Unified data access.
Consolidate data from multiple databases, APIs, and microservices in a single network call, from a single endpoint, abstracting backend complexity.
https://aws.amazon.com/pm/appsync/?trk=e37f908f-322e-4ebc-9def-9eafa78141b8&sc_channel=ps&ef_id=Cj0KCQjwmvSoBhDOARIsAK6aV7jtg2I6jyXBH6_uUOKRrRoLmXQxaGbwYBP0aO1-RmauWW55DuXSGTMaAnT9EALw_wcB:G:s&s_kwid=AL!4422!3!647301987556!e!!g!!aws%20appsync!19613610159!148358960849
upvoted 2 times

✉  **Linerd** 2 months, 2 weeks ago

Selected Answer: B

B - seems more operationally efficient

A: example to make use of GraphQL with multi DynamoDB tables <https://www.youtube.com/watch?v=HSDKN43Vx7U>
but it seems not the most operationally efficient to set it up

D: it can be useful when needs to join multi DynamoDB tables

But also "querying DynamoDB using Athena can be slower and more expensive than querying directly using DynamoDB"
refer to <https://medium.com/@saswat.sahoo.1988/combine-the-simplicity-of-sql-with-the-power-of-nosql-pt-2-cff1c524297e>
upvoted 1 times

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

Selected Answer: A

A is correct.

<https://aws.amazon.com/blogs/mobile/appsync-pipeline-resolvers-2/>

upvoted 1 times

✉ **BrijMohan08** 2 months, 4 weeks ago

Selected Answer: A

https://aws.amazon.com/pm/appsync/?trk=66d9071f-eec2-471d-9fc0-c374dbda114d&sc_channel=ps&ef_id=CjwKCAjww7KmBhAyEiwA5-PUSi9OTSRu78WOh7NuprbbbjyhVXWI4tBIPquEqRIXGn-HLFh5qOqfRoCOMMQAvD_BwE:G:s&s_kwcid=AL!4422!3!646025317347!e!!g!!aws%20appsync!19610918335!148058250160

upvoted 1 times

✉ **Wayne23Fang** 3 months ago

Selected Answer: D

I like D) the most. D. Amazon Athena Federated Query with a DynamoDB connector.

I don't like A) since this is not a GraphQL query.

I don't like B). Since Query multiple tables in DynamoDB from Lambda may not be efficient.

upvoted 1 times

✉ **cd93** 3 months, 1 week ago

Selected Answer: A

A. AppSync reduces operational effort, you only need to know GraphQL, AppSync provides caching ability to reduce loads on source

B. Also provide caches through CloudFront, but require writing more 'low-level' codes on Lambda

D. Requires a Lambda to create connection to DynamoDB source, also no caching

upvoted 1 times

✉ **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

B. Amazon CloudFront with Lambda@Edge functions

upvoted 1 times

✉ **mtmayer** 3 months, 1 week ago

Selected Answer: A

Simplify application development with GraphQL APIs by providing a single endpoint to securely query or update data from multiple databases, microservices, and APIs.

https://aws.amazon.com/pm/appsync/?trk=66d9071f-eec2-471d-9fc0-c374dbda114d&sc_channel=ps&ef_id=CjwKCAjww7KmBhAyEiwA5-PUSi9OTSRu78WOh7NuprbbbjyhVXWI4tBIPquEqRIXGn-HLFh5qOqfRoCOMMQAvD_BwE:G:s&s_kwcid=AL!4422!3!646025317347!e!!g!!aws%20appsync!19610918335!148058250160

upvoted 1 times

✉ **zakiahkhatami** 4 months ago

Selected Answer: B

i think B is correct

upvoted 1 times

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

Selected Answer: B

Cloud front was build specifically to resolve performance issues.

upvoted 1 times

✉ **narddrer** 4 months, 3 weeks ago

Selected Answer: D

option A is to query multiple DB's

Option D is to query multiple tables in DB

upvoted 1 times

✉ **wRhlH** 5 months ago

Why not c

upvoted 1 times

✉ **DrWatson** 5 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/athena/latest/ug/connectors-dynamodb.html>

upvoted 2 times

A company wants to analyze and troubleshoot Access Denied errors and Unauthorized errors that are related to IAM permissions. The company has AWS CloudTrail turned on.

Which solution will meet these requirements with the LEAST effort?

- A. Use AWS Glue and write custom scripts to query CloudTrail logs for the errors.
- B. Use AWS Batch and write custom scripts to query CloudTrail logs for the errors.
- C. Search CloudTrail logs with Amazon Athena queries to identify the errors.
- D. Search CloudTrail logs with Amazon QuickSight. Create a dashboard to identify the errors.

Correct Answer: C

Community vote distribution

C (53%) D (47%)

 **bogobob** 1 week, 5 days ago

Selected Answer: D

The question asks specifically to "analyze and troubleshoot". While Athena is easy to get the data, you then just have a list of logs. Not very useful to troubleshoot...

upvoted 1 times

 **NickGordon** 2 weeks, 5 days ago

Selected Answer: D

Quick Sight is an analytics tool. Sounds like a LEAST effort option

upvoted 2 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

Athena allows you to run SQL queries on data in Amazon S3, including CloudTrail logs. It is the easiest way to query the logs and identify specific errors without needing to write any custom code or scripts.

With Athena, you can write simple SQL queries to filter the CloudTrail logs for the "AccessDenied" and "UnauthorizedOperation" error codes. This will return the relevant log entries that you can then analyze.

upvoted 2 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: C

C for me. Using Athena with CloudTrail logs is a powerful way to enhance your analysis of AWS service activity. For example, you can use queries to identify trends and further isolate activity by attributes, such as source IP address or user.

<https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html#:~:text=CloudTrail%20Lake%20documentation.-,Using%20Athena,-with%20CloudTrail%20logs>

upvoted 1 times

 **james2033** 4 months, 2 weeks ago

Selected Answer: C

IAM and CloudTrail <https://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html#stscloudtrailexample-assumerole>.
Query CloudTrail logs by Athena <https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html#tips-for-querying-cloudtrail-logs#tips-for-querying-cloudtrail-logs>

upvoted 1 times

 **james2033** 4 months, 2 weeks ago

Choose C, not D, because need "analyze and troubleshoot", not just see on dashboard (in D).

upvoted 1 times

 **live_reply_developers** 4 months, 2 weeks ago

Selected Answer: C

Amazon Athena is an interactive query service provided by AWS that enables you to analyze data , is a little bit more suitable integrated with cloud trail that permit to verify WHO accessed the service.

upvoted 1 times

 **manuh** 5 months ago

Selected Answer: C

Dashboard isn't requires. Also refer to this <https://repost.aws/knowledge-center/troubleshoot-iam-permission-errors>

upvoted 1 times

✉ **haoAWS** 5 months ago

Selected Answer: D

I am struggling for the C and D for a long time, and ask the chatGPT. The chatGPT says D is better, since Athena requires more expertise on SQL.
upvoted 1 times

✉ **antropaws** 5 months, 1 week ago

Selected Answer: D

Both C and D are feasible. I vote for D:

Amazon QuickSight supports logging the following actions as events in CloudTrail log files:

- Whether the request was made with root or AWS Identity and Access Management user credentials
- Whether the request was made with temporary security credentials for an IAM role or federated user
- Whether the request was made by another AWS service

<https://docs.aws.amazon.com/quicksight/latest/user/logging-using-cloudtrail.html>

upvoted 1 times

✉ **PCWu** 5 months, 2 weeks ago

Selected Answer: C

The Answer will be C:

Need to use Athena to query keywords and sort out the error logs.

D: No need to use Amazon QuickSight to create the dashboard.

upvoted 1 times

✉ **Axeashes** 5 months, 2 weeks ago

Selected Answer: C

"Using Athena with CloudTrail logs is a powerful way to enhance your analysis of AWS service activity."

<https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html>

upvoted 1 times

✉ **oras2023** 5 months, 3 weeks ago

Selected Answer: C

Analyse and TROUBLESHOOT, look like Athena

upvoted 1 times

✉ **oras2023** 5 months, 2 weeks ago

<https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html>

upvoted 1 times

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

Selected Answer: D

It specifies analyze, not query logs.

Which is why option D is the best one as it provides dashboards to analyze the logs.

upvoted 3 times

A company wants to add its existing AWS usage cost to its operation cost dashboard. A solutions architect needs to recommend a solution that will give the company access to its usage cost programmatically. The company must be able to access cost data for the current year and forecast costs for the next 12 months.

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

- A. Access usage cost-related data by using the AWS Cost Explorer API with pagination.
- B. Access usage cost-related data by using downloadable AWS Cost Explorer report .csv files.
- C. Configure AWS Budgets actions to send usage cost data to the company through FTP.
- D. Create AWS Budgets reports for usage cost data. Send the data to the company through SMTP.

Correct Answer: D

Community vote distribution

A (100%)

 **TariqKipkemei** 2 weeks ago

Selected Answer: A

access to its usage cost programmatically = AWS Cost Explorer API

upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

A: correct

1. programmatically = API
2. In the next 12 months = cost explorer

upvoted 1 times

 **BrijMohan08** 2 months, 4 weeks ago

Selected Answer: A

Keyword

12 months, API Support

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

upvoted 4 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

Access usage cost-related data by using the AWS Cost Explorer API with pagination

upvoted 2 times

 **wendaz** 1 month, 2 weeks ago

don't repeat the answer, it is useless... explain , okay? i have seen your replies many time just to copy the options.. it makes no sense...

upvoted 2 times

 **james2033** 4 months, 2 weeks ago

Selected Answer: A

AWS Cost Explorer API with paginated request: <https://docs.aws.amazon.com/cost-management/latest/userguide/ce-api-best-practices.html#ce-api-best-practices-optimize-costs>

upvoted 2 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: A

From AWS Documentation*:

"You can view your costs and usage using the Cost Explorer user interface free of charge. You can also access your data programmatically using the Cost Explorer API. Each paginated API request incurs a charge of \$0.01. You can't disable Cost Explorer after you enable it."

* Source:

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

<https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-cost-explorer/interfaces/costexplorerpaginationconfiguration.html>

upvoted 3 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: A

Answer is: A

says dashboard = Cost Explorer, therefor C & D are eliminated.

also says programmatically, means non manual intervention therefor API.

upvoted 4 times

 **oras2023** 5 months, 3 weeks ago

Selected Answer: A

least operational overhead = API access

upvoted 3 times

 **oras2023** 5 months, 3 weeks ago

least operational overhead = API access

upvoted 1 times

A solutions architect is reviewing the resilience of an application. The solutions architect notices that a database administrator recently failed over the application's Amazon Aurora PostgreSQL database writer instance as part of a scaling exercise. The failover resulted in 3 minutes of downtime for the application.

Which solution will reduce the downtime for scaling exercises with the LEAST operational overhead?

- A. Create more Aurora PostgreSQL read replicas in the cluster to handle the load during failover.
- B. Set up a secondary Aurora PostgreSQL cluster in the same AWS Region. During failover, update the application to use the secondary cluster's writer endpoint.
- C. Create an Amazon ElastiCache for Memcached cluster to handle the load during failover.
- D. Set up an Amazon RDS proxy for the database. Update the application to use the proxy endpoint.

Correct Answer: D

Community vote distribution

D (90%) 10%

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

Selected Answer: D

D is the correct answer.
It is talking about the write database. Not reader.
Amazon RDS proxy allows you to automatically route write request to the healthy writer, minimizing downtime.
upvoted 8 times

✉️  **nilandd44gg** 4 months ago

One of the benefits of Amazon RDS Proxy is that it can improve application recovery time after database failovers. While RDS Proxy supports both MySQL as well as PostgreSQL engines, in this post, we will use a MySQL test workload to demonstrate how RDS Proxy reduces client recovery time after failover by up to 79% for Amazon Aurora MySQL and by up to 32% for Amazon RDS for MySQL.
<https://aws.amazon.com/blogs/database/improving-application-availability-with-amazon-rds-proxy/>
<https://aws.amazon.com/rds/proxy/faqs/>

upvoted 2 times

✉️  **Guru4Cloud**  3 months, 1 week ago

Selected Answer: D

D. Set up an Amazon RDS proxy for the database. Update the application to use the proxy endpoint.
upvoted 1 times

✉️  **hachiri** 3 months, 1 week ago

point is Aurora Multi-Master
Set up a secondary Aurora PostgreSQL cluster in the *same* AWS Region
upvoted 2 times

✉️  **hachiri** 3 months, 1 week ago

I mean correct is B
upvoted 1 times

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

Selected Answer: C

Availability is the main requirement here. Even if RDS proxy is used, it will still find the writer instance unavailable during the scaling exercise.
Best option is to create an Amazon ElastiCache for Memcached cluster to handle the load during the scaling operation.
upvoted 1 times

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

Set up an Amazon RDS proxy for the database. Update the application to use the proxy endpoint.
D is the answer
upvoted 3 times

A company has a regional subscription-based streaming service that runs in a single AWS Region. The architecture consists of web servers and application servers on Amazon EC2 instances. The EC2 instances are in Auto Scaling groups behind Elastic Load Balancers. The architecture includes an Amazon Aurora global database cluster that extends across multiple Availability Zones.

The company wants to expand globally and to ensure that its application has minimal downtime.

Which solution will provide the MOST fault tolerance?

- A. Extend the Auto Scaling groups for the web tier and the application tier to deploy instances in Availability Zones in a second Region. Use an Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
- B. Deploy the web tier and the application tier to a second Region. Add an Aurora PostgreSQL cross-Region Aurora Replica in the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.
- C. Deploy the web tier and the application tier to a second Region. Create an Aurora PostgreSQL database in the second Region. Use AWS Database Migration Service (AWS DMS) to replicate the primary database to the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
- D. Deploy the web tier and the application tier to a second Region. Use an Amazon Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.

Correct Answer: B

Community vote distribution

D (90%) 5%

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

Selected Answer: D

Auto Scaling groups can span Availability Zones, but not AWS regions.

Hence the best option is to deploy the web tier and the application tier to a second Region. Use an Amazon Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.

upvoted 11 times

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

Selected Answer: D

EC2 Auto Scaling groups are regional constructs. They can span Availability Zones, but not AWS regions

upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

527:

D is correct:

- B & C is not correct because it mentions Aurora PostgreSQL which is not mentioned in the question
- A is not correct because Auto scaling group can not span regions

upvoted 3 times

 **wsdasdasdqwdaw** 1 month ago

Simple as that.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: D

Using an Aurora global database that spans both the primary and secondary regions provides automatic replication and failover capabilities for the database tier.

Deploying the web and application tiers to a second region provides fault tolerance for those components.

Using Route53 health checks and failover routing will route traffic to the secondary region if the primary region becomes unavailable.

This provides fault tolerance across all tiers of the architecture while minimizing downtime. Promoting the secondary database to primary ensures the second region can continue operating if needed.

A is close, but doesn't provide an automatic database failover capability.

B and C provide database replication, but not automatic failover.

So D is the most comprehensive and fault tolerant architecture.

upvoted 2 times

 **Zox42** 4 months, 3 weeks ago

Selected Answer: D

Answer D

upvoted 1 times

 **Zuit** 5 months ago

Selected Answer: D

D seems fitting: Global Database and deploying it in the new region

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: B

B is correct!

upvoted 1 times

 **manuh** 5 months ago

Replicated db doesn't mean they will act as a single db once the transfer is completed. Global db is the correct approach

upvoted 1 times

 **r3mo** 5 months, 2 weeks ago

"D" is the answer: because Aws Aurora Global Database allows you to read and write from any region in the global cluster. This enables you to distribute read and write workloads globally, improving performance and reducing latency. Data is replicated synchronously across regions, ensuring strong consistency.

upvoted 3 times

 **Henrytml** 5 months, 2 weeks ago

Selected Answer: A

A is the only answer remain using ELB, both Web/App/DB has been taking care with replicating in 2nd region, lastly route 53 for failover over multiple regions

upvoted 1 times

 **manuh** 5 months ago

also Asg cant span beyond a region

upvoted 1 times

 **Henrytml** 5 months, 2 weeks ago

i will revoke my answer to standby web in 2nd region, instead of trigger to scale out

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: D

B&C are discarded.

The answer is between A and D.

I would go with D because it explicitly created this web / app tier in second region, instead A just autoscales into a secondary region, rather than always having resources in this second region.

upvoted 3 times

A data analytics company wants to migrate its batch processing system to AWS. The company receives thousands of small data files periodically during the day through FTP. An on-premises batch job processes the data files overnight. However, the batch job takes hours to finish running.

The company wants the AWS solution to process incoming data files as soon as possible with minimal changes to the FTP clients that send the files. The solution must delete the incoming data files after the files have been processed successfully. Processing for each file needs to take 3-8 minutes.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Use an Amazon EC2 instance that runs an FTP server to store incoming files as objects in Amazon S3 Glacier Flexible Retrieval. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the objects nightly from S3 Glacier Flexible Retrieval. Delete the objects after the job has processed the objects.
- B. Use an Amazon EC2 instance that runs an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the files nightly from the EBS volume. Delete the files after the job has processed the files.
- C. Use AWS Transfer Family to create an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use an Amazon S3 event notification when each file arrives to invoke the job in AWS Batch. Delete the files after the job has processed the files.
- D. Use AWS Transfer Family to create an FTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and to delete the files after they are processed. Use an S3 event notification to invoke the Lambda function when the files arrive.

Correct Answer: B

Community vote distribution

D (91%) 9%

✉ **wsdasdasdqwdaw** 1 month ago

FTP => AWS Transfer Family, => C or D, but in C is used EBS not S3 which needs EC2 and in general is more complex => very clear D.
upvoted 1 times

✉ **Guru4Cloud** 3 months, 1 week ago

Selected Answer: D

The key points:

Use AWS Transfer Family for the FTP server to receive files directly into S3. This avoids managing FTP servers.
Process each file as soon as it arrives using Lambda triggered by S3 events. Lambda provides fast processing time per file.
Lambda can also delete files after processing succeeds.
Options A, B, C involve more operational overhead of managing FTP servers and batch jobs. Processing latency would be higher waiting for batch windows.
Storing files in Glacier (Option A) adds latency for retrieving files.
upvoted 1 times

✉ **hsinchang** 4 months ago

Selected Answer: D

Processing for each file needs to take 3-8 minutes clearly indicates Lambda functions.
upvoted 1 times

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

Selected Answer: D

Process incoming data files with minimal changes to the FTP clients that send the files = AWS Transfer Family.
Process incoming data files as soon as possible = S3 event notification.
Processing for each file needs to take 3-8 minutes = AWS Lambda function.
Delete file after processing = AWS Lambda function.
upvoted 2 times

✉ **antropaws** 5 months, 1 week ago

Selected Answer: D

Most likely D.
upvoted 1 times

 **r3mo** 5 months, 2 weeks ago

"D" Since each file takes 3-8 minutes to process the lambda function can process the data file without a problem.
upvoted 1 times

 **maver144** 5 months, 2 weeks ago

Selected Answer: D

You cannot setup AWS Transfer Family to save files into EBS.
upvoted 3 times

 **oras2023** 5 months, 2 weeks ago

<https://aws.amazon.com/aws-transfer-family/>
upvoted 1 times

 **secdgs** 5 months, 2 weeks ago

Selected Answer: D

D. Because
1. process immediate when file transfer to S3 not wait for process several file in one time.
2. takes 3-8 can use Lamda.

C. Wrong because AWS Batch is use for run large-scale or large amount of data in one time.
upvoted 1 times

 **Aymanovitchy** 5 months, 3 weeks ago

To meet the requirements of processing incoming data files as soon as possible with minimal changes to the FTP clients, and deleting the files after successful processing, the most operationally efficient solution would be:

D. Use AWS Transfer Family to create an FTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and delete them after processing. Use an S3 event notification to invoke the Lambda function when the files arrive.

upvoted 1 times

 **bajwa360** 5 months, 3 weeks ago

Selected Answer: D

It should be D as lambda is more operationally viable solution given the fact each processing takes 3-8 minutes that lambda can handle
upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: C

Answer has to be between C or D.
Because Transfer Family is obvious do to FTP.
Now i would go with C because it uses AWS Batch, which makes more sense for Batch processing rather than AWS Lambda.
upvoted 1 times

 **Bill1000** 5 months, 3 weeks ago

I am between C and D. My reason is:

"The company wants the AWS solution to process incoming data files **< b>as soon as possible** with minimal changes to the FTP clients that send the files."

upvoted 2 times

A company is migrating its workloads to AWS. The company has transactional and sensitive data in its databases. The company wants to use AWS Cloud solutions to increase security and reduce operational overhead for the databases.

Which solution will meet these requirements?

- A. Migrate the databases to Amazon EC2. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.
- B. Migrate the databases to Amazon RDS Configure encryption at rest.
- C. Migrate the data to Amazon S3 Use Amazon Macie for data security and protection
- D. Migrate the database to Amazon RDS. Use Amazon CloudWatch Logs for data security and protection.

Correct Answer: A

Community vote distribution

B (100%)

 **AshishRocks** Highly Voted 5 months, 3 weeks ago

B is the answer

Why not C - Option C suggests migrating the data to Amazon S3 and using Amazon Macie for data security and protection. While Amazon Macie provides advanced security features for data in S3, it may not be directly applicable or optimized for databases, especially for transactional and sensitive data. Amazon RDS provides a more suitable environment for managing databases.

upvoted 6 times

 **Guru4Cloud** Most Recent 3 months, 1 week ago

Selected Answer: B

Migrate the databases to Amazon RDS Configure encryption at rest.

upvoted 2 times

 **wendaz** 1 month, 2 weeks ago

down voted.

upvoted 1 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: B

Reduce Ops = Migrate the databases to Amazon RDS Configure encryption at rest

upvoted 2 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: B

B for sure.

First the correct is Amazon RDS, then encryption at rest makes the database secure.

upvoted 2 times

 **oras2023** 5 months, 3 weeks ago

Selected Answer: B

B. Migrate the databases to Amazon RDS Configure encryption at rest.

Looks like best option

upvoted 3 times

A company has an online gaming application that has TCP and UDP multiplayer gaming capabilities. The company uses Amazon Route 53 to point the application traffic to multiple Network Load Balancers (NLBs) in different AWS Regions. The company needs to improve application performance and decrease latency for the online game in preparation for user growth.

Which solution will meet these requirements?

- A. Add an Amazon CloudFront distribution in front of the NLBs. Increase the Cache-Control max-age parameter.
- B. Replace the NLBs with Application Load Balancers (ALBs). Configure Route 53 to use latency-based routing.
- C. Add AWS Global Accelerator in front of the NLBs. Configure a Global Accelerator endpoint to use the correct listener ports.
- D. Add an Amazon API Gateway endpoint behind the NLBs. Enable API caching. Override method caching for the different stages.

Correct Answer: D

Community vote distribution

C (100%)

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

The key considerations are:

The application uses TCP and UDP for multiplayer gaming, so Network Load Balancers (NLBs) are appropriate. AWS Global Accelerator can be added in front of the NLBs to improve performance and reduce latency by intelligently routing traffic across AWS Regions and Availability Zones.

Global Accelerator provides static anycast IP addresses that act as a fixed entry point to application endpoints in the optimal AWS location. This improves availability and reduces latency.

The Global Accelerator endpoint can be configured with the correct NLB listener ports for TCP and UDP.

upvoted 2 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: C

TCP ,UDP, Gaming = global accelerator and Network Load Balancer

upvoted 3 times

 **Henrytm1** 5 months, 2 weeks ago

Selected Answer: C

only b and c handle TCP/UDP, and C comes with accelerator to enhance performance

upvoted 1 times

 **manuh** 5 months ago

Does alb handle udp? Can u share a source?

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: C

UDP and TCP is AWS Global accelerator as it works in the Transportation layer.

Now this with NLB is perfect.

upvoted 2 times

 **oras2023** 5 months, 3 weeks ago

Selected Answer: C

C is helping to reduce latency for end clients

upvoted 2 times

A company needs to integrate with a third-party data feed. The data feed sends a webhook to notify an external service when new data is ready for consumption. A developer wrote an AWS Lambda function to retrieve data when the company receives a webhook callback. The developer must make the Lambda function available for the third party to call.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Create a function URL for the Lambda function. Provide the Lambda function URL to the third party for the webhook.
- B. Deploy an Application Load Balancer (ALB) in front of the Lambda function. Provide the ALB URL to the third party for the webhook.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Attach the topic to the Lambda function. Provide the public hostname of the SNS topic to the third party for the webhook.
- D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Attach the queue to the Lambda function. Provide the public hostname of the SQS queue to the third party for the webhook.

Correct Answer: B

Community vote distribution

A (100%)

✉  **TariqKipkemei** Highly Voted 4 months, 1 week ago

Selected Answer: A

A function URL is a dedicated HTTP(S) endpoint for your Lambda function. When you create a function URL, Lambda automatically generates a unique URL endpoint for you.

upvoted 5 times

✉  **Orit** Most Recent 6 days, 18 hours ago

B is the answerThe best solution to make the Lambda function available for the third party to call with the MOST operational efficiency is to deploy an Application Load Balancer (ALB) in front of the Lambda function and provide the ALB URL to the third party for the webhook. This solution is the most efficient because it allows the third party to call the Lambda function without having to worry about managing the Lambda function's availability or scaling. The ALB will automatically distribute traffic across multiple Lambda functions, if necessary, and will also provide redundancy in case of a failure.

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

The key points:

A Lambda function needs to be invoked by a third party via a webhook.

Using a function URL provides a direct invoke endpoint for the Lambda function. This is simple and efficient.

Options B, C, and D insert unnecessary components like ALB, SNS, SQS between the webhook and the Lambda function. These add complexity without benefit.

A function URL can be generated and provided to the third party quickly without additional infrastructure.

upvoted 3 times

✉  **james2033** 4 months, 1 week ago

Selected Answer: A

Keyword "Lambda function" and "webhook". See <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-saas-furls.html#create-stripe-cfn-stack>

upvoted 2 times

✉  **Abrar2022** 5 months, 2 weeks ago

Selected Answer: A

key word: Lambda function URLs

upvoted 1 times

✉  **maver144** 5 months, 2 weeks ago

Selected Answer: A

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

upvoted 1 times

✉  **jkhan2405** 5 months, 2 weeks ago

Selected Answer: A

It's A

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: A

A would seem like the correct one but not sure.

upvoted 1 times

A company has a workload in an AWS Region. Customers connect to and access the workload by using an Amazon API Gateway REST API. The company uses Amazon Route 53 as its DNS provider. The company wants to provide individual and secure URLs for all customers.

Which combination of steps will meet these requirements with the MOST operational efficiency? (Choose three.)

- A. Register the required domain in a registrar. Create a wildcard custom domain name in a Route 53 hosted zone and record in the zone that points to the API Gateway endpoint.
- B. Request a wildcard certificate that matches the domains in AWS Certificate Manager (ACM) in a different Region.
- C. Create hosted zones for each customer as required in Route 53. Create zone records that point to the API Gateway endpoint.
- D. Request a wildcard certificate that matches the custom domain name in AWS Certificate Manager (ACM) in the same Region.
- E. Create multiple API endpoints for each customer in API Gateway.
- F. Create a custom domain name in API Gateway for the REST API. Import the certificate from AWS Certificate Manager (ACM).

Correct Answer: CFD

Community vote distribution

ADF (100%)

✉️  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: ADF

The key points:

Using a wildcard domain and certificate avoids managing individual domains/certs per customer. This is more efficient. The domain, hosted zone, and certificate should all be in the same region as the API Gateway REST API for simplicity. Creating multiple API endpoints per customer (Option E) adds complexity and is not required.

Option B and C add unnecessary complexity by separating domains, certificates, and hosted zones.

upvoted 3 times

✉️  **ukivanlamipi** 4 months ago

Selected Answer: ADF

<https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-custom-domains.html>
<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/AboutHZWorkingWith.html>

upvoted 2 times

✉️  **jaydesai8** 4 months, 3 weeks ago

Selected Answer: ADF

ADF - makes sense

upvoted 1 times

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

Step A involves registering the required domain in a registrar and creating a wildcard custom domain name in a Route 53 hosted zone. This allows you to map individual and secure URLs for all customers to your API Gateway endpoints.

Step D is to request a wildcard certificate from AWS Certificate Manager (ACM) that matches the custom domain name you created in Step A. This wildcard certificate will cover all subdomains and ensure secure HTTPS communication.

Step F is to create a custom domain name in API Gateway for your REST API. This allows you to associate the custom domain name with your API Gateway endpoints and import the certificate from ACM for secure communication.

upvoted 2 times

✉️  **jkhan2405** 5 months, 2 weeks ago

Selected Answer: ADF

It's ADF

upvoted 2 times

✉️  **MAMADOU** 5 months, 3 weeks ago

For me AFD

upvoted 1 times

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

Selected Answer: ADF

ADF - One to create the custom domain in Route 53 (Amazon DNS)
Second to request wildcard certificate from ADM

Thirds to import the certificate from ACM.

upvoted 2 times

 **AncaZalog** 5 months, 3 weeks ago

is ADF

upvoted 1 times

A company stores data in Amazon S3. According to regulations, the data must not contain personally identifiable information (PII). The company recently discovered that S3 buckets have some objects that contain PII. The company needs to automatically detect PII in S3 buckets and to notify the company's security team.

Which solution will meet these requirements?

- A. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData event type from Macie findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- B. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- C. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData:S3Object/Personal event type from Macie findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.
- D. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.

Correct Answer: C

Community vote distribution

A (74%) C (26%)

✉  **alexandercamachop** Highly Voted 5 months, 3 weeks ago

Selected Answer: A

B and D are discarded as Macie is to identify PII.
Now that we have between A and C.
SNS is more suitable for this option as a pub/sub service, we subscribe the security team and then they will receive the notifications.
upvoted 9 times

✉  **potomac** Most Recent 3 weeks, 1 day ago

Selected Answer: A

C is SQS, not SNS
upvoted 1 times

✉  **Wayne23Fang** 3 months ago

SQS mentioned in C.
upvoted 1 times

✉  **Ale1973** 3 months, 3 weeks ago

Selected Answer: A

Amazon SQS is typically used for decoupling and managing messages between distributed application components. It's not typically used for sending notifications directly to humans. On my opinion C isn't a best practice
upvoted 1 times

✉  **Kp88** 4 months ago

Those who say C , please read carefully (I made the same mistake lol). Teams can't be notified with SQS hence A.
upvoted 1 times

✉  **ukivanlamipi** 4 months ago

Selected Answer: C

there are different type of sensitive data: <https://docs.aws.amazon.com/macie/latest/user/findings-types.html>. if the question only focus on PII, then C is the answer. however, in reality, you will use A, because you will not want bank card, credential...etc all sensitive data , not only PII
upvoted 3 times

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

Selected Answer: A

Automatically detect PII in S3 buckets = Amazon Macie
Notify security team = Amazon SNS
Trigger notification based on SensitiveData event type from Macie findings = EventBridge
upvoted 1 times

✉  **NASHDBA** 4 months, 3 weeks ago

Selected Answer: C

There are different types of Sensitive Data. Here we are only referring to PII. Hence SensitiveData:S3Object/Personal. to use SNS, the security team must subscribe. SQS sends the information as designed

upvoted 1 times

✉ **narddrer** 4 months, 3 weeks ago

Selected Answer: C

SensitiveData:S3Object/Personal

upvoted 1 times

✉ **jaydesai8** 4 months, 3 weeks ago

Selected Answer: A

Sensitive = MACIE, and SNS to sent notification to the Security Team

upvoted 2 times

✉ **Iragmt** 4 months, 3 weeks ago

C. Because the question mentioned PII only, there are other Sensitive Data aside from PII.

reference: <https://docs.aws.amazon.com/macie/latest/user/findings-publish-event-schemas.html> look for Event example for a sensitive data finding

upvoted 2 times

✉ **Ale1973** 3 months, 3 weeks ago

But Amazon SQS is typically used for decoupling and managing messages between distributed application components. It's not typically used for sending notifications directly to humans!

upvoted 2 times

✉ **kapit** 5 months, 1 week ago

AAAAAAA

upvoted 1 times

✉ **jack79** 5 months, 2 weeks ago

C <https://docs.aws.amazon.com/macie/latest/user/findings-types.html>

and notice the ensitiveData:S3Object/Personal

The object contains personally identifiable information (such as mailing addresses or driver's license identification numbers), personal health information (such as health insurance or medical identification numbers), or a combination of the two.

upvoted 3 times

✉ **Ale1973** 3 months, 3 weeks ago

But Amazon SQS is typically used for decoupling and managing messages between distributed application components. It's not typically used for sending notifications directly to humans!

upvoted 1 times

✉ **MAMADOU** 5 months, 3 weeks ago

I vote for A, Sensitive = MACIE, and SNS to prevent Security Team

upvoted 3 times

A company wants to build a logging solution for its multiple AWS accounts. The company currently stores the logs from all accounts in a centralized account. The company has created an Amazon S3 bucket in the centralized account to store the VPC flow logs and AWS CloudTrail logs. All logs must be highly available for 30 days for frequent analysis, retained for an additional 60 days for backup purposes, and deleted 90 days after creation.

Which solution will meet these requirements MOST cost-effectively?

- A. Transition objects to the S3 Standard storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
- B. Transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
- C. Transition objects to the S3 Glacier Flexible Retrieval storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
- D. Transition objects to the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.

Correct Answer: B

Community vote distribution

C (57%)	A (35%)	9%
---------	---------	----

✉️  **alexandercamachop** Highly Voted 5 months, 3 weeks ago

Selected Answer: C

C seems the most suitable.
Is the lowest cost.
After 30 days is backup only, doesn't specify frequent access.
Therefor we must transition the items after 30 days to Glacier Flexible Retrieval.

Also it says deletion after 90 days, so all answers specifying a transition after 90 days makes no sense.
upvoted 9 times

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

Agree with you
upvoted 2 times

✉️  **deechean** Highly Voted 2 months, 4 weeks ago

Selected Answer: A

The Glacier min storage duration is 90 days. All the options using Glacier are wrong. Only A is feasible.
upvoted 6 times

✉️  **daniel33** 2 months ago

S3 Standard is priced at \$0.023 per GB for the first 50 TB stored per month
S3 Glacier Flexible Retrieval costs \$0.0036 per GB stored per month
If you move or delete data in Glacier within 90-days since their creation, you will pay an additional charge, that is called an early deletion fee. In US East you will pay \$0.004/GB if you have deleted 1 GB in 2 months, \$0.008/GB if you have deleted 1 GB in 1 month and \$0.012 if you have deleted 1 GB within 3 months.

Even with the early deletion fee, it appears to me that answer 'A' would still be cheaper.
upvoted 2 times

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

Selected Answer: C

C is most cost-effective
upvoted 1 times

✉️  **Hades2231** 3 months ago

Selected Answer: C

Things to note are: 30 days frequent access and 90 days after creation, so you only need to do 2 things, not 3. Objects in S3 will be stored by default for 30 days before you can move it to somewhere else, so C is the answer.

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

upvoted 1 times

✉️  **rjbihari** 3 months ago

C is the correct one .

As after 30 days it doesn't says about access / retrieval , only backup so move items after 30 days to Glacier Flexible Retrieval. And after it says deletion , so expiration action will ensure that the objects are deleted after 90 days, even if they are not accessed upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

I think - it is B

The first 30 days, the logs need to be highly available for frequent analysis. The S3 Standard storage class is the most expensive storage class, but it also provides the highest availability.

After 30 days, the logs still need to be retained for backup purposes, but they do not need to be accessed frequently. The S3 Standard-IA storage class is a good option for this, as it is less expensive than the S3 Standard storage class.

After 90 days, the logs can be moved to the S3 Glacier Flexible Retrieval storage class. This is the most cost-effective storage class for long-term archiving.

The expiration action will ensure that the objects are deleted after 90 days, even if they are not accessed

upvoted 1 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: C

C is the most cost effective solution.

upvoted 1 times

 **antropaws** 5 months, 1 week ago

Selected Answer: C

C most likely.

upvoted 1 times

 **y0eri** 5 months, 2 weeks ago

Selected Answer: A

Question says "All logs must be highly available for 30 days for frequent analysis" I think the answer is A. Glacier is not made for frequent access.

upvoted 2 times

 **y0eri** 5 months, 2 weeks ago

I take that back. Moderator, please delete my comment.

upvoted 4 times

 **KMohsoe** 5 months, 2 weeks ago

Selected Answer: B

I think B

upvoted 1 times

A company is building an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for its workloads. All secrets that are stored in Amazon EKS must be encrypted in the Kubernetes etcd key-value store.

Which solution will meet these requirements?

- A. Create a new AWS Key Management Service (AWS KMS) key. Use AWS Secrets Manager to manage, rotate, and store all secrets in Amazon EKS.
- B. Create a new AWS Key Management Service (AWS KMS) key. Enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster.
- C. Create the Amazon EKS cluster with default options. Use the Amazon Elastic Block Store (Amazon EBS) Container Storage Interface (CSI) driver as an add-on.
- D. Create a new AWS Key Management Service (AWS KMS) key with the alias/aws/ebs alias. Enable default Amazon Elastic Block Store (Amazon EBS) volume encryption for the account.

Correct Answer: D

Community vote distribution

B (92%)	8%
---------	----

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

B is the correct solution to meet the requirement of encrypting secrets in the etcd store for an Amazon EKS cluster.

The key points:

Create a new KMS key to use for encryption.

Enable EKS secrets encryption using that KMS key on the EKS cluster. This will encrypt secrets in the Kubernetes etcd store.

Option A uses Secrets Manager which does not encrypt the etcd store.

Option C uses EBS CSI which is unrelated to etcd encryption.

Option D enables EBS encryption but does not address etcd encryption.

upvoted 2 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: B

EKS supports using AWS KMS keys to provide envelope encryption of Kubernetes secrets stored in EKS. Envelope encryption adds an additional, customer-managed layer of encryption for application secrets or user data that is stored within a Kubernetes cluster.

<https://eksctl.io/usage/kms-encryption/>

upvoted 3 times

 **manuh** 5 months ago

Selected Answer: A

Why not a

upvoted 1 times

 **TariqKipkemei** 4 months, 1 week ago

option A does not enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: B

B is the right option.

<https://docs.aws.amazon.com/eks/latest/userguide/enable-kms.html>

upvoted 4 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: B

It is B, because we need to encrypt inside of the EKS cluster, not outside.

AWS KMS is to encrypt at rest.

upvoted 3 times

 **AncaZalog** 5 months, 3 weeks ago

is B, not D

upvoted 2 times

A company wants to provide data scientists with near real-time read-only access to the company's production Amazon RDS for PostgreSQL database. The database is currently configured as a Single-AZ database. The data scientists use complex queries that will not affect the production database. The company needs a solution that is highly available.

Which solution will meet these requirements MOST cost-effectively?

- A. Scale the existing production database in a maintenance window to provide enough power for the data scientists.
- B. Change the setup from a Single-AZ to a Multi-AZ instance deployment with a larger secondary standby instance. Provide the data scientists access to the secondary instance.
- C. Change the setup from a Single-AZ to a Multi-AZ instance deployment. Provide two additional read replicas for the data scientists.
- D. Change the setup from a Single-AZ to a Multi-AZ cluster deployment with two readable standby instances. Provide read endpoints to the data scientists.

Correct Answer: C

Community vote distribution

D (77%)	C (17%)	7%
---------	---------	----

✉  **NASHDBA** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

Highly Available = Multi-AZ Cluster
 Read-only + Near Real time = readable standby.
 Read replicas are async whereas readable standby is synchronous.
<https://stackoverflow.com/questions/70663036/differences-b-w-aws-read-replica-and-the-standby-instances>
 upvoted 11 times

✉  **Smart** 3 months ago

This^ is the reason.
 upvoted 2 times

✉  **maver144** Highly Voted 5 months, 2 weeks ago

It's either C or D. To be honest, I find the newest questions to be ridiculously hard (roughly 500+). I agree with @alexandercamachop that Multi Az in Instance mode is cheaper than Cluster. However, with Cluster we have reader endpoint available to use out-of-box, so there is no need to provide read-replicas, which also has its own costs. The ridiculous part is that I'm pretty sure even the AWS support would have troubles to answer which configuration is MOST cost-effective.

upvoted 8 times

✉  **manuh** 5 months ago

Absolutely true that 500+ questions are damn difficult to answer. I still dont know why is B incorrect. Shouldn't 1 extra be better than 2 ?
 upvoted 1 times

✉  **maver144** 5 months, 2 weeks ago

Near real-time is clue for C, since read replicas are async, but still its not obvious question.
 upvoted 2 times

✉  **bogobob** Most Recent 1 week, 5 days ago

Selected Answer: D

<https://aws.amazon.com/blogs/database/choose-the-right-amazon-rds-deployment-option-single-az-instance-multi-az-instance-or-multi-az-database-cluster/>
 C would mean you are paying for 4 instances (primary, backup, and 2 read instances). D would be 3 (primary, and 2 backup). Difficult to be sure, pricing calculator doesn't even include clusters yet.
 upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: D

Option D is the most cost-effective solution that meets the requirements for this scenario.

The key considerations are:

Data scientists need read-only access to near real-time production data without affecting performance.
 High availability is required.
 Cost should be minimized.
 upvoted 1 times

✉  **ukivanlamipi** 4 months ago

Selected Answer: D

<https://aws.amazon.com/blogs/database/choose-the-right-amazon-rds-deployment-option-single-az-instance-multi-az-instance-or-multi-az-database-cluster/>

only multi AZ cluster have reader endpoint. multi AZ instance secondary replicate is not allow to access
upvoted 1 times

msdnpro 4 months ago

Selected Answer: D

Support for D:

Amazon RDS now offers Multi-AZ deployments with readable standby instances (also called Multi-AZ DB cluster deployments) in preview. You should consider using Multi-AZ DB cluster deployments with two readable DB instances if you need additional read capacity in your Amazon RDS Multi-AZ deployment and if your application workload has strict transaction latency requirements such as single-digit milliseconds transactions.

<https://aws.amazon.com/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/>
upvoted 1 times

TariqKipkemei 4 months, 1 week ago

Selected Answer: D

Unlike Multi-AZ instance deployment, where the secondary instance can't be accessed for read or writes, Multi-AZ DB cluster deployment consists of primary instance running in one AZ serving read-write traffic and two other standby running in two different AZs serving read traffic.
upvoted 2 times

Iragmt 4 months, 3 weeks ago

Selected Answer: D

D. using Multi-AZ DB cluster deployments with two readable DB instances if you need additional read capacity in your Amazon RDS Multi-AZ deployment and if your application workload has strict transaction latency requirements such as single-digit milliseconds transactions.
<https://aws.amazon.com/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/>

while on read replicas, Amazon RDS then uses the asynchronous replication method for the DB engine to update the read replica whenever there is a change to the primary DB instance. https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html
upvoted 1 times

manuh 5 months ago

Selected Answer: B

Why not b. Shouldnt it have less number of instances than both c and d?
upvoted 2 times

baba365 4 months, 2 weeks ago

Multi-AZ is about twice the price of Single-AZ. For example:
db.t2.micro single - \$0.017/hour
db.t2.micro multi - \$0.034/hour

option C: 1 primary + 1 standby + 2 replica = 4Db
option D: 1 primary + 2 standby = 3Db

D. appears to be most cost effective
upvoted 2 times

wsdasdasdqwdaw 1 month ago

I think the best explanation I've read so far.
upvoted 1 times

baba365 4 months, 2 weeks ago

Complex queries on single db will affect performance of db
upvoted 1 times

0628atv 5 months ago

D:
<https://aws.amazon.com/tw/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/>
upvoted 1 times

vrevkov 5 months, 1 week ago

Selected Answer: D

Forgot to vote
upvoted 2 times

vrevkov 5 months, 1 week ago

I think it's D.
C: Multi-AZ instance = active + standby + two read replicas = 4 RDS instances
D: Multi-AZ cluster = Active + two standby = 3 RDS instances

Single-AZ and Multi-AZ deployments: Pricing is billed per DB instance-hour consumed from the time a DB instance is launched until it is stopped or deleted.

<https://aws.amazon.com/rds/postgresql/pricing/?pg=pr&loc=3>

In the case of a cluster, you will pay less.

upvoted 2 times

 **Axeashes** 5 months, 2 weeks ago

Selected Answer: D

Multi-AZ instance: the standby instance doesn't serve any read or write traffic.

Multi-AZ DB cluster: consists of primary instance running in one AZ serving read-write traffic and two other standby running in two different AZs serving read traffic.

<https://aws.amazon.com/blogs/database/choose-the-right-amazon-rds-deployment-option-single-az-instance-multi-az-instance-or-multi-az-database-cluster/>

upvoted 3 times

 **oras2023** 5 months, 2 weeks ago

Selected Answer: C

It looks like another question about Multi-AZ cluster/instance deployment, but in this case we no need 40 sec failover so no reasons to look at cluster and buy more resources than we need.

We provide datascience team 2 read replica for their queries.

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: C

C.

The question says highly available therefor Multi Az deployment.

Also mentions cost consideration. database instance is cheaper then cluster (D).

Also read replicas is a must since the queries are complex and can slow down the database (question has not complex queries but is a mistake must have been complex queries)

upvoted 4 times

A company runs a three-tier web application in the AWS Cloud that operates across three Availability Zones. The application architecture has an Application Load Balancer, an Amazon EC2 web server that hosts user session states, and a MySQL database that runs on an EC2 instance. The company expects sudden increases in application traffic. The company wants to be able to scale to meet future application capacity demands and to ensure high availability across all three Availability Zones.

Which solution will meet these requirements?

- A. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.
- B. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Memcached with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.
- C. Migrate the MySQL database to Amazon DynamoDB Use DynamoDB Accelerator (DAX) to cache reads. Store the session data in DynamoDB. Migrate the web server to an Auto Scaling group that is in three Availability Zones.
- D. Migrate the MySQL database to Amazon RDS for MySQL in a single Availability Zone. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

Correct Answer: B

Community vote distribution

A (68%)

B (32%)

✉  **alexandercamachop** Highly Voted 5 months, 3 weeks ago

Selected Answer: A

Memcached is best suited for caching data, while Redis is better for storing data that needs to be persisted. If you need to store data that needs to be accessed frequently, such as user profiles, session data, and application settings, then Redis is the better choice
upvoted 10 times

✉  **nonameforyou** 5 months ago

and for high availability, it's better than memcached
upvoted 1 times

✉  **nonameforyou** 5 months ago

but does rds multi-az provide the needed scalability?
upvoted 1 times

✉  **wsdasdasdqwdaw** 1 month ago

it is multi-az cluster deployment, same as B, so yes, it is providing the needed scalability. Great explanation.
upvoted 1 times

✉  **potomac** Most Recent 3 weeks, 1 day ago

Selected Answer: A

Redis is a widely adopted in-memory data store for use as a database, cache, message broker, queue, session store, and leaderboard.
<https://aws.amazon.com/elasticache/redis/>
upvoted 2 times

✉  **thanhnv142** 1 month ago

B is correct.
We are left with 2 options: A and B. But it requires that the system be able to scale to meet future application capacity demands. Redis is very good. But its drawback is not scalable. That's why they implement memcached.
upvoted 1 times

✉  **ErnShm** 2 months, 2 weeks ago

A
Redis as an in-memory data store with high availability and persistence is a popular choice among application developers to store and manage session data for internet-scale applications. Redis provides the sub-millisecond latency, scale, and resiliency required to manage session data such as user profiles, credentials, session state, and user-specific personalization.
upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

The key reasons why option A is preferable:

RDS Multi-AZ provides high availability for MySQL by synchronously replicating data across AZs. Automatic failover handles AZ outages. ElastiCache for Redis is better suited for session data caching than Memcached. Redis offers more advanced data structures and flexibility. Auto scaling across 3 AZs provides high availability for the web tier

upvoted 1 times

 **ukivanlampli** 4 months ago

Selected Answer: B

the difference between Redis and Memcache is that Memcache supports multithreaded process to handle the increase of application traffic.
<https://aws.amazon.com/elasticsearch/redis-vs-memcached/>

upvoted 2 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: B

This requirement wins for me: "be able to scale to meet future application capacity demands".
Memcached implements a multi-threaded architecture, it can make use of multiple processing cores. This means that you can handle more operations by scaling up compute capacity.

<https://aws.amazon.com/elasticsearch/redis-vs-memcached/#:~:text=by%20their%20rank.-,Multithreaded%20architecture,-Since%20Memcached%20is>

upvoted 1 times

 **plndmns** 4 months, 2 weeks ago

cache reads is memcached right?

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: B

B is correct!

upvoted 3 times

 **AncaZalog** 5 months, 3 weeks ago

is A not B

upvoted 4 times

A global video streaming company uses Amazon CloudFront as a content distribution network (CDN). The company wants to roll out content in a phased manner across multiple countries. The company needs to ensure that viewers who are outside the countries to which the company rolls out content are not able to view the content.

Which solution will meet these requirements?

- A. Add geographic restrictions to the content in CloudFront by using an allow list. Set up a custom error message.
- B. Set up a new URL for restricted content. Authorize access by using a signed URL and cookies. Set up a custom error message.
- C. Encrypt the data for the content that the company distributes. Set up a custom error message.
- D. Create a new URL for restricted content. Set up a time-restricted access policy for signed URLs.

Correct Answer: A

Community vote distribution

A (100%)

 **potomac** 3 weeks, 1 day ago

Selected Answer: A

The CloudFront geographic restrictions feature lets you control distribution of your content at the country level for all files that you're distributing with a given web distribution.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>

upvoted 2 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

Add geographic restrictions to the content in CloudFront by using an allow list. Set up a custom error message

upvoted 1 times

 **TariqKipkemei** 4 months, 1 week ago

Selected Answer: A

Add geographic restrictions to the content in CloudFront by using an allow list. Set up a custom error message.

upvoted 1 times

 **jaydesai8** 4 months, 2 weeks ago

Selected Answer: A

A makes sense - cloudfront has the capabilities of georestriction

upvoted 1 times

 **antropaws** 5 months, 1 week ago

Selected Answer: A

Pretty sure it's A.

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>

upvoted 4 times

 **AncaZalog** 5 months, 3 weeks ago

is B not A

upvoted 1 times

 **manuh** 5 months ago

Signed url or cookies can be used for the banner country as well?

upvoted 1 times

 **antropaws** 5 months, 1 week ago

Why's that?

upvoted 1 times

A company wants to use the AWS Cloud to improve its on-premises disaster recovery (DR) configuration. The company's core production business application uses Microsoft SQL Server Standard, which runs on a virtual machine (VM). The application has a recovery point objective (RPO) of 30 seconds or fewer and a recovery time objective (RTO) of 60 minutes. The DR solution needs to minimize costs wherever possible.

Which solution will meet these requirements?

- A. Configure a multi-site active/active setup between the on-premises server and AWS by using Microsoft SQL Server Enterprise with Always On availability groups.
- B. Configure a warm standby Amazon RDS for SQL Server database on AWS. Configure AWS Database Migration Service (AWS DMS) to use change data capture (CDC).
- C. Use AWS Elastic Disaster Recovery configured to replicate disk changes to AWS as a pilot light.
- D. Use third-party backup software to capture backups every night. Store a secondary set of backups in Amazon S3.

Correct Answer: D

Community vote distribution

B (67%)

C (33%)

 **potomac** 3 weeks, 1 day ago

Selected Answer: B

With the pilot light approach, you replicate your data from one environment to another and provision a copy of your core workload infrastructure, not the fully functional copy of your production environment in a recovery environment.

upvoted 1 times

 **thanhnv142** 1 month ago

C: Pilot light
- In pilot light, databases are always on, thus minimize RPO (can satisfy the 30s requirement)
- Only apps are turn off. But it can satisfy the 60 minutes requirement
- Warm standby, of course, can satisfy all the RPO and RTO requirements, but it is more expensive than pilot light

upvoted 3 times

 **richguo** 2 months, 1 week ago

Selected Answer: C

B(warm standby) is doable, but C (pilot light) is most cost effectively.
<https://aws.amazon.com/tw/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/>
upvoted 1 times

 **LazyTs** 2 months, 3 weeks ago

Selected Answer: B

The company wants to improve... so needs something guaranteed to be better than 60 mins RTO
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Configure a warm standby Amazon RDS for SQL Server database on AWS. Configure AWS Database Migration Service (AWS DMS) to use change data capture (CDC).
upvoted 1 times

 **Eminenza22** 3 months, 1 week ago

Warm standby is costlier than Pilot Light
upvoted 1 times

 **PantryRaid** 3 months, 1 week ago

Selected Answer: C

AWS DRS enables RPOs of seconds and RTOs of minutes. Pilot light is also cheaper than warm standby.
<https://aws.amazon.com/disaster-recovery/>
upvoted 2 times

 **BlueAIBird** 3 months, 4 weeks ago

C is correct.
Since it is not only your core elements that are running all the time, warm standby is usually more costly than pilot light. Warm standby is another example of active/passive failover configuration. Servers can be left running in a minimum number of EC2 instances on the smallest sizes possible.
Ref: <https://tutorialsdojo.com/backup-and-restore-vs-pilot-light-vs-warm-standby-vs-multi-site/#:~:text=Since%20it%20is%20not%20only,on%20the%20smallest%20sizes%20possible.>

upvoted 1 times

✉ **hozy_** 4 months, 1 week ago

Selected Answer: C

<https://aws.amazon.com/ko/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/>

It says Pilot Light costs less than Warm Standby.

upvoted 1 times

✉ **narddrer** 4 months, 3 weeks ago

Selected Answer: B

https://stepstocloud.com/change-data-capture/?expand_article=1

upvoted 1 times

✉ **darekw** 2 months, 3 weeks ago

Based on this link Change Data Capture (CDC) in AWS is a mechanism for tracking changes to data in DynamoDB tables. And the question refers to Microsoft SQL Server Standard

upvoted 1 times

✉ **darekw** 2 months, 3 weeks ago

ok, it's also for SQL servers:

SQL Server Change Data Capture (CDC) is a feature that enables you to capture insert, update, and delete activity on a SQL Server table,

upvoted 1 times

✉ **Zox42** 4 months, 3 weeks ago

Selected Answer: C

Answer C. RPO is in seconds and RTO 5-20 min; pilot light costs less than warm standby (and of course less than active-active).

<https://docs.aws.amazon.com/drs/latest/userguide/failback-overview.html#recovery-objectives>

upvoted 1 times

✉ **haoAWS** 5 months ago

Selected Answer: B

The answer should be B. ACD cannot make the RPO for only 30 seconds.

upvoted 1 times

✉ **haoAWS** 5 months ago

Sorry for mistake, A can also make RPO very low, but A is more expensive than B.

upvoted 1 times

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

Selected Answer: B

I guess this question requires two answers. I think the answers would be both B & D.

upvoted 1 times

✉ **haoAWS** 5 months ago

D does not make sense since RPO is 30 seconds, back up every night is too long.

upvoted 1 times

✉ **Abrar2022** 5 months, 2 weeks ago

Selected Answer: B

Keyword: change data capture (CDC).

upvoted 1 times

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

Selected Answer: B

B is the correct one.

C and D are discarded as makes no sense.

Between A and B is because B is RDS which is a managed service, we can use even to pay only for used resources when needed. Leveraging AWS DMS it replicates / syncs the data.

upvoted 3 times

✉ **maver144** 5 months, 2 weeks ago

C makes sense.

However using AWS Elastic Disaster Recovery configured to replicate disk changes is more likely to be backup & restore than pilot light.

upvoted 1 times

✉ **Bill1000** 5 months, 3 weeks ago

Why 'D'? Can someone explain?

How can 'D' meet the 30s RPO?

upvoted 1 times

A company has an on-premises server that uses an Oracle database to process and store customer information. The company wants to use an AWS database service to achieve higher availability and to improve application performance. The company also wants to offload reporting from its primary database system.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Use AWS Database Migration Service (AWS DMS) to create an Amazon RDS DB instance in multiple AWS Regions. Point the reporting functions toward a separate DB instance from the primary DB instance.
- B. Use Amazon RDS in a Single-AZ deployment to create an Oracle database. Create a read replica in the same zone as the primary DB instance. Direct the reporting functions to the read replica.
- C. Use Amazon RDS deployed in a Multi-AZ cluster deployment to create an Oracle database. Direct the reporting functions to use the reader instance in the cluster deployment.
- D. Use Amazon RDS deployed in a Multi-AZ instance deployment to create an Amazon Aurora database. Direct the reporting functions to the reader instances.

Correct Answer: D

Community vote distribution

D (60%)

C (40%)

✉  **mrsoa**  4 months ago

Selected Answer: D

Its D
Multi-AZ DB clusters aren't available with the following engines:
RDS for MariaDB
RDS for Oracle
RDS for SQL Server

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RDS_Fea_Regions_DB-eng.Feature.MultiAZDBClusters.html
upvoted 17 times

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

Selected Answer: C

C. Use Amazon RDS deployed in a Multi-AZ cluster deployment to create an Oracle database. Direct the reporting functions to use the reader instance in the cluster deployment.

A and B discarded.

The answer is between C and D

D says use an Amazon RDS to build an Amazon Aurora, makes no sense.

C is the correct one, high availability in multi az deployment.

Also point the reporting to the reader replica.

upvoted 10 times

✉  **bogobob** 1 week, 5 days ago

using RDS to build Aurora from an Oracle DB <https://aws.amazon.com/tutorials/break-free-from-legacy-databases/migrate-oracle-to-amazon-aurora/>
upvoted 1 times

✉  **EK2k**  2 weeks, 3 days ago

Selected Answer: C

It should be C. Oracle DB is supported in RDS Multi-AZ with one standby for HA. <https://aws.amazon.com/rds/features/multi-az/>. Additionally, a reader instance/replica could be added to RDS Multi-AZ with one standby setup to offload the read requests. Aurora is only supported MySQL and Postgres compatible DB so "D" is out.

upvoted 1 times

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: D

Multi-AZ DB clusters are NOT available with the following engines:
RDS for MariaDB
RDS for Oracle
RDS for SQL Server

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RDS_Fea_Regions_DB-eng.Feature.MultiAZDBClusters.html
upvoted 1 times

 **danielmakita** 1 month ago

It is C. Aurora database doesn't support Oracle.
upvoted 1 times

 **wsdasdasdqwdaw** 1 month ago

You can use Aurora instead of Oracle. There are tutorials how to migrate Oracle to Aurora. On top C is not supported. The is not Multi-AZ DB CLUSTER for Oracle.
upvoted 1 times

 **wsdasdasdqwdaw** 1 month ago

It is D
upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

None options seems valid. Not C because it is not supported. But not D as well. RDS is not Aurora. They are two separate services. Additionally, In multi AZ instance deployment, it only provides fault tolerance, not High avai.
upvoted 1 times

 **Nikki013** 3 months ago

Selected Answer: D

Multi-AZ Cluster does not support Oracle as engine:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RDS_Fea_Regions_DB-eng.Feature.MultiAZDBClusters.html
upvoted 1 times

 **Bennyboy789** 3 months ago

Selected Answer: D

D is my choice.
Multi-AZ DB cluster does not support Oracle DB.
upvoted 2 times

 **rjbihari** 3 months ago

Option C is correct one .
As there is no option for 'Aurora(Oracle Compatible)'.so this kick out D from race.
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

Using RDS Multi-AZ provides high availability and failover capabilities for the primary Oracle database.

The reader instance in the Multi-AZ cluster can be used for offloading reporting workloads from the primary instance. This improves performance.

RDS Multi-AZ has automatic failover between AZs. DMS and Aurora migrations (A, D) would incur more effort and downtime.

Single-AZ with a read replica (B) does not provide the AZ failover capability that Multi-AZ does.
upvoted 1 times

 **ukivanlamipi** 3 months, 2 weeks ago

Selected Answer: D

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html
upvoted 3 times

 **darekw** 3 months, 3 weeks ago

Amazon RDS supports Multi-AZ deployments for Oracle as a high-availability, failover solution.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Oracle.html
upvoted 2 times

 **TariqKipkemei** 4 months ago

Selected Answer: C

So I just tried from the aws console and under engine type there is no option for 'Aurora(Oracle Compatible)'.
This leaves option C as the best answer.
upvoted 3 times

 **jaydesai8** 4 months, 2 weeks ago

Selected Answer: C

Use Amazon RDS deployed in a Multi-AZ instance deployment to create an Amazon Aurora database - RDS with Amazon Aurora is a misleading
upvoted 2 times

 **tld2128** 4 months, 3 weeks ago

I vote C, option D use RDS to create Aurora not make sense
upvoted 1 times

 **Mlytics_SOC** 4 months, 3 weeks ago

C
https://aws.amazon.com/rds/oracle/faqs/?nc1=h_ls

upvoted 1 times

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

Selected Answer: C

Multi AZ RDS for Oracle

<https://aws.amazon.com/blogs/aws/multi-az-option-for-amazon-rds-oracle/>

upvoted 1 times

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

Never mind its D.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/create-multi-az-db-cluster.html>

upvoted 1 times

✉️ **Caes12352** 4 months, 3 weeks ago

pepega

upvoted 1 times

A company wants to build a web application on AWS. Client access requests to the website are not predictable and can be idle for a long time. Only customers who have paid a subscription fee can have the ability to sign in and use the web application.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

- A. Create an AWS Lambda function to retrieve user information from Amazon DynamoDB. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.
- B. Create an Amazon Elastic Container Service (Amazon ECS) service behind an Application Load Balancer to retrieve user information from Amazon RDS. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.
- C. Create an Amazon Cognito user pool to authenticate users.
- D. Create an Amazon Cognito identity pool to authenticate users.
- E. Use AWS Amplify to serve the frontend web content with HTML, CSS, and JS. Use an integrated Amazon CloudFront configuration.
- F. Use Amazon S3 static web hosting with PHP, CSS, and JS. Use Amazon CloudFront to serve the frontend web content.

Correct Answer: ACE

Community vote distribution

ACE (71%)	ACF (18%)	7%
-----------	-----------	----

✉  **manOfThePeople** Highly Voted 2 months, 4 weeks ago

If in doubt between E or F. S3 doesn't support server-side scripts, PHP is a server-side script.

The answer is ACE.

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

upvoted 7 times

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

Selected Answer: ACE

Use exclusion method: No need for Container (no need run all time), remove B. PHP cannot run with static Amazon S3, remove F.

Use selection method: Idle for sometime, choose AWS Lambda, choose A. "Amazon Cognito is an identity platform for web and mobile apps." (<https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html>), choose C. Create an identity pool <https://docs.aws.amazon.com/cognito/latest/developerguide/tutorial-create-identity-pool.html> . AWS Amplify <https://aws.amazon.com/amplify/> for build full-stack web-app in hours.

upvoted 5 times

✉  **potomac** Most Recent 3 weeks, 1 day ago

Selected Answer: ACE

User Pool = authentication

Identity Pool = authorization

upvoted 2 times

✉  **thanhnv142** 1 month, 1 week ago

A D F:

A: for hosting the dynamic content of the app. Pay as execution

D: for granting temporary privilege access to users who has paid a fee.

F: for hosting the static content of the app

upvoted 1 times

✉  **kwang312** 2 months, 1 week ago

Selected Answer: ACE

ACE is correct answer

upvoted 2 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: CEF

C) Create an Amazon Cognito user pool to authenticate users.

E) Use AWS Amplify to serve the frontend web content with HTML, CSS, and JS. Use an integrated CloudFront configuration.

F) Use Amazon S3 static web hosting with PHP, CSS, and JS. Use Amazon CloudFront to serve the frontend web content.

upvoted 1 times

✉  **TariqKipkemei** 4 months ago

Selected Answer: ACE

Build a web application = AWS Amplify
Sign in users = Amazon Cognito user pool
Traffic can be idle for a long time = AWS Lambda

Amazon S3 does not support server-side scripting such as PHP, JSP, or ASP.NET.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html?icmpid=docs_amazons3_console#:~:text=website%20relies%20on,-server%2Dside,-processing%2C%20including%20server
Traffic can be idle for a long time = AWS Lambda
upvoted 1 times

✉ **baba365** 4 months, 2 weeks ago

Ans: ACF

use AWS SDK for PHP/JS with S3

https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/php_s3_code_examples.html
upvoted 1 times

✉ **unbendable** 1 month ago

did you actually read the link or just copy the first link from google here? the sdk is intended for usage in a php application. it does not say anything about php support in a s3 bucket
upvoted 1 times

✉ **Zox42** 4 months, 3 weeks ago

Selected Answer: ACE

Answer is ACE

upvoted 1 times

✉ **jaydesai8** 4 months, 3 weeks ago

Selected Answer: ACE

Lambda =serverless
User Pool = For user authentication
Amplify = hosting web/mobile apps
upvoted 2 times

✉ **live_reply_developers** 5 months ago

Selected Answer: ACE

S3 doesn't support PHP as stated in answer F.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html>
upvoted 1 times

✉ **wRhlH** 5 months ago

Selected Answer: ACE

I don't think S3 can handle anything dynamic such as PHP. So I go for ACE
upvoted 1 times

✉ **msdnpro** 5 months, 1 week ago

Selected Answer: ACE

Option B (Amazon ECS) is not the best option since the website "can be idle for a long time", so Lambda (Option A) is a more cost-effective choice.

Option D is incorrect because User pools are for authentication (identity verification) while Identity pools are for authorization (access control).

Option F is wrong because S3 web hosting only supports static web files like HTML/CSS, and does not support PHP or JavaScript.
upvoted 4 times

✉ **0628atv** 5 months ago

https://aws.amazon.com/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-1/?nc1=h_ls
upvoted 2 times

✉ **antropaws** 5 months, 1 week ago

Selected Answer: ACF

ACF no doubt. Check the difference between user pools and identity pools.
upvoted 2 times

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

Selected Answer: ACE

These are the correct answers !
upvoted 1 times

✉ **bestedeki** 5 months, 2 weeks ago

Selected Answer: ADF

A. serverless
D. identity pools
F. S3 to host static content with CloudFront distribution

upvoted 1 times

 **oras2023** 5 months, 2 weeks ago

Selected Answer: ADF

- A: long idle = server less
- D: authorisation with Identity Pool
- F: S3 for static web content with CloudFront distribution as well based on access patterns to data

upvoted 1 times

 **oras2023** 5 months, 2 weeks ago

ACF:
<https://repost.aws/knowledge-center/cognito-user-pools-identity-pools>

upvoted 2 times

A media company uses an Amazon CloudFront distribution to deliver content over the internet. The company wants only premium customers to have access to the media streams and file content. The company stores all content in an Amazon S3 bucket. The company also delivers content on demand to customers for a specific purpose, such as movie rentals or music downloads.

Which solution will meet these requirements?

- A. Generate and provide S3 signed cookies to premium customers.
- B. Generate and provide CloudFront signed URLs to premium customers.
- C. Use origin access control (OAC) to limit the access of non-premium customers.
- D. Generate and activate field-level encryption to block non-premium customers.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Generate and provide CloudFront signed URLs to premium customers.

upvoted 1 times

 **TariqKipkemei** 4 months ago

Selected Answer: B

Use CloudFront signed URLs or signed cookies to restrict access to documents, business data, media streams, or content that is intended for selected users, for example, users who have paid a fee.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html#:~:text=CloudFront%20signed%20URLs>
upvoted 2 times

 **james2033** 4 months, 2 weeks ago

Selected Answer: B

See <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html#private-content-how-signed-urls-work>

upvoted 1 times

 **haoAWS** 5 months ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>
Notice that A is not correct because it should be CloudFront signed URL, not S3.

upvoted 2 times

 **antropaws** 5 months, 1 week ago

Why not C?

upvoted 1 times

 **antropaws** 5 months, 1 week ago

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-cloudfront-introduces-origin-access-control-oac/>
upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: B

Signed URLs

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>
upvoted 2 times

 **haoAWS** 5 months ago

Then why A is incorrect?

upvoted 1 times

A company runs Amazon EC2 instances in multiple AWS accounts that are individually bled. The company recently purchased a Savings Plan. Because of changes in the company's business requirements, the company has decommissioned a large number of EC2 instances. The company wants to use its Savings Plan discounts on its other AWS accounts.

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

- A. From the AWS Account Management Console of the management account, turn on discount sharing from the billing preferences section.
- B. From the AWS Account Management Console of the account that purchased the existing Savings Plan, turn on discount sharing from the billing preferences section. Include all accounts.
- C. From the AWS Organizations management account, use AWS Resource Access Manager (AWS RAM) to share the Savings Plan with other accounts.
- D. Create an organization in AWS Organizations in a new payer account. Invite the other AWS accounts to join the organization from the management account.
- E. Create an organization in AWS Organizations in the existing AWS account with the existing EC2 instances and Savings Plan. Invite the other AWS accounts to join the organization from the management account.

Correct Answer: AE

Community vote distribution

AE (62%) AD (15%) CE (15%) 8%

✉  **Aigerim2010** [Highly Voted ] 4 months, 3 weeks ago

i had this question today
upvoted 6 times

✉  **ErnShm** [Most Recent ] 2 months, 3 weeks ago

AE
<https://repost.aws/questions/QUQoJuQLNOTDiyEuCLARIBFQ/transfer-savings-plan-across-organizations#:~:text=AWS%20Support%20can%20transfer%20Savings%20Plans%20from%20the%20management%20account%20to%20a%20member%20account%20or%20from%20a%20member%20account%20to%20the%20management%20account%20within%20a%20single%20Organization%20with%20an%20AWS%20Support%20Case.>
upvoted 1 times

✉  **Nikki013** 3 months ago

Selected Answer: AD
It is not recommended to have workload on the management account.
upvoted 1 times

✉  **lemur88** 3 months ago

Selected Answer: AD
Not E - it mentions using an account with existing EC2s as the management account, which goes against the best practice for a management account
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html
upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: AE
AE is best
upvoted 1 times

✉  **TariqKipkemei** 4 months ago

Selected Answer: AE
AE is best
upvoted 1 times

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

Selected Answer: AE
- B is not accepted, because "include all accounts", remove B.
- D has "Create an organization in AWS Organization in a new payer account", it is wrong, remove D.
- at C: AWS Resource Access Manager (AWS RAM) <https://aws.amazon.com/ram/> it is for security, not for billing. Remove C.
Has A, E remain, and choosed.

A. "turn on discount sharing" is ok. This case: Has discount for many EC2 instances in one account, then want to share with other user. At E, create Organization, then share.

upvoted 1 times

 **antropaws** 5 months, 1 week ago

Selected Answer: AE

I vote AE.

upvoted 1 times

 **MrAWSAssociate** 5 months, 1 week ago

Selected Answer: AE

AE are correct !

upvoted 1 times

 **oras2023** 5 months, 2 weeks ago

Selected Answer: CD

It's not good practice to create a payer account with any workload so it must be D.

By the reason that we need Organizations for sharing, then we need to turn on its from our PAYER account. (all sub-accounts start share discounts)

upvoted 1 times

 **oras2023** 5 months, 2 weeks ago

changed to AD

upvoted 3 times

 **maver144** 5 months, 2 weeks ago

Selected Answer: AE

@alexandercamachop it is AE. I believe its just typo. RAM is not needed anyhow.

upvoted 3 times

 **oras2023** 5 months, 2 weeks ago

You are right

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

upvoted 2 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: CE

C & E for sure.

In order to share savings plans, we need an organization.

Create that organization first and then invite everyone to it.

From that console share it other accounts.

upvoted 2 times

A retail company uses a regional Amazon API Gateway API for its public REST APIs. The API Gateway endpoint is a custom domain name that points to an Amazon Route 53 alias record. A solutions architect needs to create a solution that has minimal effects on customers and minimal data loss to release the new version of APIs.

Which solution will meet these requirements?

- A. Create a canary release deployment stage for API Gateway. Deploy the latest API version. Point an appropriate percentage of traffic to the canary stage. After API verification, promote the canary stage to the production stage.
- B. Create a new API Gateway endpoint with a new version of the API in OpenAPI YAML file format. Use the import-to-update operation in merge mode into the API in API Gateway. Deploy the new version of the API to the production stage.
- C. Create a new API Gateway endpoint with a new version of the API in OpenAPI JSON file format. Use the import-to-update operation in overwrite mode into the API in API Gateway. Deploy the new version of the API to the production stage.
- D. Create a new API Gateway endpoint with new versions of the API definitions. Create a custom domain name for the new API Gateway API. Point the Route 53 alias record to the new API Gateway API custom domain name.

Correct Answer: A

Community vote distribution

A (100%)

 **dddww12** Highly Voted 4 months, 2 weeks ago

what are the total number of questions this package has as on 14 July 2023 , is it 544 or 551 ?

upvoted 7 times

 **AudreyNguyenHN** Highly Voted 3 months, 4 weeks ago

We made it all the way here. Good luck everyone!

upvoted 5 times

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

Selected Answer: A

In a canary release deployment, total API traffic is separated at random into a production release and a canary release with a pre-configured ratio. Typically, the canary release receives a small percentage of API traffic and the production release takes up the rest. The updated API features are only visible to API traffic through the canary. You can adjust the canary traffic percentage to optimize test coverage or performance.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/canary-release.html>

upvoted 2 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

Using a canary release deployment allows incremental rollout of the new API version to a percentage of traffic. This minimizes impact on customers and potential data loss during the release.

upvoted 1 times

 **TariqKipkemei** 4 months ago

Selected Answer: A

Minimal effects on customers and minimal data loss = Canary deployment

upvoted 2 times

 **james2033** 4 months, 2 weeks ago

Selected Answer: A

Key word "canary release". See this term in See: <https://www.jetbrains.com/teamcity/ci-cd-guide/concepts/canary-release/> and/or <https://martinfowler.com/bliki/CanaryRelease.html>

upvoted 1 times

 **Abrar2022** 5 months, 2 weeks ago

Selected Answer: A

keyword: "latest versions on an api"

Canary release is a software development strategy in which a "new version of an API" (as well as other software) is deployed for testing purposes.

upvoted 2 times

 **jkhan2405** 5 months, 2 weeks ago

Selected Answer: A

It's A

upvoted 1 times

 **alexandercamachop** 5 months, 3 weeks ago

Selected Answer: A

A. Create a canary release deployment stage for API Gateway. Deploy the latest API version. Point an appropriate percentage of traffic to the canary stage. After API verification, promote the canary stage to the production stage.

Canary release meaning only certain percentage of the users.

upvoted 3 times

A company wants to direct its users to a backup static error page if the company's primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53. The domain is pointing to an Application Load Balancer (ALB). The company needs a solution that minimizes changes and infrastructure overhead.

Which solution will meet these requirements?

- A. Update the Route 53 records to use a latency routing policy. Add a static error page that is hosted in an Amazon S3 bucket to the records so that the traffic is sent to the most responsive endpoints.
- B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page that is hosted in an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- C. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance that hosts a static error page as endpoints. Configure Route 53 to send requests to the instance only if the health checks fail for the ALB.
- D. Update the Route 53 records to use a multivalue answer routing policy. Create a health check. Direct traffic to the website if the health check passes. Direct traffic to a static error page that is hosted in Amazon S3 if the health check does not pass.

Correct Answer: B

Community vote distribution

B (86%) 14%

 **TariqKipkemei** 1 week, 5 days ago

Selected Answer: B

Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page that is hosted in an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.

upvoted 1 times

 **ssa03** 2 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 3 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: D

Setting up a Route 53 active-passive failover configuration with the ALB as the primary endpoint and an Amazon S3 static website as the passive endpoint meets the requirements with minimal overhead.

Route 53 health checks can monitor the ALB health. If the ALB becomes unhealthy, traffic will automatically failover to the S3 static website. This provides automatic failover with minimal configuration changes

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Sorry. I mean B

upvoted 2 times

 **Nirav1112** 3 months, 3 weeks ago

B is correct

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: B

B seems correct

upvoted 2 times

 **Bmaster** 3 months, 4 weeks ago

B is correct..

<https://repost.aws/knowledge-center/fail-over-s3-r53>

upvoted 1 times

A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.

What should a solutions architect recommend?

- A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
- B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.
- C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.
- D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Correct Answer: D

Community vote distribution

D (100%)

 **TariqKipkemei** 1 week, 5 days ago

Selected Answer: D

Use Tape Gateway to replace physical tapes on premises with virtual tapes on AWS—reducing your data storage costs without changing your tape-based backup workflows. Tape Gateway supports all leading backup applications and caches virtual tapes on premises for low-latency data access. It compresses your tape data, encrypts it, and stores it in a virtual tape library in Amazon Simple Storage Service (Amazon S3). From there, you can transfer it to either Amazon S3 Glacier Flexible Retrieval or Amazon S3 Glacier Deep Archive to help minimize your long-term storage costs.

<https://aws.amazon.com/storagegateway/vtl/#:~:text=Use-,Tape%20Gateway,-to%20replace%20physical>
upvoted 1 times

 **Nisarg2121** 1 month, 1 week ago

Selected Answer: D

Tape Gateway is use for attach with app.
upvoted 2 times

 **gouranga45** 1 month, 2 weeks ago

Selected Answer: D

Option says it all
upvoted 2 times

 **Po_chih** 1 month, 2 weeks ago

Selected Answer: D

Tape Gateway enables you to replace using physical tapes on premises with virtual tapes in AWS without changing existing backup workflows. Tape Gateway supports all leading backup applications and caches virtual tapes on premises for low-latency data access. Tape Gateway encrypts data between the gateway and AWS for secure data transfer, and compresses data and transitions virtual tapes between Amazon S3 and Amazon S3 Glacier Flexible Retrieval, or Amazon S3 Glacier Deep Archive, to minimize storage costs.
upvoted 1 times

 **ssa03** 2 months, 3 weeks ago

Selected Answer: D

https://aws.amazon.com/storagegateway/vtl/?nc1=h_ls
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: D

Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.
upvoted 1 times

 **Bmaster** 3 months, 4 weeks ago

D is correct

https://aws.amazon.com/storagegateway/vtl/?nc1=h_ls
upvoted 1 times

A company has data collection sensors at different locations. The data collection sensors stream a high volume of data to the company. The company wants to design a platform on AWS to ingest and process high-volume streaming data. The solution must be scalable and support data collection in near real time. The company must store the data in Amazon S3 for future reporting.

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

- A. Use Amazon Kinesis Data Firehose to deliver streaming data to Amazon S3.
- B. Use AWS Glue to deliver streaming data to Amazon S3.
- C. Use AWS Lambda to deliver streaming data and store the data to Amazon S3.
- D. Use AWS Database Migration Service (AWS DMS) to deliver streaming data to Amazon S3.

Correct Answer: A

Community vote distribution

A (76%) D (24%)

 **TariqKipkemei** 1 week, 5 days ago

Selected Answer: A

Amazon Kinesis Data Firehose: Capture, transform, and load data streams into AWS data stores (S3) in near real-time.

https://aws.amazon.com/pm/kinesis/?gclid=CjwKCAiAu9yqBhBmEiwAHTx5px9z182o0HBEX0BGXU7VeOCOdNpkJMxgbSfvCHINKN4NHVnbEa0Y1xoCuU0QAvD_BwE&trk=239a97c0-9c5d-42a5-ac65-7381b62f3756&sc_channel=ps&ef_id=CjwKCAiAu9yqBhBmEiwAHTx5px9z182o0HBEX0BGXU7VeOCOdNpkJMxgbSfvCHINKN4NHVnbEa0Y1xoCuU0QAvD_BwE:G:s&s_kwcid=AL!4422!3!651612444428!e!!g!!kinesis%20firehose!19836376048!149982297311#:~:text=Kinesis%20Data%20Firehose-,Capture%2C,-transform%2C%20and%20load

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: A

A for sure

upvoted 2 times

 **ssa03** 2 months, 3 weeks ago

Selected Answer: A

Correct Answer: A

upvoted 2 times

 **manOfThePeople** 2 months, 4 weeks ago

A is the answer, near real-time = Kinesis Data Firehose.

upvoted 3 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: D

Use Amazon Kinesis Data Firehose to deliver streaming data to Amazon S3

upvoted 2 times

 **bjexamprep** 3 months, 2 weeks ago

Selected Answer: D

Kinesis Data Firehose is only real-time answer

upvoted 2 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: A

A is the correct answer

upvoted 2 times

 **Deepakin96** 3 months, 3 weeks ago

Selected Answer: A

Kinesis = Near Real Time

upvoted 3 times

 **Kaiden123** 3 months, 4 weeks ago

Selected Answer: A

Data collection in near real time = Amazon Kinesis Data Firehose
upvoted 3 times

 **Bmaster** 3 months, 4 weeks ago

A is correct..

upvoted 1 times

A company has separate AWS accounts for its finance, data analytics, and development departments. Because of costs and security concerns, the company wants to control which services each AWS account can use.

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

- A. Use AWS Systems Manager templates to control which AWS services each department can use.
- B. Create organization units (OUs) for each department in AWS Organizations. Attach service control policies (SCPs) to the OUs.
- C. Use AWS CloudFormation to automatically provision only the AWS services that each department can use.
- D. Set up a list of products in AWS Service Catalog in the AWS accounts to manage and control the usage of specific AWS services.

Correct Answer: B

Community vote distribution

B (88%) 13%

 **TariqKipkemei** 1 week, 5 days ago

Selected Answer: B

Create organization units (OUs) for each department in AWS Organizations. Attach service control policies (SCPs) to the OUs
upvoted 1 times

 **ssa03** 2 months, 3 weeks ago

Selected Answer: B

Correct Answer: B
upvoted 1 times

 **lemur88** 3 months ago

Selected Answer: B

SCPs to centralize permissioning
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Create organization units (OUs) for each department in AWS Organizations. Attach service control policies (SCPs) to the OUs.
upvoted 1 times

 **xyb** 3 months, 3 weeks ago

Selected Answer: B

control services --> SCP
upvoted 1 times

 **Ale1973** 3 months, 3 weeks ago

Selected Answer: D

My rational: Scenary is "A company has separate AWS accounts", it is not mentioning anything about use of Organizations or needs related to centralized management of these accounts.
Then, set up a list of products in AWS Service Catalog in the AWS accounts (on each AWS account) is the best way to manage and control the usage of specific AWS services.
upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: B

BBBBBBBB
upvoted 1 times

 **Deepakin96** 3 months, 3 weeks ago

Selected Answer: B

To control different AWS account you required AWS Organisation
upvoted 1 times

 **Bmaster** 3 months, 4 weeks ago

B is correct!!!!

upvoted 1 times

A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devise a strategy that maximizes security without increasing operational overhead.

What should the solutions architect do to meet these requirements?

- A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
- B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
- C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
- D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

Correct Answer: B

Community vote distribution

B (100%)

 **TariqKipkemei** 1 week, 5 days ago

Selected Answer: B

Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway
upvoted 1 times

 **ssa03** 2 months, 3 weeks ago

Selected Answer: B

Correct Answer: B
upvoted 2 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
upvoted 1 times

 **Deepakin96** 3 months, 3 weeks ago

Selected Answer: B

NAT Gateway is safe
upvoted 2 times

 **Bmaster** 3 months, 4 weeks ago

B is correct
upvoted 1 times

A company is using AWS Key Management Service (AWS KMS) keys to encrypt AWS Lambda environment variables. A solutions architect needs to ensure that the required permissions are in place to decrypt and use the environment variables.

Which steps must the solutions architect take to implement the correct permissions? (Choose two.)

- A. Add AWS KMS permissions in the Lambda resource policy.
- B. Add AWS KMS permissions in the Lambda execution role.
- C. Add AWS KMS permissions in the Lambda function policy.
- D. Allow the Lambda execution role in the AWS KMS key policy.
- E. Allow the Lambda resource policy in the AWS KMS key policy.

Correct Answer: BD

Community vote distribution

BD (100%)

 **TariqKipkemei** 1 week, 5 days ago

Selected Answer: BD

Allow the Lambda execution role in the AWS KMS key policy then add AWS KMS permissions in the role.
upvoted 1 times

 **ssa03** 2 months, 3 weeks ago

Selected Answer: BD

Correct Answer: BD
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: BD

To decrypt environment variables encrypted with AWS KMS, Lambda needs to be granted permissions to call KMS APIs. This is done in two places:

The Lambda execution role needs kms:Decrypt and kms:GenerateDataKey permissions added. The execution role governs what AWS services the function code can access.

The KMS key policy needs to allow the Lambda execution role to have kms:Decrypt and kms:GenerateDataKey permissions for that specific key. This allows the execution role to use that particular key.

upvoted 3 times

 **Nirav1112** 3 months, 3 weeks ago

its B & D

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: BD

BD BD BD BD
upvoted 1 times

 **Deepakin96** 3 months, 3 weeks ago

Selected Answer: BD

Its B and D
upvoted 1 times

 **Bmaster** 3 months, 4 weeks ago

My choice is B,D
upvoted 1 times

A company has a financial application that produces reports. The reports average 50 KB in size and are stored in Amazon S3. The reports are frequently accessed during the first week after production and must be stored for several years. The reports must be retrievable within 6 hours.

Which solution meets these requirements MOST cost-effectively?

- A. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier after 7 days.
- B. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days.
- C. Use S3 Intelligent-Tiering. Configure S3 Intelligent-Tiering to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Glacier.
- D. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier Deep Archive after 7 days.

Correct Answer: B

Community vote distribution

A (54%) C (42%) 4%

 **zjcorpuz** Highly Voted 3 months, 3 weeks ago

Answer is A

Amazon S3 Glacier:

Expedited Retrieval: Provides access to data within 1-5 minutes.

Standard Retrieval: Provides access to data within 3-5 hours.

Bulk Retrieval: Provides access to data within 5-12 hours.

Amazon S3 Glacier Deep Archive:

Standard Retrieval: Provides access to data within 12 hours.

Bulk Retrieval: Provides access to data within 48 hours.

upvoted 14 times

 **oayoade** Highly Voted 3 months, 1 week ago

Selected Answer: C

All the "....after 7 days" options are wrong.

Before you transition objects to S3 Standard-IA or S3 One Zone-IA, you must store them for at least 30 days in Amazon S3

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html#:~:text=Minimum%20Days%20for%20Transition%20to%20S3%20Standard%2DIA%20or%20S3%20One%20Zone%2DIA>

upvoted 8 times

 **Hades2231** 3 months ago

This is worth noticing! Glad I came across your comment 1 day before my test.

upvoted 3 times

 **franbarberan** 2 months ago

the 7 days limitation is only if you want to move from s3 standart to S3 Standard-IA or S3 One Zone-IA, if you move to s3 glacier dont have this limitation, correct answer is A

upvoted 6 times

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

Selected Answer: A

Any option with S3 Intelligent-Tiering is out, this is only required when the access patterns are unknown.

From the question the access patterns are well known, enough to tie the frequently accessed reports to S3 standard and transition them to S3 glacier after 7days.

upvoted 2 times

 **iwannabeawsgod** 1 month, 1 week ago

Selected Answer: A

its A for me

upvoted 1 times

 **Carlos_O** 1 month, 3 weeks ago

Selected Answer: A

Tiene mas sentido

upvoted 1 times

 **sl2man** 1 month, 3 weeks ago

Selected Answer: A

Option A

Amazon S3 Glacier Standard Retrieval: Provides access to data within 3-5 hours.

upvoted 1 times

✉ **Ramdi1** 2 months ago

Selected Answer: A

most cost effective has to be glacier so A
With C it is using intelligence tiering which is 30 days minimum from what I have read, I may be wrong on how I read that.
upvoted 1 times

✉ **tabyDolly** 2 months, 1 week ago

answer A
frequent access during the first week -> keeps data in s3 standard for 7 days
stored for several year and retrievable within 6 hours -> can be moved to s3 glacier for data archive purpose
upvoted 1 times

✉ **anikety123** 2 months, 2 weeks ago

Selected Answer: A

Its A. Data cannot be transitioned from Intelligent Tiering to Standard IA
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>
upvoted 2 times

✉ **MII1975** 2 months, 3 weeks ago

Selected Answer: C

Check Oayoade comment, before transition, 30 days in S3 the files have to be, young padawans
upvoted 2 times

✉ **ssa03** 2 months, 3 weeks ago

Selected Answer: C

Correct Answer: C
upvoted 1 times

✉ **ersin13** 3 months, 3 weeks ago

I agree with zjcorpuz the answer is A
upvoted 1 times

✉ **D10SJoker** 3 months, 3 weeks ago

Selected Answer: A

Option A
upvoted 3 times

✉ **D10SJoker** 3 months, 3 weeks ago

For me it's A because option D uses Amazon S3 Glacier Deep Archive, which has 12-48 hours retrieval of data.
upvoted 3 times

✉ **mrsoa** 3 months, 3 weeks ago

Selected Answer: A

For me its A because S3 glacier Flexible retrieval standard can retrieve files in 3 to 5 hours

D is incorrect because S3 glacier deep archive needs 12 hours minimum to retrieve files

B and C are more expensive comparing to A and D
upvoted 3 times

✉ **RazSteel** 3 months, 4 weeks ago

Selected Answer: D

For me its D coz the size of files are 50kb
upvoted 1 times

✉ **PLN6302** 3 months ago

I think option D also.because we have to retrieve the data within 6 hours that can be possible with S3 glacier deep archive
upvoted 2 times

✉ **darekw** 2 months ago

The Amazon S3 Glacier Deep Archive storage class provides two retrieval options ranging from 12-48 hours.
upvoted 1 times

✉ **Josantru** 4 months ago

Correct C.
is halting the storage of data for a number of years
upvoted 3 times

A company needs to optimize the cost of its Amazon EC2 instances. The company also needs to change the type and family of its EC2 instances every 2-3 months.

What should the company do to meet these requirements?

- A. Purchase Partial Upfront Reserved Instances for a 3-year term.
- B. Purchase a No Upfront Compute Savings Plan for a 1-year term.
- C. Purchase All Upfront Reserved Instances for a 1-year term.
- D. Purchase an All Upfront EC2 Instance Savings Plan for a 1-year term.

Correct Answer: D

Community vote distribution

B (100%)

 **Guru4Cloud** Highly Voted 3 months, 1 week ago

Selected Answer: B

The key considerations are:

The company needs flexibility to change EC2 instance types and families every 2-3 months. This rules out Reserved Instances which lock you into an instance type and family for 1-3 years.
A Compute Savings Plan allows switching instance types and families freely within the term as needed. No Upfront is more flexible than All Upfront.
A 1-year term balances commitment and flexibility better than a 3-year term given the company's changing needs.
With No Upfront, the company only pays for usage monthly without an upfront payment. This optimizes cost.

upvoted 6 times

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

Selected Answer: B

Only Compute Savings Plan allows you to change instance family.

upvoted 1 times

 **avky** 3 months, 2 weeks ago

Selected Answer: B

" needs to change the type and family of its EC2 instances". that means B I think.
upvoted 1 times

 **Kiki_Pass** 3 months, 3 weeks ago

Selected Answer: B

"EC2 Instance Savings Plans give you the flexibility to change your usage between instances WITHIN a family in that region."
<https://aws.amazon.com/savingsplans/compute-pricing/>
upvoted 2 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: B

B is the right answer
upvoted 1 times

 **Bmaster** 3 months, 4 weeks ago

B is correct..
'EC2 Instance Savings Plans' can't change 'family'.
upvoted 1 times

 **Josantru** 4 months ago

Correct B.
To change 'Family' always Compute saving plan, right?
upvoted 3 times

A solutions architect needs to review a company's Amazon S3 buckets to discover personally identifiable information (PII). The company stores the PII data in the us-east-1 Region and us-west-2 Region.

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

- A. Configure Amazon Macie in each Region. Create a job to analyze the data that is in Amazon S3.
- B. Configure AWS Security Hub for all Regions. Create an AWS Config rule to analyze the data that is in Amazon S3.
- C. Configure Amazon Inspector to analyze the data that is in Amazon S3.
- D. Configure Amazon GuardDuty to analyze the data that is in Amazon S3.

Correct Answer: A

Community vote distribution

A (100%)

 **TariqKipkemei** 1 week, 2 days ago

Selected Answer: A

Amazon Macie = PII

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

The key reasons are:

Amazon Macie is designed specifically for discovering and classifying sensitive data like PII in S3. This makes it the optimal service to use. Macie can be enabled directly in the required Regions rather than enabling it across all Regions which is unnecessary. This minimizes overhead. Macie can be set up to automatically scan the specified S3 buckets on a schedule. No need to create separate jobs. Security Hub is for security monitoring across AWS accounts, not specific for PII discovery. More overhead than needed. Inspector and GuardDuty are not built for PII discovery in S3 buckets. They provide broader security capabilities.

upvoted 3 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: A

AWS Macie = PII detection

upvoted 3 times

 **Deepakin96** 3 months, 3 weeks ago

Selected Answer: A

Amazon Macie will identify all PII

upvoted 2 times

A company's SAP application has a backend SQL Server database in an on-premises environment. The company wants to migrate its on-premises application and database server to AWS. The company needs an instance type that meets the high demands of its SAP database. On-premises performance data shows that both the SAP application and the database have high memory utilization.

Which solution will meet these requirements?

- A. Use the compute optimized instance family for the application. Use the memory optimized instance family for the database.
- B. Use the storage optimized instance family for both the application and the database.
- C. Use the memory optimized instance family for both the application and the database.
- D. Use the high performance computing (HPC) optimized instance family for the application. Use the memory optimized instance family for the database.

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud**  3 months, 1 week ago

Selected Answer: C

Since both the app and database have high memory needs, the memory optimized family like R5 instances meet those requirements well. Using the same instance family simplifies management and operations, rather than mixing instance types.
Compute optimized instances may not provide enough memory for the SAP app's needs.
Storage optimized is overkill for the database's compute and memory needs.
HPC is overprovisioned for the SAP app.

upvoted 6 times

 **TariqKipkemei**  1 week, 2 days ago

Selected Answer: C

Use the memory optimized instance family for both the application and the database
upvoted 1 times

 **manOfThePeople** 2 months, 4 weeks ago

High memory utilization = memory optimized.
C is the answer
upvoted 3 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: C

I thyink its C
upvoted 1 times

A company runs an application in a VPC with public and private subnets. The VPC extends across multiple Availability Zones. The application runs on Amazon EC2 instances in private subnets. The application uses an Amazon Simple Queue Service (Amazon SQS) queue.

A solutions architect needs to design a secure solution to establish a connection between the EC2 instances and the SQS queue.

Which solution will meet these requirements?

- A. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the private subnets. Add to the endpoint a security group that has an inbound access rule that allows traffic from the EC2 instances that are in the private subnets.
- B. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach to the interface endpoint a VPC endpoint policy that allows access from the EC2 instances that are in the private subnets.
- C. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach an Amazon SQS access policy to the interface VPC endpoint that allows requests from only a specified VPC endpoint.
- D. Implement a gateway endpoint for Amazon SQS. Add a NAT gateway to the private subnets. Attach an IAM role to the EC2 instances that allows access to the SQS queue.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** Highly Voted 3 months, 1 week ago

Selected Answer: A

An interface VPC endpoint is a private way to connect to AWS services without having to expose your VPC to the public internet. This is the most secure way to connect to Amazon SQS from the private subnets.

Configuring the endpoint to use the private subnets ensures that the traffic between the EC2 instances and the SQS queue is only within the VPC. This helps to protect the traffic from being intercepted by a malicious actor.

Adding a security group to the endpoint that has an inbound access rule that allows traffic from the EC2 instances that are in the private subnets further restricts the traffic to only the authorized sources. This helps to prevent unauthorized access to the SQS queue.

upvoted 5 times

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

Selected Answer: A

Answer is A

upvoted 1 times

 **TariqKipkemei** 1 week, 2 days ago

Interface endpoints enable connectivity to services over AWS PrivateLink. It is a collection of one or more elastic network interfaces with a private IP address that serves as an entry point for traffic destined to a supported service.

Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the private subnets. Add to the endpoint a security group that has an inbound access rule that allows traffic from the EC2 instances that are in the private subnets.

upvoted 1 times

 **potomac** 1 month ago

A is correct

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: A

I think its A

upvoted 1 times

 **Bmaster** 3 months, 4 weeks ago

A is correct.

B,C: 'Configuring endpoints to use public subnets' --> Invalid

D: No Gateway Endpoint for SQS.

upvoted 4 times

A solutions architect is using an AWS CloudFormation template to deploy a three-tier web application. The web application consists of a web tier and an application tier that stores and retrieves user data in Amazon DynamoDB tables. The web and application tiers are hosted on Amazon EC2 instances, and the database tier is not publicly accessible. The application EC2 instances need to access the DynamoDB tables without exposing API credentials in the template.

What should the solutions architect do to meet these requirements?

- A. Create an IAM role to read the DynamoDB tables. Associate the role with the application instances by referencing an instance profile.
- B. Create an IAM role that has the required permissions to read and write from the DynamoDB tables. Add the role to the EC2 instance profile, and associate the instance profile with the application instances.
- C. Use the parameter section in the AWS CloudFormation template to have the user input access and secret keys from an already-created IAM user that has the required permissions to read and write from the DynamoDB tables.
- D. Create an IAM user in the AWS CloudFormation template that has the required permissions to read and write from the DynamoDB tables. Use the GetAtt function to retrieve the access and secret keys, and pass them to the application instances through the user data.

Correct Answer: B

Community vote distribution

B (82%)

A (18%)

 **Nisarg2121** 1 month, 1 week ago

Selected Answer: B

B is correct, A total wrong because "read the DynamoDB tables", so what about write in database.
upvoted 3 times

 **darekw** 3 months, 1 week ago

question says: ...application tier stores and retrieves user data in Amazon DynamoDB tables... so it needs read and write access
A) is only read access
B) seems to be the right answer
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Option B is the correct approach to meet the requirements:

Create an IAM role with permissions to access DynamoDB
Add the IAM role to an EC2 Instance Profile
Associate the Instance Profile with the application EC2 instances
This allows the instances to assume the IAM role to obtain temporary credentials to access DynamoDB.
upvoted 2 times

 **anibinaadi** 3 months, 2 weeks ago

Explanation. Both A and B seems suitable. But Option A is incorrect because it says "Associate the role with the application instances by referencing an instance profile". Which just only a Part of the solution.

In API/AWS CLI following steps are required to complete the Role-> instance profile association-> to instance.

1. Create an IAM Role
 2. add-role-to-instance-profile (aws iam add-role-to-instance-profile --role-name S3Access --instance-profile-name Webserver)
 3. associate-iam-instance-profile (aws ec2 associate-iam-instance-profile --instance-id i-123456789abcde123 --iam-instance-profile Name=admin-role)
- hence Option B is correct.

upvoted 2 times

 **DannyKang5649** 3 months, 2 weeks ago

Selected Answer: B

Why "No read and write" ? The question clearly states that application tier STORE and RETRIEVE the data from DynamoDB. Which means write and read... I think answer should be B

upvoted 2 times

 **xyb** 3 months, 3 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/80755-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Ale1973** 3 months, 3 weeks ago

Selected Answer: B

My rationl: Option A is wrong because the scenario says "stores and retrieves user data in Amazon DynamoDB tables", STORES and RETRIVE, if you set a role to READ, you can write on DinamoDB database

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: A

AAAAAAA

upvoted 1 times

 **kangho** 3 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

A solutions architect manages an analytics application. The application stores large amounts of semistructured data in an Amazon S3 bucket. The solutions architect wants to use parallel data processing to process the data more quickly. The solutions architect also wants to use information that is stored in an Amazon Redshift database to enrich the data.

Which solution will meet these requirements?

- A. Use Amazon Athena to process the S3 data. Use AWS Glue with the Amazon Redshift data to enrich the S3 data.
- B. Use Amazon EMR to process the S3 data. Use Amazon EMR with the Amazon Redshift data to enrich the S3 data.
- C. Use Amazon EMR to process the S3 data. Use Amazon Kinesis Data Streams to move the S3 data into Amazon Redshift so that the data can be enriched.
- D. Use AWS Glue to process the S3 data. Use AWS Lake Formation with the Amazon Redshift data to enrich the S3 data.

Correct Answer: D

Community vote distribution

B (52%)

A (48%)

 **Guru4Cloud** Highly Voted 3 months, 1 week ago

Selected Answer: B

Option B is the correct solution that meets the requirements:

Use Amazon EMR to process the semi-structured data in Amazon S3. EMR provides a managed Hadoop framework optimized for processing large datasets in S3.

EMR supports parallel data processing across multiple nodes to speed up the processing.

EMR can integrate directly with Amazon Redshift using the EMR-Redshift integration. This allows querying the Redshift data from EMR and joining it with the S3 data.

This enables enriching the semi-structured S3 data with the information stored in Redshift

upvoted 6 times

 **zjcorpuz** Highly Voted 3 months, 3 weeks ago

By combining AWS Glue and Amazon Redshift, you can process the semistructured data in parallel using Glue ETL jobs and then store the processed and enriched data in a structured format in Amazon Redshift. This approach allows you to perform complex analytics efficiently and at scale.

upvoted 5 times

 **aragornfsm** Most Recent 1 day, 11 hours ago

i think a is correct

semistructured data ==> Athena

upvoted 1 times

 **riyasara** 3 days, 13 hours ago

Athena is not designed for parallel data processing. So it's B

upvoted 1 times

 **TariqKipkemei** 1 week, 2 days ago

Selected Answer: A

Answer is A

upvoted 1 times

 **TariqKipkemei** 1 week, 2 days ago

Selected Answer: B

From this documentation looks like EMR cannot interface with S3.

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

I will settle with option A.

upvoted 1 times

 **bogobob** 1 week, 6 days ago

Selected Answer: B

For those answering A, AWS Glue can directly query S3, it can't use Athena as a source of data. The questions say the Redshift data should be used to "enrich" which means that the Redshift data needs to be "added" to the S3 data. A doesn't allow that.

upvoted 1 times

 **hungta** 1 week, 6 days ago

Selected Answer: B

Choose option B.

Option A is not correct. Amazon Athena is suitable for querying data directly from S3 using SQL and allows parallel processing of S3 data.

AWS Glue can be used for data preparation and enrichment but might not directly integrate with Amazon Redshift for enrichment.

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: A

Athena and Redshift both do SQL query

upvoted 1 times

 **Sab123** 1 month, 3 weeks ago

Selected Answer: A

semi-structure supported by Athena not by EMR

upvoted 3 times

 **JKevin778** 2 months ago

Selected Answer: A

athena for s3

upvoted 1 times

 **BrijMohan08** 3 months ago

Selected Answer: B

EMR Works best for Analytics based solutions.

upvoted 2 times

 **ukivanlamipi** 3 months, 2 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/architecture/reduce-archive-cost-with-serverless-data-archiving/>

upvoted 4 times

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs?

- A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.
- B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.
- C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
- D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Correct Answer: C

Community vote distribution

C (100%)

 **TariqKipkemei** 1 week, 2 days ago

Selected Answer: C

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different Regions (also known as an inter-Region VPC peering connection).

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html#:~:text=A-,VPC%20peering,-connection%20is%20a>
upvoted 1 times

 **BrijMohan08** 3 months ago

Selected Answer: C

Transit Gateway network peering.
VPC Peering to peer 2 or more VPC in the same region.
upvoted 3 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

The key reasons are:

VPC peering provides private connectivity between VPCs without using public IP space.
Data transferred between peered VPCs is free as long as they are in the same region.
500 GB/month inter-VPC data transfer fits within peering free tier.
Transit Gateway (Option A) incurs hourly charges plus data transfer fees. More costly than peering.
Site-to-Site VPN (Option B) incurs hourly charges and data transfer fees. More expensive than peering.
Direct Connect (Option D) has high hourly charges and would be overkill for this use case.
upvoted 3 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: C

VPC peering is the most cost-effective solution
upvoted 1 times

 **Deepakin96** 3 months, 3 weeks ago

Selected Answer: C

Communicating with two VPC in same account = VPC Peering
upvoted 1 times

 **luiscc** 3 months, 4 weeks ago

Selected Answer: C

C is the correct answer.

VPC peering is the most cost-effective way to connect two VPCs within the same region and AWS account. There are no additional charges for VPC peering beyond standard data transfer rates.

Transit Gateway and VPN add additional hourly and data processing charges that are not necessary for simple VPC peering.

Direct Connect provides dedicated network connectivity, but is overkill for the relatively low inter-VPC data transfer needs described here. It has high fixed costs plus data transfer rates.

For occasional inter-VPC communication of moderate data volumes within the same region and account, VPC peering is the most cost-effective solution. It provides simple private connectivity without transfer charges or network appliances.

upvoted 2 times

Question #559

Topic 1

A company hosts multiple applications on AWS for different product lines. The applications use different compute resources, including Amazon EC2 instances and Application Load Balancers. The applications run in different AWS accounts under the same organization in AWS Organizations across multiple AWS Regions. Teams for each product line have tagged each compute resource in the individual accounts.

The company wants more details about the cost for each product line from the consolidated billing feature in Organizations.

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

- A. Select a specific AWS generated tag in the AWS Billing console.
- B. Select a specific user-defined tag in the AWS Billing console.
- C. Select a specific user-defined tag in the AWS Resource Groups console.
- D. Activate the selected tag from each AWS account.
- E. Activate the selected tag from the Organizations management account.

Correct Answer: BE

Community vote distribution

BE (100%)

 **Guru4Cloud**  3 months, 1 week ago

Selected Answer: BE

The reasons are:

User-defined tags were created by each product team to identify resources. Selecting the relevant tag in the Billing console will group costs. The tag must be activated from the Organizations management account to consolidate billing across all accounts. AWS generated tags are predefined by AWS and won't align to product lines. Resource Groups (Option C) helps manage resources but not billing. Activating the tag from each account (Option D) is not needed since Organizations centralizes billing.

upvoted 6 times

 **potomac**  3 weeks, 1 day ago

Selected Answer: BE

Your user-defined cost allocation tags represent the tag key, which you activate in the Billing console.

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: BE

BE BE BE BE

upvoted 1 times

 **Kiki_Pass** 3 months, 3 weeks ago

Selected Answer: BE

"Only a management account in an organization and single accounts that aren't members of an organization have access to the cost allocation tags manager in the Billing and Cost Management console."

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

upvoted 1 times

A company's solutions architect is designing an AWS multi-account solution that uses AWS Organizations. The solutions architect has organized the company's accounts into organizational units (OUs).

The solutions architect needs a solution that will identify any changes to the OU hierarchy. The solution also needs to notify the company's operations team of any changes.

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

- A. Provision the AWS accounts by using AWS Control Tower. Use account drift notifications to identify the changes to the OU hierarchy.
- B. Provision the AWS accounts by using AWS Control Tower. Use AWS Config aggregated rules to identify the changes to the OU hierarchy.
- C. Use AWS Service Catalog to create accounts in Organizations. Use an AWS CloudTrail organization trail to identify the changes to the OU hierarchy.
- D. Use AWS CloudFormation templates to create accounts in Organizations. Use the drift detection operation on a stack to identify the changes to the OU hierarchy.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** Highly Voted 3 months, 1 week ago

Selected Answer: A

The key advantages you highlight of Control Tower are convincing:

Fully managed service simplifies multi-account setup.
Built-in account drift notifications detect OU changes automatically.
More scalable and less complex than Config rules or CloudTrail.
Better security and compliance guardrails than custom options.
Lower operational overhead compared to other solution

upvoted 7 times

 **Bmaster** Highly Voted 3 months, 4 weeks ago

A is correct.

<https://docs.aws.amazon.com/controllertower/latest/userguide/what-is-control-tower.html>
<https://docs.aws.amazon.com/controllertower/latest/userguide/prevention-and-notification.html>

upvoted 5 times

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

Selected Answer: A

AWS Control Tower provides passive and active methods of drift monitoring protection for preventive controls.

upvoted 1 times

 **darekw** 3 months, 1 week ago

<https://docs.aws.amazon.com/controllertower/latest/userguide/prevention-and-notification.html>

upvoted 1 times

A company's website handles millions of requests each day, and the number of requests continues to increase. A solutions architect needs to improve the response time of the web application. The solutions architect determines that the application needs to decrease latency when retrieving product details from the Amazon DynamoDB table.

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

- A. Set up a DynamoDB Accelerator (DAX) cluster. Route all read requests through DAX.
- B. Set up Amazon ElastiCache for Redis between the DynamoDB table and the web application. Route all read requests through Redis.
- C. Set up Amazon ElastiCache for Memcached between the DynamoDB table and the web application. Route all read requests through Memcached.
- D. Set up Amazon DynamoDB Streams on the table, and have AWS Lambda read from the table and populate Amazon ElastiCache. Route all read requests through ElastiCache.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **mrsoa**  3 months, 3 weeks ago

Selected Answer: A

A , because B,C and D contains ElastiCache which required a heavy code changes, so more operational overhead
upvoted 6 times

✉️  **TariqKipkemei**  1 week, 1 day ago

Selected Answer: A

decrease latency when retrieving product details from the Amazon DynamoDB = Amazon DynamoDB Accelerator (DAX)
upvoted 1 times

✉️  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

The key reasons:

DAX provides a DynamoDB-compatible caching layer to reduce read latency. It is purpose-built for accelerating DynamoDB workloads.
Using DAX requires minimal application changes - only read requests are routed through it.
DAX handles caching logic automatically without needing complex integration code.
ElastiCache Redis/Memcached (Options B/C) require more integration work to sync DynamoDB data.
Using Lambda and Streams to populate ElastiCache (Option D) is a complex event-driven approach requiring ongoing maintenance.
DAX plugs in seamlessly to accelerate DynamoDB with very little operational overhead
upvoted 2 times

✉️  **Deepakin96** 3 months, 3 weeks ago

Selected Answer: A

DynamoDB = DAX
upvoted 2 times

✉️  **Bmaster** 3 months, 4 weeks ago

only A
upvoted 2 times

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not travel across the internet.

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

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create an interface endpoint for Amazon EC2.
- D. Create an elastic network interface for the endpoint in each of the subnets of the VPC.
- E. Create a security group entry in the endpoint's security group to provide access.

Correct Answer: AB

Community vote distribution

AB (66%)	BE (28%)	6%
----------	----------	----

 **ukivanlampli**  3 months, 2 weeks ago

Selected Answer: AB

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-ddb.html>

upvoted 8 times

 **Guru4Cloud**  3 months, 1 week ago

Selected Answer: BE

The reasons are:

A gateway endpoint for DynamoDB enables private connectivity between DynamoDB and the VPC. This allows EC2 instances to access DynamoDB APIs without traversing the internet.

A security group entry is needed to allow the EC2 instances access to the DynamoDB endpoint over the VPC.

An interface endpoint is used for services like S3 and Systems Manager, not DynamoDB.

Route table entries route traffic within a VPC but do not affect external connectivity.

Elastic network interfaces are not needed for gateway endpoints.

upvoted 6 times

 **unbendable** 1 month ago

"The outbound rules for the security group for instances that access DynamoDB through the gateway endpoint must allow traffic to DynamoDB", <https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-ddb.html>

The option however is talking about the security group of the endpoint

upvoted 1 times

 **TariqKipkemei**  1 week, 1 day ago

Selected Answer: AB

Create a gateway endpoint for DynamoDB then create a route table entry for the endpoint

upvoted 1 times

 **EdenWang** 1 week, 4 days ago

Selected Answer: BE

refer to question 555

upvoted 1 times

 **cciesam** 2 weeks, 1 day ago

Selected Answer: AB

<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html#vpc-endpoints-routing>

Traffic from your VPC to Amazon S3 or DynamoDB is routed to the gateway endpoint. Each subnet route table must have a route that sends traffic destined for the service to the gateway endpoint using the prefix list for the service.

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: AB

You can access Amazon DynamoDB from your VPC using gateway VPC endpoints. After you create the gateway endpoint, you can add it as a target in your route table for traffic destined from your VPC to DynamoDB.

upvoted 1 times

 **danielmakita** 1 month ago

It is A and B. Not E because security group does not span VPCs.

upvoted 2 times

 **iwannabeawsgod** 1 month, 1 week ago

Selected Answer: AB

A and B for sure
upvoted 2 times

 **loveaws** 1 month, 3 weeks ago

B and D.
upvoted 1 times

 **baba365** 2 months ago

Answer: E.
Example Question #555 -

Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the private subnets. Add to the endpoint a security group that has an inbound access rule that allows traffic from the EC2 instances that are in the private subnets.

upvoted 2 times

 **Devsin2000** 2 months ago

Selected Answer: BE

A - incorrect, because "When you create a gateway endpoint, you select the VPC route tables for the subnets that you enable. The route is automatically added to each route table that you select."
E- Security Group must allow the communication
upvoted 2 times

 **kwang312** 2 months, 1 week ago

Selected Answer: AB

A,B is correct
upvoted 2 times

 **avkya** 3 months, 2 weeks ago

Selected Answer: AB

You can access Amazon DynamoDB from your VPC using gateway VPC endpoints. After you create the gateway endpoint, you can add it as a target in your route table for traffic destined from your VPC to DynamoDB.
upvoted 4 times

 **vini15** 3 months, 2 weeks ago

Should be AB
Gateway endpoint donot provision ENI as the entry point it just need an entry in the route table.
upvoted 1 times

 **ersin13** 3 months, 3 weeks ago

This resource are in same vpc .We can use gateway andpoint first we have to create gateway endpoint and wa added and point to associated route table. So answer is B-D
upvoted 2 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: AB

AB AB AB

C,D,E work for any other aws services but for S3 and Dynamodb we use VPC endpoint
upvoted 2 times

 **Soei** 3 months, 3 weeks ago

Selected Answer: BD

B,D is correct
upvoted 2 times

A company runs its applications on both Amazon Elastic Kubernetes Service (Amazon EKS) clusters and on-premises Kubernetes clusters. The company wants to view all clusters and workloads from a central location.

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

- A. Use Amazon CloudWatch Container Insights to collect and group the cluster information.
- B. Use Amazon EKS Connector to register and connect all Kubernetes clusters.
- C. Use AWS Systems Manager to collect and view the cluster information.
- D. Use Amazon EKS Anywhere as the primary cluster to view the other clusters with native Kubernetes commands.

Correct Answer: B

Community vote distribution

B (86%) 14%

 **TariqKipkemei** 1 week, 1 day ago

Selected Answer: B

View all clusters and workloads (incl on-prem) from a central location = Amazon EKS Connector
Create and operate Kubernetes clusters on your own infrastructure = Amazon EKS Anywhere

<https://aws.amazon.com/eks/eks-anywhere/#:~:text=Amazon-,EKS%20Anywhere,-lets%20you%20create>

<https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html#:~:text=You%20can%20use-,Amazon%20EKS%20Connector,-to%20register%20and>

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: B

It is B

upvoted 1 times

 **ErnShm** 2 months, 3 weeks ago

B

You can use Amazon EKS Connector to register and connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console. After a cluster is connected, you can see the status, configuration, and workloads for that cluster in the Amazon EKS console. You can use this feature to view connected clusters in Amazon EKS console, but you can't manage them. The Amazon EKS Connector requires an agent that is an open source project on Github. For additional technical content, including frequently asked questions and troubleshooting, see Troubleshooting issues in Amazon EKS Connector

The Amazon EKS Connector can connect the following types of Kubernetes clusters to Amazon EKS.

On-premises Kubernetes clusters

Self-managed clusters that are running on Amazon EC2

Managed clusters from other cloud providers

upvoted 4 times

 **thainguyensunya** 3 months ago

Selected Answer: B

Definitely B.

"You can use Amazon EKS Connector to register and connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console. After a cluster is connected, you can see the status, configuration, and workloads for that cluster in the Amazon EKS console."

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

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

The key reasons:

EKS Connector allows registering external Kubernetes clusters (on-premises and otherwise) with Amazon EKS

This provides a unified view and management of all clusters within the EKS console.

EKS Connector handles keeping resources in sync across connected clusters.

This centralized approach minimizes operational overhead compared to using separate tools.

CloudWatch Container Insights (Option A) only provides metrics and logs, not cluster management.

Systems Manager (Option C) is more general purpose and does not natively integrate with EKS.
EKS Anywhere (Option D) would not provide a single pane of glass for external clusters.

upvoted 2 times

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

Amazon EKS Connector enables you to create and manage a centralized view of all your Kubernetes clusters, regardless of whether they are Amazon EKS clusters or on-premises Kubernetes clusters. It allows you to register these clusters with your Amazon EKS control plane, providing a unified management interface for all clusters.

upvoted 1 times

✉️ **avkya** 3 months, 2 weeks ago

Selected Answer: B

You can use Amazon EKS Connector to register and connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console. After a cluster is connected, you can see the status, configuration, and workloads for that cluster in the Amazon EKS console. You can use this feature to view connected clusters in Amazon EKS console, but you can't manage them

upvoted 1 times

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

Selected Answer: D

only D can connect to on-perm

upvoted 1 times

✉️ **mrsoa** 3 months, 3 weeks ago

seems B

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

upvoted 4 times

✉️ **Bmaster** 3 months, 4 weeks ago

Only B

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

upvoted 2 times

A company is building an ecommerce application and needs to store sensitive customer information. The company needs to give customers the ability to complete purchase transactions on the website. The company also needs to ensure that sensitive customer data is protected, even from database administrators.

Which solution meets these requirements?

- A. Store sensitive data in an Amazon Elastic Block Store (Amazon EBS) volume. Use EBS encryption to encrypt the data. Use an IAM instance role to restrict access.
- B. Store sensitive data in Amazon RDS for MySQL. Use AWS Key Management Service (AWS KMS) client-side encryption to encrypt the data.
- C. Store sensitive data in Amazon S3. Use AWS Key Management Service (AWS KMS) server-side encryption to encrypt the data. Use S3 bucket policies to restrict access.
- D. Store sensitive data in Amazon FSx for Windows Server. Mount the file share on application servers. Use Windows file permissions to restrict access.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** Highly Voted 3 months, 1 week ago

Selected Answer: B

The key reasons are:

RDS MySQL provides a fully managed database service well suited for an ecommerce application.
AWS KMS client-side encryption allows encrypting sensitive data before it hits the database. The data remains encrypted at rest.
This protects sensitive customer data from database admins and privileged users.
EBS encryption (Option A) protects data at rest but not in use. IAM roles don't prevent admin access.
S3 (Option C) encrypts data at rest on the server side. Bucket policies don't restrict admin access.
FSx file permissions (Option D) don't prevent admin access to unencrypted data.

upvoted 6 times

 **riyasara** Most Recent 3 days, 6 hours ago

Answer is option C. option B is not ideal because Amazon RDS for MySQL is a relational database service that is optimized for structured data, not for storing sensitive customer information. Moreover, by using client-side encryption with AWS KMS, you need to encrypt and decrypt the data in your application code, which increases the risk of exposing your data in transit or at rest. You also need to manage the encryption keys yourself, which adds complexity and overhead to your application.

upvoted 1 times

 **wsdasdasdqwdaw** 1 month ago

I would go for B, because RDS (database admins), but I would like to see as well encryption at rest as well, not only in transit.
upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: B

Using client-side encryption we can protect specific fields and guarantee only decryption if the client has access to an API key, we can protect specific fields even from database admins

upvoted 2 times

 **D10SJoker** 3 months, 3 weeks ago

Selected Answer: B

For me it's B because of "client-side encryption to encrypt the data"
upvoted 1 times

 **h8er** 3 months, 3 weeks ago

keyword - database administrators

upvoted 3 times

 **Kiki_Pass** 3 months, 3 weeks ago

Selected Answer: B

"even from database administrators" -> "Client Side encryption"

upvoted 2 times

 **Bmaster** 3 months, 4 weeks ago

My choice is B
upvoted 3 times

Question #565

Topic 1

A company has an on-premises MySQL database that handles transactional data. The company is migrating the database to the AWS Cloud. The migrated database must maintain compatibility with the company's applications that use the database. The migrated database also must scale automatically during periods of increased demand.

Which migration solution will meet these requirements?

- A. Use native MySQL tools to migrate the database to Amazon RDS for MySQL. Configure elastic storage scaling.
- B. Migrate the database to Amazon Redshift by using the mysqldump utility. Turn on Auto Scaling for the Amazon Redshift cluster.
- C. Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon Aurora. Turn on Aurora Auto Scaling.
- D. Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon DynamoDB. Configure an Auto Scaling policy.

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud**  3 months, 1 week ago

Selected Answer: C

The key reasons are:

DMS provides an easy migration path from MySQL to Aurora while minimizing downtime.
Aurora is a MySQL-compatible relational database service that will maintain compatibility with the company's applications.
Aurora Auto Scaling allows the database to automatically scale up and down based on demand to handle increased workloads.
RDS MySQL (Option A) does not scale as well as the Aurora architecture.
Redshift (Option B) is for analytics, not transactional data, and may not be compatible.
DynamoDB (Option D) is a NoSQL datastore and lacks MySQL compatibility.

upvoted 5 times

 **TariqKipkemei**  1 week, 1 day ago

Selected Answer: C

on-premises MySQL database, transactional data, maintain compatibility, scale automatically = Amazon Aurora
migrating the database to the AWS Cloud = AWS Database Migration Service

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

Aurora is a MySQL-compatible relational database service
upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: C

Aurora is better in autoscaling than RDS
upvoted 1 times

 **Bmaster** 3 months, 4 weeks ago

C is correct
A is incorrect. RDS for MySQL does not scale automatically during periods of increased demand.
B is incorrect. Redshift is used for data sharing purposes.
D is incorrect. you must change application codes.

upvoted 1 times

 **Eminenza22** 3 months, 4 weeks ago

Amazon RDS now supports Storage Auto Scaling
upvoted 1 times

A company runs multiple Amazon EC2 Linux instances in a VPC across two Availability Zones. The instances host applications that use a hierarchical directory structure. The applications need to read and write rapidly and concurrently to shared storage.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 bucket. Allow access from all the EC2 instances in the VPC.
- B. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system from each EC2 instance.
- C. Create a file system on a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to all the EC2 instances.
- D. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. Synchronize the EBS volumes across the different EC2 instances.

Correct Answer: A

Community vote distribution

B (92%) 8%

 **Josantru**  4 months ago

Correct B.

How is Amazon EFS different than Amazon S3?

Amazon EFS provides shared access to data using a traditional file sharing permissions model and hierarchical directory structure via the NFSv4 protocol. Applications that access data using a standard file system interface provided through the operating system can use Amazon EFS to take advantage of the scalability and reliability of file storage in the cloud without writing any new code or adjusting applications.

Amazon S3 is an object storage platform that uses a simple API for storing and accessing data. Applications that do not require a file system structure and are designed to work with object storage can use Amazon S3 as a massively scalable, durable, low-cost object storage solution.

upvoted 8 times

 **TariqKipkemei**  1 week, 1 day ago

Selected Answer: B

hierarchical directory structure, read and write rapidly and concurrently to shared storage = Amazon Elastic File System

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: B

Amazon EFS simultaneously supports on-premises servers using a traditional file permissions model, file locking, and hierarchical directory structure through the NFS v4 protocol.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

The key reasons:

EFS provides a scalable, high performance NFS file system that can be concurrently accessed from multiple EC2 instances.

It supports the hierarchical directory structure needed by the applications.

EFS is elastic, growing and shrinking automatically as needed.

It can be accessed from instances across AZs, meeting the shared storage requirement.

S3 object storage (option A) lacks the file system semantics needed by the apps.

EBS volumes (options C and D) are attached to a single instance and would require replication and syncing to share across instances.

EFS is purpose-built for this use case of a shared file system across Linux instances and aligns best with the performance, concurrency, and availability needs.

upvoted 3 times

 **barracouto** 3 months, 2 weeks ago

Selected Answer: B

Going with b

upvoted 1 times

 **Bennyboy789** 3 months, 2 weeks ago

Selected Answer: B

C and D involve using Amazon EBS volumes, which are block storage. While they can be attached to EC2 instances, they might not provide the same level of shared concurrent access as Amazon EFS. Additionally, synchronizing EBS volumes across different EC2 instances (as in option D) can be complex and error-prone.

Therefore, for a scenario where multiple EC2 instances need to rapidly and concurrently access shared storage with a hierarchical directory structure, Amazon EFS is the best solution.

upvoted 2 times

 **ukivanlamipi** 3 months, 2 weeks ago

Selected Answer: B

s3 is flat structure. EBS multi mount only for same available zone

upvoted 1 times

 **Dana12345** 3 months, 3 weeks ago

Selected Answer: B

Because Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple instances that are in the same Availability Zone. The infra contains 2 AZ's.

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: B

B is the correct answer

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

B is the correct answer

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

upvoted 1 times

 **RazSteel** 3 months, 4 weeks ago

Selected Answer: C

I think that C is the best option coz io2 can share storage and multi attach.

upvoted 1 times

 **PLN6302** 3 months ago

hierarchical directory structure is present in EFS

upvoted 1 times

A solutions architect is designing a workload that will store hourly energy consumption by business tenants in a building. The sensors will feed a database through HTTP requests that will add up usage for each tenant. The solutions architect must use managed services when possible. The workload will receive more features in the future as the solutions architect adds independent components.

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

- A. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in an Amazon DynamoDB table.
- B. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon S3 bucket to store the processed data.
- C. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in a Microsoft SQL Server Express database on an Amazon EC2 instance.
- D. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon Elastic File System (Amazon EFS) shared file system to store the processed data.

Correct Answer: A

Community vote distribution

A (100%)

 **TariqKipkemei** 1 week, 1 day ago

Selected Answer: A

Workload runs every hour, must use managed services, more features in the future, LEAST operational overhead = AWS Lambda functions. HTTP requests, must use managed services, more features in the future, LEAST operational overhead = API Gateway. Must use managed services, more features in the future, LEAST operational overhead =Amazon DynamoDB.

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

The key reasons are:

- API Gateway removes the need to manage servers to receive the HTTP requests from sensors
- Lambda functions provide a serverless compute layer to process data as needed
- DynamoDB is a fully managed NoSQL database that scales automatically
- This serverless architecture has minimal operational overhead to manage
- Options B, C, and D all require managing EC2 instances which increases ops workload
- Option C also adds SQL Server admin tasks and licensing costs
- Option D uses EFS file storage which requires capacity planning and management

upvoted 3 times

 **ersin13** 3 months, 3 weeks ago

key word is "must use managed services when possible" api ,lambda dynamodb are serverless. so answer is A

upvoted 1 times

 **Kiki_Pass** 3 months, 3 weeks ago

Selected Answer: A

"The workload will receive more features in the future ..." -> DynamoDB

upvoted 3 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: A

A seems to be the right answer

upvoted 4 times

 **Bmaster** 3 months, 4 weeks ago

A is correct.

upvoted 2 times

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure.

The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data.

Which combination of storage and caching should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

Correct Answer: A

Community vote distribution

A (100%)

 **TariqKipkemei** 1 week, 1 day ago

Selected Answer: A

Storing and viewing engineering drawings = Amazon S3

Support caching to minimize the amount of time that users wait for the engineering drawings to load = Amazon CloudFront

upvoted 1 times

 **wsdasdasdqwdaw** 1 month ago

CF caching and S3 supports petabytes data

upvoted 2 times

 **lemur88** 3 months ago

Selected Answer: A

CF allows caching

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

The key reasons are:

S3 provides highly durable and scalable object storage capable of handling petabytes of data cost-effectively.

CloudFront can be used to cache S3 content at the edge, minimizing latency for users and speeding up access to the engineering drawings.

The global CloudFront edge network is ideal for caching large amounts of static media like drawings.

EBS provides block storage but lacks the scale and durability of S3 for large media files.

Glacier is cheaper archival storage but has higher latency unsuited for frequent access.

Storage Gateway and ElastiCache may play a role but do not align as well to the main requirements.

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: A

The answer seems A:

B : Glacier for archiving

C : i dont think EBS scale to petabytes (I am not sure about that)

D : it incorrect becasueAll application components will be deployed on the AWS infrastructure

upvoted 2 times

 **Bmaster** 3 months, 4 weeks ago

A is correct

upvoted 3 times

An Amazon EventBridge rule targets a third-party API. The third-party API has not received any incoming traffic. A solutions architect needs to determine whether the rule conditions are being met and if the rule's target is being invoked.

Which solution will meet these requirements?

- A. Check for metrics in Amazon CloudWatch in the namespace for AWS/Events.
- B. Review events in the Amazon Simple Queue Service (Amazon SQS) dead-letter queue.
- C. Check for the events in Amazon CloudWatch Logs.
- D. Check the trails in AWS CloudTrail for the EventBridge events.

Correct Answer: A

Community vote distribution

A (50%) D (33%) C (17%)

✉️  **TariqKipkemei** 1 week, 1 day ago

Selected Answer: D

CloudWatch is a monitoring service for AWS resources and applications. CloudTrail is a web service that records API activity in your AWS account. CloudWatch monitors applications and infrastructure performance in the AWS environment. CloudTrail monitors actions in the AWS environment.
upvoted 1 times

✉️  **EdenWang** 1 week, 4 days ago

Selected Answer: C

C should be correct, I check in AWS management concole.
upvoted 1 times

✉️  **potomac** 3 weeks, 1 day ago

Selected Answer: A

should be A
upvoted 1 times

✉️  **ibu007** 2 months, 3 weeks ago

Selected Answer: D

Check the trails in AWS CloudTrail for the EventBridge events.
upvoted 1 times

✉️  **lemur88** 3 months ago

Selected Answer: A

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-monitoring.html>
upvoted 4 times

✉️  **Eminenza22** 3 months, 1 week ago

Selected Answer: C

Amazon CloudWatch Logs is a service that collects and stores logs from Amazon Web Services (AWS) resources. These logs can be used to troubleshoot problems, monitor performance, and audit activity.
The other options are incorrect:

Option A: CloudWatch metrics are used to track the performance of AWS resources. They are not used to store events.
Option B: Amazon SQS dead-letter queues are used to store messages that cannot be delivered to their intended recipients. They are not used to store events.
Option D: AWS CloudTrail is a service that records AWS API calls. It can be used to track the activity of EventBridge rules, but it does not store the events themselves.
upvoted 2 times

✉️  **Eminenza22** 3 months ago

Errata Corrigé

A

EventBridge sends metrics to Amazon CloudWatch every minute for everything from the number of matched events to the number of times a target is invoked by a rule.
<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-monitoring.html>
upvoted 1 times

✉️  **Eminenza22** 3 months ago

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html>
upvoted 1 times

✉  **jayce5** 3 months, 1 week ago

Selected Answer: D

The answer is D:

"CloudTrail captures API calls made by or on behalf of your AWS account from the EventBridge console and to EventBridge API operations."
(<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-logging-monitoring.html>)

upvoted 2 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: D

The key reasons:

AWS CloudTrail provides visibility into EventBridge operations by logging API calls made by EventBridge.

Checking the CloudTrail trails will show the PutEvents API calls made when EventBridge rules match an event pattern.

CloudTrail will also log the Invoke API call when the rule target is triggered.

CloudWatch metrics and logs contain runtime performance data but not info on rule evaluation and targeting.

SQS dead letter queues collect failed event deliveries but won't provide insights on successful invocations.

CloudTrail is purpose-built to log operational events and API activity so it can confirm if the EventBridge rule is being evaluated and triggering the target as expected.

upvoted 2 times

✉  **Eminenza22** 3 months, 1 week ago

Amazon CloudWatch Logs is a service that collects and stores logs from Amazon Web Services (AWS) resources. These logs can be used to troubleshoot problems, monitor performance, and audit activity.

The other options are incorrect:

Option A: CloudWatch metrics are used to track the performance of AWS resources. They are not used to store events.

Option B: Amazon SQS dead-letter queues are used to store messages that cannot be delivered to their intended recipients. They are not used to store events.

Option D: AWS CloudTrail is a service that records AWS API calls. It can be used to track the activity of EventBridge rules, but it does not store the events themselves.

upvoted 1 times

✉  **Bennyboy789** 3 months, 3 weeks ago

Selected Answer: A

Option A is the most appropriate solution because Amazon EventBridge publishes metrics to Amazon CloudWatch. You can find relevant metrics in the "AWS/Events" namespace, which allows you to monitor the number of events matched by the rule and the number of invocations to the rule's target.

upvoted 3 times

✉  **h8er** 3 months, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html>

upvoted 1 times

A company has a large workload that runs every Friday evening. The workload runs on Amazon EC2 instances that are in two Availability Zones in the us-east-1 Region. Normally, the company must run no more than two instances at all times. However, the company wants to scale up to six instances each Friday to handle a regularly repeating increased workload.

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

- A. Create a reminder in Amazon EventBridge to scale the instances.
- B. Create an Auto Scaling group that has a scheduled action.
- C. Create an Auto Scaling group that uses manual scaling.
- D. Create an Auto Scaling group that uses automatic scaling.

Correct Answer: A

Community vote distribution

B (100%)

 **Bmaster** Highly Voted 3 months, 4 weeks ago

B is correct.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>
upvoted 6 times

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

Selected Answer: B

runs every Friday evening = an Auto Scaling group that has a scheduled action
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

The key reasons:

Auto Scaling scheduled actions allow defining specific dates/times to scale out or in. This can be used to scale to 6 instances every Friday evening automatically.

Scheduled scaling removes the need for manual intervention to scale up/down for the workload.

EventBridge reminders and manual scaling require human involvement each week adding overhead.

Automatic scaling responds to demand and may not align perfectly to scale out every Friday without additional tuning.

Scheduled Auto Scaling actions provide the automation needed to scale for the weekly workload without ongoing operational overhead.
upvoted 1 times

 **Sat897** 3 months, 3 weeks ago

Selected Answer: B

Predicted period.. So schedule the instance
upvoted 3 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: B

B seems to be correct
upvoted 1 times

 **Deepakin96** 3 months, 3 weeks ago

Selected Answer: B

When we know the run time is Friday, we can schedule the instance to 6
upvoted 2 times

 **Josantru** 4 months ago

Correct B.

upvoted 3 times

A company is creating a REST API. The company has strict requirements for the use of TLS. The company requires TLSv1.3 on the API endpoints. The company also requires a specific public third-party certificate authority (CA) to sign the TLS certificate.

Which solution will meet these requirements?

- A. Use a local machine to create a certificate that is signed by the third-party CA import the certificate into AWS Certificate Manager (ACM). Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
- B. Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
- C. Use AWS Certificate Manager (ACM) to create a certificate that is signed by the third-party CA. Import the certificate into AWS Certificate Manager (ACM). Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.
- D. Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.

Correct Answer: A

Community vote distribution

A (52%)

B (48%)

✉  **luiscc**  4 months ago

Selected Answer: B

AWS Certificate Manager (ACM) is a service that lets you easily provision, manage, and deploy SSL/TLS certificates for use with AWS services and your internal resources. By creating a certificate in ACM that is signed by the third-party CA, the company can meet its requirement for a specific public third-party CA to sign the TLS certificate.

upvoted 8 times

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

Selected Answer: A

I don't understand why some many people vote B. In ACM, you can either request certificate from Amazon CA or import an existing certificate. There is no option in ACM that allow you to request a certificate that can be signed by third party CA.

upvoted 7 times

✉  **markoniz** 2 months, 1 week ago

I fully agree

upvoted 1 times

✉  **wsdasdasdqwdaw** 1 month ago

Hmm AWS is saying:

ACM certificates can be used to establish secure communications across the internet or within an internal network. You can request a publicly trusted certificate directly from ACM (an "ACM certificate") or import a publicly trusted certificate issued by a third party. Self-signed certificates are also supported. To provision your organization's internal PKI, you can issue ACM certificates signed by a private certificate authority (CA) created and managed by AWS Private CA. The CA may either reside in your account or be shared with you by a different account.

<https://docs.aws.amazon.com/acm/latest/userguide/gs.html>

upvoted 3 times

✉  **numark**  1 day, 13 hours ago

Answer is A: Can I import a third-party certificate and use it with AWS services?

Yes. If you want to use a third-party certificate with Amazon CloudFront, Elastic Load Balancing, or Amazon API Gateway, you may import it into ACM using the AWS Management Console, AWS CLI, or ACM APIs. ACM does not manage the renewal process for imported certificates. You can use the AWS Management Console to monitor the expiration dates of an imported certificates and import a new third-party certificate to replace an expiring one.

upvoted 1 times

✉  **TariqKipkemei** 6 days, 23 hours ago

Selected Answer: A

It's 22/Nov/2023 and from the console you cant create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. But you could obtain it externally then import it into ACM.

upvoted 1 times

✉  **Tshring** 1 week, 1 day ago

Selected Answer: B

Option B meets these requirements:

- API Gateway HTTP APIs support TLS 1.3
 - ACM can import certificates signed by third-party CAs
 - API Gateway provides REST APIs
- upvoted 1 times

✉ **NickGordon** 2 weeks, 5 days ago

Selected Answer: A

In ACM you can't create a cert signed by another CA. Dude, try it by yourself. There is no such option!

upvoted 1 times

✉ **chen0305_099** 3 months, 1 week ago

WHY NOT A?

upvoted 1 times

✉ **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

Use ACM to create a certificate signed by the third-party CA. ACM integrates with external CAs.

Create an API Gateway HTTP API with a custom domain name.

Configure the custom domain to use the ACM certificate. API Gateway supports configuring custom domains with ACM certificates. This allows serving the API over TLS using the required third-party certificate and TLS 1.3 support.

upvoted 2 times

✉ **taustin2** 3 months, 2 weeks ago

Selected Answer: A

You can provide certificates for your integrated AWS services either by issuing them directly with ACM or by importing third-party certificates into the ACM management system.

upvoted 1 times

✉ **vini15** 3 months, 2 weeks ago

Should be A.

We need to import third-party certificate to ACM.

upvoted 4 times

✉ **darkknight23** 3 months, 3 weeks ago

Selected Answer: A

I am not sure between A and B. I think A makes more sense, as the only way to do it in ACM is to import it and not create it.

upvoted 2 times

✉ **mrsoa** 3 months, 3 weeks ago

Why not A?

B : Everything looks logic but we need a specific public CA to sign the certificate, I am not sure if we all the CAs in the ACM
C and D are not correct because we need API gateway for the HTTP

upvoted 2 times

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

What's the difference between B and C?

upvoted 1 times

✉ **czyboi** 3 months, 2 weeks ago

Lambda function URL does not support REST

upvoted 1 times

✉ **RaksAWS** 4 months ago

correct answer B

upvoted 2 times

✉ **Josantru** 4 months ago

Correct C

upvoted 1 times

A company runs an application on AWS. The application receives inconsistent amounts of usage. The application uses AWS Direct Connect to connect to an on-premises MySQL-compatible database. The on-premises database consistently uses a minimum of 2 GiB of memory.

The company wants to migrate the on-premises database to a managed AWS service. The company wants to use auto scaling capabilities to manage unexpected workload increases.

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

- A. Provision an Amazon DynamoDB database with default read and write capacity settings.
- B. Provision an Amazon Aurora database with a minimum capacity of 1 Aurora capacity unit (ACU).
- C. Provision an Amazon Aurora Serverless v2 database with a minimum capacity of 1 Aurora capacity unit (ACU).
- D. Provision an Amazon RDS for MySQL database with 2 GiB of memory.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Guru4Cloud**  3 months, 1 week ago

Selected Answer: C

The key reasons:

Aurora Serverless v2 provides auto-scaling so the database can handle inconsistent workloads and spikes automatically without admin intervention.

It can scale down to zero when not in use to minimize costs.

The minimum 1 ACU capacity is sufficient to replace the on-prem 2 GiB database based on the info given.

Serverless capabilities reduce admin overhead for capacity management.

DynamoDB lacks MySQL compatibility and requires more hands-on management.

RDS and provisioned Aurora require manually resizing instances to scale, increasing admin overhead.

upvoted 6 times

✉  **TariqKipkemei**  6 days, 23 hours ago

Selected Answer: C

LEAST administrative overhead = Serverless

upvoted 1 times

✉  **kambarami** 2 months, 1 week ago

the questions are hard from 500 +

upvoted 3 times

✉  **ibu007** 3 months, 2 weeks ago

Selected Answer: C

serverless = LEAST overhead

upvoted 2 times

✉  **D10SJoker** 3 months, 3 weeks ago

Why not D?

upvoted 1 times

✉  **mrsoa** 3 months, 3 weeks ago

Selected Answer: C

C seems to be the right answer

Instead of provisioning and managing database servers, you specify Aurora capacity units (ACUs). Each ACU is a combination of approximately 2 gigabytes (GB) of memory, corresponding CPU, and networking. Database storage automatically scales from 10 gibibytes (GiB) to 128 tebibytes (TiB), the same as storage in a standard Aurora DB cluster

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v1.how-it-works.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.html>

upvoted 1 times

✉  **Bmaster** 3 months, 4 weeks ago

C is correct.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html#aurora-serverless-v2.how-it-works.capacity>
upvoted 2 times

A company wants to use an event-driven programming model with AWS Lambda. The company wants to reduce startup latency for Lambda functions that run on Java 11. The company does not have strict latency requirements for the applications. The company wants to reduce cold starts and outlier latencies when a function scales up.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure Lambda provisioned concurrency.
- B. Increase the timeout of the Lambda functions.
- C. Increase the memory of the Lambda functions.
- D. Configure Lambda SnapStart.

Correct Answer: C

Community vote distribution

D (100%)

✉  **Guru4Cloud**  3 months, 1 week ago

Selected Answer: D

The key reasons:

SnapStart keeps functions initialized and ready to respond quickly, eliminating cold starts.
 SnapStart is optimized for applications without aggressive latency needs, reducing costs.
 It scales automatically to match traffic spikes, eliminating outliers when scaling up.
 SnapStart is a native Lambda feature with no additional charges, keeping costs low.
 Provisioned concurrency incurs charges for always-on capacity reserved. More costly than SnapStart.
 Increasing timeout and memory do not directly improve startup performance like SnapStart.

upvoted 7 times

✉  **TariqKipkemei**  6 days, 23 hours ago

Selected Answer: D

Lambda SnapStart it is.

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html#:~:text=RSS-,Lambda%20SnapStart,-for%20Java%20can>
 upvoted 1 times

✉  **TariqKipkemei** 6 days, 23 hours ago

only because its a Java 11 app...if it were any other besides Java I believe Provisioned concurrency could help.

upvoted 1 times

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: D

Lambda SnapStart for Java can improve startup performance for latency-sensitive applications by up to 10x at no extra cost, typically with no changes to your function code.

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>
 upvoted 1 times

✉  **BrijMohan08** 3 months ago

Selected Answer: D

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>
 upvoted 1 times

✉  **skyphilip** 3 months, 1 week ago

Selected Answer: D

D is correct

Lambda SnapStart for Java can improve startup performance for latency-sensitive applications by up to 10x at no extra cost, typically with no changes to your function code. The largest contributor to startup latency (often referred to as cold start time) is the time that Lambda spends initializing the function, which includes loading the function's code, starting the runtime, and initializing the function code.

With SnapStart, Lambda initializes your function when you publish a function version. Lambda takes a Firecracker microVM snapshot of the memory and disk state of the initialized execution environment, encrypts the snapshot, and caches it for low-latency access. When you invoke the function version for the first time, and as the invocations scale up, Lambda resumes new execution environments from the cached snapshot instead of initializing them from scratch, improving startup latency.

upvoted 1 times

 **anikety123** 3 months, 1 week ago

Selected Answer: D

Both Lambda SnapStart and provisioned concurrency can reduce cold starts and outlier latencies when a function scales up. SnapStart helps you improve startup performance by up to 10x at no extra cost. Provisioned concurrency keeps functions initialized and ready to respond in double-digit milliseconds. Configuring provisioned concurrency incurs charges to your AWS account. Use provisioned concurrency if your application has strict cold start latency requirements. You can't use both SnapStart and provisioned concurrency on the same function version.

upvoted 3 times

 **avkya** 3 months, 2 weeks ago

"SnapStart does not support provisioned concurrency, the arm64 architecture, Amazon Elastic File System (Amazon EFS), or ephemeral storage greater than 512 MB." The question says "The company wants to reduce cold starts" This means provisioned concurrency. I'm a little bit confused with D.

upvoted 2 times

 **Woodlawn5700** 3 months, 3 weeks ago

D

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: D

D is the answer

Lambda SnapStart for Java can improve startup performance for latency-sensitive applications by up to 10x at no extra cost, typically with no changes to your function code. The largest contributor to startup latency (often referred to as cold start time) is the time that Lambda spends initializing the function, which includes loading the function's code, starting the runtime, and initializing the function code.

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

upvoted 2 times

 **Bmaster** 3 months, 4 weeks ago

D is best!!

A is not MOST cost effectively.

lambda snapshot is new feature for lambda.

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

upvoted 2 times

 **Bmaster** 3 months, 4 weeks ago

misspell.... lambda snapstart

upvoted 1 times

 **RaksAWS** 4 months ago

why not D

It should work

upvoted 2 times

A financial services company launched a new application that uses an Amazon RDS for MySQL database. The company uses the application to track stock market trends. The company needs to operate the application for only 2 hours at the end of each week. The company needs to optimize the cost of running the database.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the existing RDS for MySQL database to an Aurora Serverless v2 MySQL database cluster.
- B. Migrate the existing RDS for MySQL database to an Aurora MySQL database cluster.
- C. Migrate the existing RDS for MySQL database to an Amazon EC2 instance that runs MySQL. Purchase an instance reservation for the EC2 instance.
- D. Migrate the existing RDS for MySQL database to an Amazon Elastic Container Service (Amazon ECS) cluster that uses MySQL container images to run tasks.

Correct Answer: A

Community vote distribution

A (79%) B (21%)

✉️  **TariqKipkemei** 6 days, 23 hours ago

Selected Answer: A

Answer is A.

Here are the key distinctions:

Amazon Aurora: provides built-in security, continuous backups, serverless compute, up to 15 read replicas, automated multi-Region replication, and integrations with other AWS services.

Amazon Aurora Serverless: is an on-demand, auto-scaling configuration for Aurora where the database automatically starts up, shuts down, and scales capacity up or down based on your application's needs.

With serverless the db will shut down when not in use.

upvoted 2 times

✉️  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

The key reasons are:

Aurora Serverless v2 scales compute capacity automatically based on actual usage, down to zero when not in use. This minimizes costs for intermittent usage.

Since it only runs for 2 hours per week, the application is ideal for a serverless architecture like Aurora Serverless.

Aurora Serverless v2 charges per second when the database is active, unlike RDS which charges hourly.

Aurora Serverless provides higher availability than self-managed MySQL on EC2 or ECS.

Using reserved EC2 instances or ECS still incurs charges when not in use versus the fine-grained scaling of serverless.

Standard Aurora clusters have a minimum capacity unlike the auto-scaling serverless architecture.

upvoted 4 times

✉️  **anikety123** 3 months, 1 week ago

Selected Answer: A

Option is A

upvoted 2 times

✉️  **hachiri** 3 months, 1 week ago

Selected Answer: A

Aurora Serverless

- Automated database instantiation and auto-scaling based on actual usage
- Good for infrequent, intermittent or unpredictable workloads
- No capacity planning needed
- Pay per second, can be more cost-effective

upvoted 2 times

✉️  **vini15** 3 months, 2 weeks ago

will go with A

Amazon Aurora Serverless v2 is suitable for the most demanding, highly variable workloads. For example, your database usage might be heavy for a short period of time, followed by long periods of light activity or no activity at all.

upvoted 2 times

 **msdnpro** 3 months, 3 weeks ago

Selected Answer: A

"Amazon Aurora Serverless v2 is suitable for the most demanding, highly variable workloads. For example, your database usage might be heavy for a short period of time, followed by long periods of light activity or no activity at all."

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html>

upvoted 1 times

 **ersin13** 3 months, 3 weeks ago

A. Migrate the existing RDS for MySQL database to an Aurora Serverless v2 MySQL database cluster.

upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: B

B seems to be the correct answer, because if we have a predictable workload Aurora database seems to be most cost effective however if we have unpredictable workload aurora serverless seems to be more cost effective because our database will scale up and down

for more informations please read this article

<https://medium.com/trackit/aurora-or-aurora-serverless-v2-which-is-more-cost-effective-bcd12e172dcf>

upvoted 3 times

 **Chef_couincouin** 2 weeks, 4 days ago

according to the link, i understand that Aurora Serverless is ideal for sudden peaks in database usage with moderate or minimal usage during other periods of the day. So Answear is A

upvoted 1 times

 **Smart** 3 months ago

True but due to autoscaling - it will be cheaper...check example#1 in the your link.

upvoted 1 times

 **Smart** 3 months ago

Correct Answer is A

upvoted 1 times

A company deploys its applications on Amazon Elastic Kubernetes Service (Amazon EKS) behind an Application Load Balancer in an AWS Region. The application needs to store data in a PostgreSQL database engine. The company wants the data in the database to be highly available. The company also needs increased capacity for read workloads.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Create an Amazon DynamoDB database table configured with global tables.
- B. Create an Amazon RDS database with Multi-AZ deployments.
- C. Create an Amazon RDS database with Multi-AZ DB cluster deployment.
- D. Create an Amazon RDS database configured with cross-Region read replicas.

Correct Answer: B

Community vote distribution

C (100%)

 **TariqKipkemei** 6 days, 22 hours ago

Selected Answer: C

Multi-AZ DB cluster deployments provides two readable DB instances if you need additional read capacity
upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

C is correct
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

RDS Multi-AZ DB cluster deployments provide high availability, automatic failover, and increased read capacity.
A multi-AZ cluster automatically handles replicating data across AZs in a single region.
This maintains operational efficiency as it is natively managed by RDS without needing external replication.
DynamoDB global tables involve complex provisioning and requires app changes.
RDS read replicas require manual setup and management of replication.
RDS Multi-AZ clustering is purpose-built by AWS for HA PostgreSQL deployments and balancing read workloads.
upvoted 3 times

 **avkya** 3 months, 2 weeks ago

Selected Answer: C

Multi-AZ DB clusters provide high availability, increased capacity for read workloads, and lower write latency when compared to Multi-AZ DB instance deployments.
upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: C

CCCCCCCCC_cCC_cCCCCccccCc
upvoted 1 times

 **luiscc** 3 months, 4 weeks ago

Selected Answer: C

DB cluster deployment can scale read workloads by adding read replicas. This provides increased capacity for read workloads without impacting the write workload.
upvoted 4 times

A company is building a RESTful serverless web application on AWS by using Amazon API Gateway and AWS Lambda. The users of this web application will be geographically distributed, and the company wants to reduce the latency of API requests to these users.

Which type of endpoint should a solutions architect use to meet these requirements?

- A. Private endpoint
- B. Regional endpoint
- C. Interface VPC endpoint
- D. Edge-optimized endpoint

Correct Answer: D

Community vote distribution

D (100%)

 **TariqKipkemei** 6 days, 22 hours ago

Selected Answer: D

An edge-optimized API endpoint typically routes requests to the nearest CloudFront Point of Presence (POP), which could help in cases where your clients are geographically distributed. This is the default endpoint type for API Gateway REST APIs.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-endpoint-types.html#:~:text=API%20endpoint%20typically,-routes,-requests%20to%20the>
upvoted 1 times

 **dilaaziz** 3 weeks, 1 day ago

Selected Answer: D

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-endpoint-types.html>
upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: D

An edge-optimized API endpoint typically routes requests to the nearest CloudFront Point of Presence (POP), which could help in cases where your clients are geographically distributed. This is the default endpoint type for API Gateway REST APIs.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-endpoint-types.html>
upvoted 3 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: D

Edge-optimized endpoint
upvoted 2 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: D

The correct answer is D

API Gateway - Endpoint Types

- Edge-Optimized (default): For global clients
 - Requests are routed through the CloudFront Edge locations (improves latency)
 - The API Gateway still lives in only one region
 - Regional:
 - For clients within the same region
 - Could manually combine with CloudFront (more control over the caching strategies and the distribution)
 - Private:
 - Can only be accessed from your VPC using an interface VPC endpoint (ENI)
 - Use a resource policy to define access
- upvoted 3 times

 **Josantru** 4 months ago

Correct D.

Edge-optimized API endpoints

An edge-optimized API endpoint is best for geographically distributed clients. API requests are routed to the nearest CloudFront Point of Presence (POP). This is the default endpoint type for API Gateway REST APIs.

upvoted 2 times

A company uses an Amazon CloudFront distribution to serve content pages for its website. The company needs to ensure that clients use a TLS certificate when accessing the company's website. The company wants to automate the creation and renewal of the TLS certificates.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Use a CloudFront security policy to create a certificate.
- B. Use a CloudFront origin access control (OAC) to create a certificate.
- C. Use AWS Certificate Manager (ACM) to create a certificate. Use DNS validation for the domain.
- D. Use AWS Certificate Manager (ACM) to create a certificate. Use email validation for the domain.

Correct Answer: D

Community vote distribution

C (100%)

 **Bmaster** Highly Voted 3 months, 4 weeks ago

C is correct.

"ACM provides managed renewal for your Amazon-issued SSL/TLS certificates. This means that ACM will either renew your certificates automatically (if you are using DNS validation), or it will send you email notices when expiration is approaching. These services are provided for both public and private ACM certificates."

<https://docs.aws.amazon.com/acm/latest/userguide/managed-renewal.html>
upvoted 5 times

 **ibu007** Most Recent 2 months, 3 weeks ago

Selected Answer: C

Use AWS Certificate Manager (ACM) to create a certificate. Use DNS validation for the domain
upvoted 2 times

 **chen0305_099** 3 months, 1 week ago

Selected Answer: C

C 似乎是正確的
upvoted 3 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

The key reasons are:

AWS Certificate Manager (ACM) provides free public TLS/SSL certificates and handles certificate renewals automatically.
Using DNS validation with ACM is operationally efficient since it automatically makes changes to Route 53 rather than requiring manual validation steps.
ACM integrates natively with CloudFront distributions for delivering HTTPS content.
CloudFront security policies and origin access controls do not issue TLS certificates.
Email validation requires manual steps to approve the domain validation emails for each renewal.
upvoted 4 times

 **Kiki_Pass** 3 months, 3 weeks ago

Selected Answer: C

"DNS Validation is preferred for automation purposes" -- Stephane's course on Udemy
upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: C

C seems to be correct
upvoted 1 times

 **nananashi** 3 months, 4 weeks ago

I think the general product uses DNS rather than email to automate, is the given answer correct?
upvoted 1 times

A company deployed a serverless application that uses Amazon DynamoDB as a database layer. The application has experienced a large increase in users. The company wants to improve database response time from milliseconds to microseconds and to cache requests to the database.

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

- A. Use DynamoDB Accelerator (DAX).
- B. Migrate the database to Amazon Redshift.
- C. Migrate the database to Amazon RDS.
- D. Use Amazon ElastiCache for Redis.

Correct Answer: A

Community vote distribution

A (92%) 8%

✉  **h8er**  3 months, 3 weeks ago

Selected Answer: A

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for Amazon DynamoDB that delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second.

[https://aws.amazon.com/dynamodb/dax/#:~:text=Amazon%20DynamoDB%20Accelerator%20\(DAX\)%20is,millions%20of%20requests%20per%20second](https://aws.amazon.com/dynamodb/dax/#:~:text=Amazon%20DynamoDB%20Accelerator%20(DAX)%20is,millions%20of%20requests%20per%20second).

upvoted 8 times

✉  **TariqKipkemei**  6 days, 22 hours ago

Selected Answer: A

improve DynamoDB response time from milliseconds to microseconds and to cache requests to the database = DynamoDB Accelerator (DAX)

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

Use DynamoDB Accelerator (DAX).

upvoted 1 times

✉  **mrsoa** 3 months, 3 weeks ago

Selected Answer: A

A is the right answer

upvoted 2 times

✉  **Bmaster** 3 months, 4 weeks ago

Correct A.

upvoted 1 times

A company runs an application that uses Amazon RDS for PostgreSQL. The application receives traffic only on weekdays during business hours. The company wants to optimize costs and reduce operational overhead based on this usage.

Which solution will meet these requirements?

- A. Use the Instance Scheduler on AWS to configure start and stop schedules.
- B. Turn off automatic backups. Create weekly manual snapshots of the database.
- C. Create a custom AWS Lambda function to start and stop the database based on minimum CPU utilization.
- D. Purchase All Upfront reserved DB instances.

Correct Answer: C

Community vote distribution

A (90%) 10%

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: A

The Instance Scheduler on AWS solution automates the starting and stopping of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS) instances.

This solution helps reduce operational costs by stopping resources that are not in use and starting them when they are needed. The cost savings can be significant if you leave all of your instances running at full utilization continuously.

<https://aws.amazon.com/solutions/implementations/instance-scheduler-on-aws/>

upvoted 1 times

✉  **ibu007** 2 months, 3 weeks ago

Selected Answer: A

A. Use the Instance Scheduler on AWS to configure start and stop schedules

upvoted 2 times

✉  **baba365** 2 months ago

Why not D?

upvoted 2 times

✉  **ErnShm** 2 months, 3 weeks ago

A

<https://docs.aws.amazon.com/solutions/latest/instance-scheduler-on-aws/solution-overview.html>

upvoted 1 times

✉  **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

Purpose-built scheduling minimizes operational overhead.

Aligns instance running time precisely with business hour demands.

Maintains backups unlike disabling auto backups.

More cost effective and flexible than reserved instances.

Simpler to implement than a custom Lambda function.

upvoted 2 times

✉  **anikety123** 3 months, 1 week ago

Selected Answer: B

Its B. Check the AWS link

https://aws.amazon.com/solutions/implementations/instance-scheduler-on-aws/?nc1=h_ls

upvoted 1 times

✉  **anikety123** 3 months, 1 week ago

Sorry I wanted to select A.

upvoted 2 times

✉  **mrsoa** 3 months, 3 weeks ago

Selected Answer: A

A

<https://aws.amazon.com/solutions/implementations/instance-scheduler-on-aws/>

upvoted 1 times

 **luiscc** 4 months ago

Selected Answer: A

Scheduler do the job

upvoted 3 times

A company uses locally attached storage to run a latency-sensitive application on premises. The company is using a lift and shift method to move the application to the AWS Cloud. The company does not want to change the application architecture.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for Lustre file system to run the application.
- B. Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP2 volume to run the application.
- C. Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for OpenZFS file system to run the application.
- D. Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP3 volume to run the application.

Correct Answer: B

Community vote distribution

D (100%)

 **TariqKipkemei** 6 days, 22 hours ago

Selected Answer: D

MOST cost-effectively =GP3

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: D

gp3 offers SSD-performance at a 20% lower cost per GB than gp2 volumes.

upvoted 1 times

 **bojila** 2 months, 4 weeks ago

GP3 is the lastest version

upvoted 1 times

 **Hades2231** 3 months ago

Selected Answer: D

GP3 is the lastest version, and it is cost effective

upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: D

GP3 is preferable over GP2, FSx for Lustre, and FSx for OpenZFS is clear and convincing:

GP3 offers identical latency performance to GP2 at a lower price point.

FSx options are higher performance but more expensive and require application changes.

GP3 aligns better with lift and shift needs as a directly attached block storage volume.

upvoted 2 times

 **taustin2** 3 months, 2 weeks ago

Selected Answer: D

Migrate your Amazon EBS volumes from gp2 to gp3 and save up to 20% on costs.

upvoted 2 times

 **Vadbro7** 3 months, 2 weeks ago

Y not gp2

upvoted 1 times

 **Ale1973** 3 months, 3 weeks ago

Selected Answer: D

My rational:

Options A y C are based on autoscaling-group and no make sense for me on this scenary.

Then, use Amazon EBS is the solution and GP2 or GP3 is the question.

Requirement requires the most COST effective solution, then, I choose GP3

upvoted 2 times

A company runs a stateful production application on Amazon EC2 instances. The application requires at least two EC2 instances to always be running.

A solutions architect needs to design a highly available and fault-tolerant architecture for the application. The solutions architect creates an Auto Scaling group of EC2 instances.

Which set of additional steps should the solutions architect take to meet these requirements?

- A. Set the Auto Scaling group's minimum capacity to two. Deploy one On-Demand Instance in one Availability Zone and one On-Demand Instance in a second Availability Zone.
- B. Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two On-Demand Instances in a second Availability Zone.
- C. Set the Auto Scaling group's minimum capacity to two. Deploy four Spot Instances in one Availability Zone.
- D. Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two Spot Instances in a second Availability Zone.

Correct Answer: D

Community vote distribution

B (67%)

A (33%)

 **luiscc** Highly Voted 4 months ago

Selected Answer: B

By setting the Auto Scaling group's minimum capacity to four, the architect ensures that there are always at least two running instances. Deploying two On-Demand Instances in each of two Availability Zones ensures that the application is highly available and fault-tolerant. If one Availability Zone becomes unavailable, the application can still run in the other Availability Zone.

upvoted 10 times

 **Ale1973** Highly Voted 3 months, 3 weeks ago

Selected Answer: A

My rational is: Highly available = 2 AZ, and then 2 EC2 instances always running is 1 EC2 in each AZ. If an entire AZ fails, SacalinGroup deploy the minimun instances (2) on the running AZ

upvoted 8 times

 **baba365** 2 months ago

Ans: A.

The application requires at least two EC2 instances to always be running = 2 minimum capacity... minimum cap of 4 ec2 will work but a waste of resources that doesn't follow well archi. framework.

upvoted 1 times

 **Ramdi1** 1 month, 3 weeks ago

it says always have to have two running, hence you need 4. two in each AV. it might be a waste of resource but if that what is required by the company then so be it. Also you out the 4 you cannot use spot instances because if the two instances on the on demand go down and you need to use the spot instance they could be called back at any point.

upvoted 3 times

 **Ramdi1** 1 month, 3 weeks ago

AZ * not AV

upvoted 1 times

 **1rob** Most Recent 1 day, 16 hours ago

Selected Answer: B

From <<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-best-practices.html>> : Spot Instances are not suitable for workloads that are inflexible, stateful, fault-intolerant, or tightly coupled between instance nodes. So C and D don't fit.

From <<https://docs.aws.amazon.com/whitepapers/latest/real-time-communication-on-aws/use-multiple-availability-zones.html>> : Within the constructs of AWS, customers are encouraged to run their workloads in more than one Availability Zone. This ensures that customer applications can withstand even a complete Availability Zone failure - a very rare event in itself.

So a HA solution in this case implies a total of 4 instances, 2 per AZ.

upvoted 1 times

 **TariqKipkemei** 6 days, 1 hour ago

Selected Answer: B

The main requirement here is a 'highly available and fault-tolerant architecture for the application', this covered by option B. The application requires at least two EC2 instances to always be running, main word here being 'atleast' which means more than two is ok.
upvoted 1 times

 **Ramdi1** 1 month, 3 weeks ago

Selected Answer: B

B - Need 2 in each AZ and you cant use spot instances as it could be recalled.
upvoted 1 times

 **Mandar15** 1 month, 4 weeks ago

Selected Answer: B

Stateful is keyword here. 2 is minimum required all time.
upvoted 1 times

 **MII1975** 2 months, 3 weeks ago

Selected Answer: A

If a complete AZ fails, autoscale will launch a second EC2 in the running AZ. If that short period of time is not always, which is not, then the answer is B, but I would take my chances and select A in the exam xD because the application is highly available and fault-tolerant.
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: B

- Minimum of 4 ensures at least 2 instances are always running in each AZ, meeting the HA requirement.
 - On-Demand instances provide consistent performance and availability, unlike Spot.
 - Spreading across 2 AZs adds fault tolerance, protecting from AZ failure.
- upvoted 2 times

 **darkknight23** 3 months, 3 weeks ago

Selected Answer: B

While Spot Instances can be used to reduce costs, they might not provide the same level of availability and guaranteed uptime that On-Demand Instances offer. So I will go with B and not D.
upvoted 1 times

 **Sat897** 3 months, 3 weeks ago

Selected Answer: B

Highly available - 2 AZ and then 2 EC2 instances always running. 2 in each AZ.
upvoted 1 times

 **Sat897** 3 months, 3 weeks ago

Highly available - 2 AZ and then 2 EC2 instances always running. 2 in each AZ..
upvoted 1 times

An ecommerce company uses Amazon Route 53 as its DNS provider. The company hosts its website on premises and in the AWS Cloud. The company's on-premises data center is near the us-west-1 Region. The company uses the eu-central-1 Region to host the website. The company wants to minimize load time for the website as much as possible.

Which solution will meet these requirements?

- A. Set up a geolocation routing policy. Send the traffic that is near us-west-1 to the on-premises data center. Send the traffic that is near eu-central-1 to eu-central-1.
- B. Set up a simple routing policy that routes all traffic that is near eu-central-1 to eu-central-1 and routes all traffic that is near the on-premises datacenter to the on-premises data center.
- C. Set up a latency routing policy. Associate the policy with us-west-1.
- D. Set up a weighted routing policy. Split the traffic evenly between eu-central-1 and the on-premises data center.

Correct Answer: A

Community vote distribution

A (86%) 14%

 **TariqKipkemei** 6 days, 1 hour ago

Selected Answer: A

Geolocation routing policy allows you to route traffic based on the location of your users.
upvoted 1 times

 **t0nx** 6 days, 14 hours ago

Selected Answer: C

C. Set up a latency routing policy. Associate the policy with us-west-1.

Explanation:

A latency routing policy directs traffic based on the lowest network latency to the specified AWS endpoint. Since the on-premises data center is near the us-west-1 Region, associating the policy with us-west-1 ensures that users near that region will be directed to the on-premises data center.

This allows for optimal routing, minimizing the load time for users based on their geographical proximity to the respective hosting locations (us-west-1 and eu-central-1).

Options A, B, and D do not explicitly consider latency or are not optimal for minimizing load time:

Option A (geolocation routing policy) would direct traffic based on the geographic location of the user but may not necessarily optimize for the lowest latency.
upvoted 1 times

 **Chiquitabandita** 1 week, 2 days ago

except I don't think that it should be applied to the west region. If Geolocation is applied and the west is closer to the client, but the west is having intermittent issues at the time, they will have a longer latency even though closer to that region. this is why I would apply latency in a real world solution.
upvoted 1 times

 **Chiquitabandita** 1 week, 2 days ago

in real world I think it should use latency routing if the main concern is to lower the latency but AWS likes to promote geolocation and if that is in the question I think that will be the answer so I choose A.
upvoted 1 times

 **baba365** 2 months ago

The company wants to minimize load time for the website as much as possible... between data Centre and website or between users and website?
upvoted 1 times

 **Hades2231** 3 months ago

Selected Answer: A

Geolocation is the key word
upvoted 1 times

 **lemur88** 3 months ago

Selected Answer: A

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy-geo.html>
upvoted 1 times

✉ **Guru4Cloud** 3 months, 1 week ago

Selected Answer: A

The key reasons are:

Geolocation routing allows you to route users to the closest endpoint based on their geographic location. This will provide the lowest latency.
Routing us-west-1 traffic to the on-premises data center minimizes latency for those users since it is also located near there.
Routing eu-central-1 traffic to the eu-central-1 AWS region minimizes latency for users nearby.
This achieves routing users to the closest endpoint on a geographic basis to optimize for low latency.

upvoted 3 times

✉ **PLN6302** 3 months ago

why can't be the option C

upvoted 1 times

✉ **lemur88** 3 months ago

You cannot associate the policy to us-west-1 as the AWS account is in eu-central-1

upvoted 3 times

A company has 5 PB of archived data on physical tapes. The company needs to preserve the data on the tapes for another 10 years for compliance purposes. The company wants to migrate to AWS in the next 6 months. The data center that stores the tapes has a 1 Gbps uplink internet connectivity.

Which solution will meet these requirements MOST cost-effectively?

- A. Read the data from the tapes on premises. Stage the data in a local NFS storage. Use AWS DataSync to migrate the data to Amazon S3 Glacier Flexible Retrieval.
- B. Use an on-premises backup application to read the data from the tapes and to write directly to Amazon S3 Glacier Deep Archive.
- C. Order multiple AWS Snowball devices that have Tape Gateway. Copy the physical tapes to virtual tapes in Snowball. Ship the Snowball devices to AWS. Create a lifecycle policy to move the tapes to Amazon S3 Glacier Deep Archive.
- D. Configure an on-premises Tape Gateway. Create virtual tapes in the AWS Cloud. Use backup software to copy the physical tape to the virtual tape.

Correct Answer: C

Community vote distribution

C (95%)	5%
---------	----

✉️  **adeyinkaamole** Highly Voted 3 months ago

If you have made it to the end of the exam dump, you will definitely pass your exams in Jesus name. After over a year of Procrastination, I am finally ready to write my AWS Solutions Architect Exam. Thank you Exam Topics
upvoted 9 times

✉️  **Hades2231** Highly Voted 3 months ago

Selected Answer: C

Ready for the exam tomorrow. Wish you guys all the best. BTW Snowball Device comes in handy when you need to move a huge amount of data but cant afford any bandwidth loss
upvoted 7 times

✉️  **TariqKipkemei** Most Recent 6 days, 1 hour ago

Selected Answer: C

Migrate petabyte-scale data stored on physical tapes to AWS using AWS Snowball
<https://aws.amazon.com/snowball/#:~:text=Migrate,-,petabyte%2Dscale,-,data%20stored%20on>
upvoted 1 times

✉️  **hungta** 1 week, 5 days ago

Selected Answer: C

5 PB data is too huge for using 1Gbps uplink. With this uplink, it takes more than 1 year to migrate this data.
upvoted 1 times

✉️  **baba365** 2 months ago

Answer: D for most cost effective.

If you are looking for a cost-effective, durable, long-term, offsite alternative for data archiving, deploy a Tape Gateway. With its virtual tape library (VTL) interface, you can use your existing tape-based backup software infrastructure to store data on virtual tape cartridges that you create -

<https://docs.aws.amazon.com/storagegateway/latest/tgw/WhatIsStorageGateway.html>
upvoted 1 times

✉️  **Devsin2000** 2 months ago

D
<https://aws.amazon.com/storagegateway/vtl/>
the bandwidth and available time is ample
upvoted 1 times

✉️  **nnecode** 2 months, 1 week ago

Selected Answer: A

The most cost-effective solution to meet the requirements is to read the data from the tapes on premises. Stage the data in a local NFS storage. Use AWS DataSync to migrate the data to Amazon S3 Glacier Flexible Retrieval.

This solution is the most cost-effective because it uses the least amount of bandwidth. AWS DataSync is a service that transfers data between on-premises storage and Amazon S3. It uses a variety of techniques to optimize the transfer speed and reduce c

upvoted 1 times

 **lemur88** 3 months ago

Selected Answer: C

Only thing that makes sense given the 1Gbps limitation
upvoted 1 times

 **Guru4Cloud** 3 months, 1 week ago

Selected Answer: C

Option C is likely the most cost-effective solution given the large data size and limited internet bandwidth. The physical data transfer and integration with the existing tape infrastructure provides efficiency benefits that can optimize the cost.
upvoted 2 times

 **barracouto** 3 months, 2 weeks ago

Selected Answer: C

Went through this dump twice now. Exam is in about an hour. Will update with results.
upvoted 2 times

 **Vaishali12** 3 months, 1 week ago

how was ur exam?
was these dump que helpful?
upvoted 1 times

 **riccardoto** 3 months, 2 weeks ago

Finished the dump today - taking my exam tomorrow :-) Wish me luck!
upvoted 4 times

 **Ale1973** 3 months, 3 weeks ago

My rational: question is about which solution will meet these requirements MOST cost-effectively, not MOST time or effectively, then, my response is D (using Tape Gateways)
upvoted 4 times

 **D10SJoker** 3 months, 3 weeks ago

Selected Answer: C

For me it's C
upvoted 1 times

 **PrincePazol** 3 months, 3 weeks ago

Selected Answer: C

Taking my exams today
upvoted 1 times

 **mrsoa** 3 months, 3 weeks ago

Selected Answer: C

C is the right answer, because we need atleast 1 year to transfer the data over the internet
upvoted 2 times

 **Deepakin96** 3 months, 3 weeks ago

Selected Answer: C

C is my answer
upvoted 2 times

A company is deploying an application that processes large quantities of data in parallel. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to prevent groups of nodes from sharing the same underlying hardware.

Which networking solution meets these requirements?

- A. Run the EC2 instances in a spread placement group.
- B. Group the EC2 instances in separate accounts.
- C. Configure the EC2 instances with dedicated tenancy.
- D. Configure the EC2 instances with shared tenancy.

Correct Answer: A

Community vote distribution

A (60%)

C (40%)

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

Selected Answer: C

C is the correct answer.

Configuring the EC2 instances with dedicated tenancy ensures that each instance will run on isolated, single-tenant hardware. This meets the requirement to prevent groups of nodes from sharing underlying hardware.

A spread placement group only provides isolation at the Availability Zone level. Instances could still share hardware within an AZ.
upvoted 5 times

✉  **TariqKipkemei**  6 days, 1 hour ago

Selected Answer: A

Keywords 'prevent groups of nodes from sharing the same underlying hardware'.

Spread Placement Group strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

upvoted 1 times

✉  **cciesam** 2 weeks, 2 days ago

Selected Answer: A

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Each instances is placed on seven different racks, each rack has its own network and power source.

upvoted 1 times

✉  **wsdadasdqwdaw** 1 month ago

Another tricky question, but I would go for A because:

Dedicated instances:

Dedicated Instances are EC2 instances that run on hardware that's dedicated to a single customer. Dedicated Instances that belong to different AWS accounts are physically isolated at a hardware level, even if those accounts are linked to a single payer account. However, Dedicated Instances might share hardware with other instances from the same AWS account that are not Dedicated Instances.
Which is not the desired option.

Spread – strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

That's why A.

upvoted 2 times

✉  **garuta** 2 months ago

Selected Answer: C

C is clear.

upvoted 1 times

✉  **Devsin2000** 2 months ago

A

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

upvoted 2 times

✉  **taustin2** 2 months, 1 week ago

Selected Answer: A

Spread Placement Group strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.
upvoted 1 times

 **Eminenza22** 2 months, 4 weeks ago

Selected Answer: A
Option A is the correct answer. It suggests running the EC2 instances in a spread placement group. This solution is cost-effective and requires minimal development effort .

upvoted 2 times

 **Eminenza22** 2 months, 4 weeks ago

The placement group reduces the risk of simultaneous failures by spreading the instances across distinct underlying hardware
upvoted 1 times

 **czyboi** 3 months ago

Selected Answer: A
A spread placement group is a group of instances that are each placed on distinct hardware.
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>
upvoted 4 times

A solutions architect is designing a disaster recovery (DR) strategy to provide Amazon EC2 capacity in a failover AWS Region. Business requirements state that the DR strategy must meet capacity in the failover Region.

Which solution will meet these requirements?

- A. Purchase On-Demand Instances in the failover Region.
- B. Purchase an EC2 Savings Plan in the failover Region.
- C. Purchase regional Reserved Instances in the failover Region.
- D. Purchase a Capacity Reservation in the failover Region.

Correct Answer: C

Community vote distribution

D (88%) 13%

 **TariqKipkemei** 6 days, 1 hour ago

Selected Answer: D

Capacity Reservations mitigate against the risk of being unable to get On-Demand capacity in case there are capacity constraints. If you have strict capacity requirements, and are running business-critical workloads that require a certain level of long or short-term capacity assurance, create a Capacity Reservation to ensure that you always have access to Amazon EC2 capacity when you need it, for as long as you need it.

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: D

Capacity Reservations enable you to reserve capacity for your Amazon EC2 instances in a specific Availability Zone for any duration. This gives you the flexibility to selectively add capacity reservations and still get the Regional RI discounts for that usage. By creating Capacity Reservations, you ensure that you always have access to Amazon EC2 capacity when you need it, for as long as you need it.

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Savings Plans does not provide a capacity reservation.

upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

Capacity Reservations allocate EC2 capacity in a specific AWS Region for you to launch instances.

The capacity is reserved and available to be utilized when needed, meeting the requirement to provide EC2 capacity in the failover region.

Other options do not reserve capacity. On-Demand provides flexible capacity but does not reserve capacity upfront. Savings Plans and Reserved Instances provide discounts but do not reserve capacity.

Capacity Reservations allow defining instance attributes like instance type, platform, Availability Zone so the reserved capacity matches the production environment.

upvoted 2 times

 **Eminenza22** 2 months, 3 weeks ago

Selected Answer: D

A regional Reserved Instance does not reserve capacity

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-scope.html>

upvoted 1 times

 **judyda** 2 months, 3 weeks ago

Selected Answer: D

reserved instances for price discount. need capacity reservation.

upvoted 2 times

 **gispankaj** 2 months, 4 weeks ago

Selected Answer: C

The Reserved Instance discount applies to instance usage within the instance family, regardless of size.

upvoted 1 times

 **ErnShm** 2 months, 4 weeks ago

D

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>

upvoted 1 times

A company has five organizational units (OUs) as part of its organization in AWS Organizations. Each OU correlates to the five businesses that the company owns. The company's research and development (R&D) business is separating from the company and will need its own organization. A solutions architect creates a separate new management account for this purpose.

What should the solutions architect do next in the new management account?

- A. Have the R&D AWS account be part of both organizations during the transition.
- B. Invite the R&D AWS account to be part of the new organization after the R&D AWS account has left the prior organization.
- C. Create a new R&D AWS account in the new organization. Migrate resources from the prior R&D AWS account to the new R&D AWS account.
- D. Have the R&D AWS account join the new organization. Make the new management account a member of the prior organization.

Correct Answer: C

Community vote distribution

B (73%)

C (27%)

 **TariqKipkemei** 6 days, 1 hour ago

Selected Answer: B

As per this document, B is clearly the answer.

<https://repost.aws/knowledge-center/organizations-move-accounts#:~:text=In%20either%20case%2C-,perform%20these%20actions,-for%20each%20member>

upvoted 1 times

 **Joben** 2 months ago

Selected Answer: B

In either case, perform these actions for each member account:

- Remove the member account from the old organization.
- Send an invite to the member account from the new organization.
- Accept the invite to the new organization from the member account.

<https://repost.aws/knowledge-center/organizations-move-accounts>

upvoted 4 times

 **Guru4Cloud** 2 months, 1 week ago

Selected Answer: C

Creating a brand new AWS account in the new organization (Option C) allows for a clean separation and migration of only the necessary resources from the old account to the new.

upvoted 2 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: C

When separating a business unit from an AWS Organizations structure, best practice is to:

- Create a new AWS account dedicated for the business unit in the new organization
 - Migrate resources from the old account to the new account
 - Remove the old account from the original organization
- This allows a clean break between the organizations and avoids any linking between them after separation.

upvoted 1 times

 **ErnShm** 2 months, 4 weeks ago

B

<https://aws.amazon.com/blogs/mt/migrating-accounts-between-aws-organizations-with-consolidated-billing-to-all-features/>

upvoted 2 times

 **gispankaj** 2 months, 4 weeks ago

Selected Answer: B

account can leave current organization and then join new organization.

upvoted 3 times

A company is designing a solution to capture customer activity in different web applications to process analytics and make predictions. Customer activity in the web applications is unpredictable and can increase suddenly. The company requires a solution that integrates with other web applications. The solution must include an authorization step for security purposes.

Which solution will meet these requirements?

- A. Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives in an Amazon Elastic File System (Amazon EFS) file system. Authorization is resolved at the GWLB.
- B. Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis data stream that stores the information that the company receives in an Amazon S3 bucket. Use an AWS Lambda function to resolve authorization.
- C. Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis Data Firehose that stores the information that the company receives in an Amazon S3 bucket. Use an API Gateway Lambda authorizer to resolve authorization.
- D. Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives on an Amazon Elastic File System (Amazon EFS) file system. Use an AWS Lambda function to resolve authorization.

Correct Answer: D

Community vote distribution

C (100%)

 **ralfj**  2 months, 4 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambda-authorizer.html>

upvoted 5 times

 **TariqKipkemei**  6 days, 1 hour ago

Selected Answer: C

Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis Data Firehose that stores the information that the company receives in an Amazon S3 bucket. Use an API Gateway Lambda authorizer to resolve authorization.

upvoted 1 times

 **wsdasdasdqwdaw** 1 month ago

Using ECS just to stores the information is a overkill. So B or C then, lambda authoriser is the key word => C

upvoted 2 times

 **Eminenza22** 2 months, 4 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/lambda/latest/dg/services-kinesisfirehose.html>

upvoted 2 times

 **ErnShm** 2 months, 4 weeks ago

C

authorizer is configured for the method. If it is, API Gateway calls the Lambda function. The Lambda function authenticates the caller by means such as the following: Calling out to an OAuth provider to get an OAuth access token

upvoted 2 times

 **gispankaj** 2 months, 4 weeks ago

Selected Answer: C

lambda authoriser seems to be logical solution.

upvoted 2 times

An ecommerce company wants a disaster recovery solution for its Amazon RDS DB instances that run Microsoft SQL Server Enterprise Edition. The company's current recovery point objective (RPO) and recovery time objective (RTO) are 24 hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a cross-Region read replica and promote the read replica to the primary instance.
- B. Use AWS Database Migration Service (AWS DMS) to create RDS cross-Region replication.
- C. Use cross-Region replication every 24 hours to copy native backups to an Amazon S3 bucket.
- D. Copy automatic snapshots to another Region every 24 hours.

Correct Answer: B

Community vote distribution

D (100%)

 **potomac** 3 weeks, 1 day ago

Selected Answer: D

Amazon RDS creates and saves automated backups of your DB instance or Multi-AZ DB cluster during the backup window of your DB instance. RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. RDS saves the automated backups of your DB instance according to the backup retention period that you specify. If necessary, you can recover your DB instance to any point in time during the backup retention period.

upvoted 1 times

 **wsdasdasdqwdaw** 1 month ago

most cost-effective way is just copying the snapshot (24h delta in the storage). => D

upvoted 2 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

Dddddddddd

upvoted 2 times

 **Eminenza22** 2 months, 3 weeks ago

Selected Answer: D

This is the most cost-effective solution because it does not require any additional AWS services. Amazon RDS automatically creates snapshots of your DB instances every hour. You can copy these snapshots to another Region every 24 hours to meet your RPO and RTO requirements.

The other solutions are more expensive because they require additional AWS services. For example, AWS DMS is a more expensive service than AWS RDS.

upvoted 2 times

 **TiaguteVital** 2 months, 3 weeks ago

Selected Answer: D

Snapshots are always a cost-efficiency way to have a DR plan.

upvoted 2 times

A company runs a web application on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer that has sticky sessions enabled. The web server currently hosts the user session state. The company wants to ensure high availability and avoid user session state loss in the event of a web server outage.

Which solution will meet these requirements?

- A. Use an Amazon ElastiCache for Memcached instance to store the session data. Update the application to use ElastiCache for Memcached to store the session state.
- B. Use Amazon ElastiCache for Redis to store the session state. Update the application to use ElastiCache for Redis to store the session state.
- C. Use an AWS Storage Gateway cached volume to store session data. Update the application to use AWS Storage Gateway cached volume to store the session state.
- D. Use Amazon RDS to store the session state. Update the application to use Amazon RDS to store the session state.

Correct Answer: D

Community vote distribution

B (88%)	12%
---------	-----

 **potomac** 3 weeks, 1 day ago

Selected Answer: B

B is correct

upvoted 1 times

 **franbarberan** 2 months ago

Selected Answer: D

Elastic cache is Only for RDS

upvoted 2 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: B

The key points are:

ElastiCache Redis provides in-memory caching that can deliver microsecond latency for session data.

Redis supports replication and multi-AZ which can provide high availability for the cache.

The application can be updated to store session data in ElastiCache Redis rather than locally on the web servers.

If a web server fails, the user can be routed via the load balancer to another web server which can retrieve their session data from the highly available ElastiCache Redis cluster.

upvoted 4 times

 **gispankaj** 2 months, 4 weeks ago

Selected Answer: B

redis is correct since it provides high availability and data persistance

upvoted 3 times

 **Eminenza22** 2 months, 4 weeks ago

Selected Answer: B

B is the correct answer. It suggests using Amazon ElastiCache for Redis to store the session state. Update the application to use ElastiCache for Redis to store the session state. This solution is cost-effective and requires minimal development effort.

upvoted 3 times

 **czyboi** 3 months ago

Selected Answer: B

high availability => use redis instead of Elastich memcache

upvoted 4 times

A company migrated a MySQL database from the company's on-premises data center to an Amazon RDS for MySQL DB instance. The company sized the RDS DB instance to meet the company's average daily workload. Once a month, the database performs slowly when the company runs queries for a report. The company wants to have the ability to run reports and maintain the performance of the daily workloads.

Which solution will meet these requirements?

- A. Create a read replica of the database. Direct the queries to the read replica.
- B. Create a backup of the database. Restore the backup to another DB instance. Direct the queries to the new database.
- C. Export the data to Amazon S3. Use Amazon Athena to query the S3 bucket.
- D. Resize the DB instance to accommodate the additional workload.

Correct Answer: A

Community vote distribution

A (100%)

 **TariqKipkemei** 5 days, 1 hour ago

Selected Answer: A

queries for reports = read replica
upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: A

Create a read replica of the database. Direct the queries to the read replica.
upvoted 2 times

 **Eminenza22** 2 months, 3 weeks ago

Selected Answer: A

This is the most cost-effective solution because it does not require any additional AWS services. A read replica is a copy of a database that is synchronized with the primary database. You can direct the queries for the report to the read replica, which will not affect the performance of the daily workloads
upvoted 1 times

 **TiaguteVital** 2 months, 3 weeks ago

Selected Answer: A

Clearly the right choice, with a read replica all the queries needed for a report are done in the replica, leaving the primary on best performance for write
upvoted 1 times

A company runs a container application by using Amazon Elastic Kubernetes Service (Amazon EKS). The application includes microservices that manage customers and place orders. The company needs to route incoming requests to the appropriate microservices.

Which solution will meet this requirement MOST cost-effectively?

- A. Use the AWS Load Balancer Controller to provision a Network Load Balancer.
- B. Use the AWS Load Balancer Controller to provision an Application Load Balancer.
- C. Use an AWS Lambda function to connect the requests to Amazon EKS.
- D. Use Amazon API Gateway to connect the requests to Amazon EKS.

Correct Answer: C

Community vote distribution

D (62%)

B (38%)

✉  **1rob** 1 day, 20 hours ago

Selected Answer: B

Routing requests to the appr. microserv. can easily be done with ALB and ingress. The ingress handles routing rules to the micro.serv. With answer D you wil still need ALB or NLB as can be seen in the pics of <https://aws.amazon.com/blogs/containers/integrate-amazon-api-gateway-with-amazon-eks/> or <https://aws.amazon.com/blogs/containers/microservices-development-using-aws-controllers-for-kubernetes-ack-and-amazon-eks-blueprints/> so that is not the most cost-effectively.

upvoted 1 times

✉  **TariqKipkemei** 5 days, 1 hour ago

Selected Answer: D

Both ALB and API gateway can be used to route traffic to the microservices, but the question seeks the most 'cost effective' option.

You are charged for each hour or partial hour that an Application Load Balancer is running, and the number of Load Balancer Capacity Units (LCU) used per hour.

With Amazon API Gateway, you only pay when your APIs are in use.

I say API gateway is the best option for this case.

upvoted 1 times

✉  **t0nx** 6 days, 14 hours ago

Selected Answer: B

AWS Load Balancer Controller: The AWS Load Balancer Controller is a Kubernetes controller that makes it easy to set up an Application Load Balancer (ALB) or Network Load Balancer (NLB) for your Amazon EKS clusters. It simplifies the process of managing load balancers for applications running on EKS.

Application Load Balancer (ALB): ALB is a Layer 7 load balancer that is capable of routing requests based on content, such as URL paths or hostnames. This makes it suitable for routing requests to different microservices based on specific criteria.

Cost-Effectiveness: ALB is typically more cost-effective than an NLB, and it provides additional features at the application layer, which may be useful for routing requests to microservices based on specific conditions.

Option D: Amazon API Gateway is designed for creating, publishing, and managing APIs. While it can integrate with Amazon EKS, it may be more feature-rich and complex than needed for simple routing to microservices within an EKS cluster.

upvoted 1 times

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: D

API Gateway provides an entry point to your microservices.

<https://aws.amazon.com/blogs/containers/integrate-amazon-api-gateway-with-amazon-eks/>

upvoted 1 times

✉  **ccmc** 3 weeks, 3 days ago

B is correct, it is a required before exposing through api gateway

upvoted 1 times

✉  **thanhnv142** 1 month ago

B: is correct.

For EKS, use application load balancer to expose microservices

upvoted 2 times

 **KhasDenis** 2 months ago

Selected Answer: B

Routing to ms in k8s -> Ingresses -> Ingress Controller -> AWS Load Balancer Controller <https://kubernetes-sigs.github.io/aws-load-balancer-controller/v2.6/>
upvoted 3 times

 **RDM10** 2 months, 1 week ago

Microservices--> API--> API GW
upvoted 3 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

D. Use Amazon API Gateway to connect the requests to Amazon EKS.
upvoted 3 times

 **MII1975** 2 months, 3 weeks ago

Selected Answer: D

API Gateway is a fully managed service that makes it easy for you to create, publish, maintain, monitor, and secure APIs at any scale. API Gateway provides an entry point to your microservices.
upvoted 1 times

 **Eminenza22** 2 months, 4 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/containers/microservices-development-using-aws-controllers-for-kubernetes-ack-and-amazon-eks-blueprints/>
upvoted 1 times

 **ralfj** 2 months, 4 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/containers/integrate-amazon-api-gateway-with-amazon-eks/>
upvoted 1 times

A company uses AWS and sells access to copyrighted images. The company's global customer base needs to be able to access these images quickly. The company must deny access to users from specific countries. The company wants to minimize costs as much as possible.

Which solution will meet these requirements?

- A. Use Amazon S3 to store the images. Turn on multi-factor authentication (MFA) and public bucket access. Provide customers with a link to the S3 bucket.
- B. Use Amazon S3 to store the images. Create an IAM user for each customer. Add the users to a group that has permission to access the S3 bucket.
- C. Use Amazon EC2 instances that are behind Application Load Balancers (ALBs) to store the images. Deploy the instances only in the countries the company services. Provide customers with links to the ALBs for their specific country's instances.
- D. Use Amazon S3 to store the images. Use Amazon CloudFront to distribute the images with geographic restrictions. Provide a signed URL for each customer to access the data in CloudFront.

Correct Answer: C

Community vote distribution

D (100%)

 **TariqKipkemei** 5 days, 1 hour ago

Selected Answer: D

Store images = Amazon S3
global customer base needs to be able to access these images quickly = Amazon CloudFront
deny access to users from specific countries = Amazon CloudFront geographic restrictions, signed URLs
upvoted 1 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: D

D. Use Amazon S3 to store the images. Use Amazon CloudFront to distribute the images with geographic restrictions. Provide a signed URL for each customer to access the data in CloudFront.

upvoted 2 times

 **Colz** 2 months, 2 weeks ago

Correct answer is D

upvoted 1 times

 **hubbabubba** 2 months, 3 weeks ago

Selected Answer: D

answer is D
upvoted 1 times

 **Eminenza22** 2 months, 4 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>
upvoted 2 times

 **ralfj** 2 months, 4 weeks ago

Selected Answer: D

Use Cloudfront and geographic restriction
upvoted 4 times

A solutions architect is designing a highly available Amazon ElastiCache for Redis based solution. The solutions architect needs to ensure that failures do not result in performance degradation or loss of data locally and within an AWS Region. The solution needs to provide high availability at the node level and at the Region level.

Which solution will meet these requirements?

- A. Use Multi-AZ Redis replication groups with shards that contain multiple nodes.
- B. Use Redis shards that contain multiple nodes with Redis append only files (AOF) turned on.
- C. Use a Multi-AZ Redis cluster with more than one read replica in the replication group.
- D. Use Redis shards that contain multiple nodes with Auto Scaling turned on.

Correct Answer: A

Community vote distribution

A (63%) C (19%) B (19%)

✉  **TariqKipkemei** 5 days, 1 hour ago

Selected Answer: A

Multi-AZ is only supported on Redis clusters that have more than one node in each shard (node groups).

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html#:~:text=node%20in%20each-,shard,-Topics>
upvoted 1 times

✉  **t0nx** 6 days, 14 hours ago

Selected Answer: C

C. Use a Multi-AZ Redis cluster with more than one read replica in the replication group.

In summary, option C, using a Multi-AZ Redis cluster with more than one read replica, is designed to provide both node-level and AWS Region-level high availability, making it the most suitable choice for the given requirements.

upvoted 1 times

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: A

the replication structure is contained within a shard (called node group in the API/CLI) which is contained within a Redis cluster

A shard (in the API and CLI, a node group) is a hierarchical arrangement of nodes, each wrapped in a cluster. Shards support replication. Within a shard, one node functions as the read/write primary node. All the other nodes in a shard function as read-only replicas of the primary node.

upvoted 1 times

✉  **thanhnv142** 1 month, 1 week ago

C is correct.

Not A because in replication mode, shard have multiple nodes by default.

B and D not correct because that not an option

upvoted 1 times

✉  **iwannabeawsgod** 1 month, 1 week ago

Selected Answer: C

its c for me

upvoted 1 times

✉  **bsbs1234** 1 month, 2 weeks ago

C:

Cluster mode will create multiple shards, when node level failure, request of shard that not impacted will not has any performance impact. If the issue at AZ level, spread traffic between multiple shards shall also reduce the performance degrade.

upvoted 1 times

✉  **loveaws** 1 month, 3 weeks ago

C.

Option A is not ideal because it doesn't mention read replicas, and it's generally better to have read replicas for both performance and high availability.

Option B mentions Redis append-only files (AOF), but AOF alone doesn't provide high availability or fault tolerance.

Option D mentions Auto Scaling, but this doesn't directly address high availability at the Region level or data replication

upvoted 1 times

✉  **taustin2** 2 months ago

Multi-AZ is only supported on Redis clusters that have more than one node in each shard.

upvoted 1 times

✉  **taustin2** 2 months ago

Selected Answer: A

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

upvoted 3 times

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

Selected Answer: A

Multi-AZ replication groups provide automatic failover between AZs if there is an issue with the primary AZ. This provides high availability at the region level

upvoted 2 times

✉  **xyb** 2 months, 2 weeks ago

Selected Answer: C

Enabling ElastiCache Multi-AZ with automatic failover on your Redis cluster (in the API and CLI, replication group) improves your fault tolerance. This is true particularly in cases where your cluster's read/write primary cluster becomes unreachable or fails for any reason. Multi-AZ with automatic failover is only supported on Redis clusters that support replication

upvoted 1 times

✉  **MII1975** 2 months, 3 weeks ago

Selected Answer: A

I would go with A too

I would go with A, Using AOF can't protect you from all failure scenarios.

For example, if a node fails due to a hardware fault in an underlying physical server, ElastiCache will provision a new node on a different server. In this case, the AOF is not available and can't be used to recover the data.

upvoted 1 times

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

Selected Answer: A

Hate to say this, but I read the two docs linked below, and I still think the answer is A. Turning on AOF helps in data persistence after failure, but it does nothing for availability unless you use Multi-AZ replica groups.

upvoted 2 times

✉  **Eminenza22** 2 months, 4 weeks ago

Selected Answer: B

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

upvoted 2 times

✉  **ralfj** 2 months, 4 weeks ago

Selected Answer: B

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

upvoted 1 times

A company plans to migrate to AWS and use Amazon EC2 On-Demand Instances for its application. During the migration testing phase, a technical team observes that the application takes a long time to launch and load memory to become fully productive.

Which solution will reduce the launch time of the application during the next testing phase?

- A. Launch two or more EC2 On-Demand Instances. Turn on auto scaling features and make the EC2 On-Demand Instances available during the next testing phase.
- B. Launch EC2 Spot Instances to support the application and to scale the application so it is available during the next testing phase.
- C. Launch the EC2 On-Demand Instances with hibernation turned on. Configure EC2 Auto Scaling warm pools during the next testing phase.
- D. Launch EC2 On-Demand Instances with Capacity Reservations. Start additional EC2 instances during the next testing phase.

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud**  2 months, 2 weeks ago

Selected Answer: C

Using EC2 hibernation and Auto Scaling warm pools will help address this:

Hibernation saves the in-memory state of the EC2 instance to persistent storage and shuts the instance down. When the instance is started again, the in-memory state is restored, which launches much faster than launching a new instance.

Warm pools pre-initialize EC2 instances and keep them ready to fulfill requests, reducing launch time. The hibernated instances can be added to a warm pool.

When auto scaling scales out during the next testing phase, it will be able to launch instances from the warm pool rapidly since they are already initialized

upvoted 5 times

 **TariqKipkemei**  5 days, 1 hour ago

Selected Answer: C

If an instance or application takes a long time to bootstrap and build a memory footprint in order to become fully productive, you can use hibernation to pre-warm the instance. To pre-warm the instance, you:

Launch it with hibernation enabled.

Bring it to a desired state.

Hibernate it so that it's ready to be resumed to the desired state whenever needed.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html#:~:text=you%20can%20use-,hibernation,-to%20pre%2Dwarm>
upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

With Amazon EC2 hibernation enabled, you can maintain your EC2 instances in a "pre-warmed" state so these can get to a productive state faster.

upvoted 1 times

 **tabbyDolly** 2 months, 1 week ago

C: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html>

upvoted 2 times

 **ralfj** 2 months, 4 weeks ago

Selected Answer: C

just use hibernation option so you won't load the full EC2 Instance

upvoted 1 times

A company's applications run on Amazon EC2 instances in Auto Scaling groups. The company notices that its applications experience sudden traffic increases on random days of the week. The company wants to maintain application performance during sudden traffic increases.

Which solution will meet these requirements MOST cost-effectively?

- A. Use manual scaling to change the size of the Auto Scaling group.
- B. Use predictive scaling to change the size of the Auto Scaling group.
- C. Use dynamic scaling to change the size of the Auto Scaling group.
- D. Use schedule scaling to change the size of the Auto Scaling group.

Correct Answer: C

Community vote distribution

C (100%)

 **TariqKipkemei** 5 days, 1 hour ago

Selected Answer: C

Dynamic scaling
upvoted 1 times

 **dilaaziz** 3 weeks, 6 days ago

Selected Answer: C

<https://aws.amazon.com/ec2/autoscaling/faqs/>
upvoted 1 times

 **tabbyDolly** 2 months, 1 week ago

C - "sudden traffic increases on random days of the week" --> dynamic scaling
upvoted 4 times

 **Guru4Cloud** 2 months, 2 weeks ago

Selected Answer: C

C is the best answer here. Dynamic scaling is the most cost-effective way to automatically scale the Auto Scaling group to maintain performance during random traffic spikes.
upvoted 2 times

 **ralfj** 2 months, 4 weeks ago

Selected Answer: C

Dynamic Scaling – This is yet another type of Auto Scaling in which the number of EC2 instances is changed automatically depending on the signals received. Dynamic Scaling is a good choice when there is a high volume of unpredictable traffic.

<https://www.developer.com/web-services/aws-auto-scaling-types-best-practices/#:~:text=Dynamic%20Scaling%20%E2%80%93%20This%20is%20yet,high%20volume%20of%20unpredictable%20traffic.>
upvoted 3 times

An ecommerce application uses a PostgreSQL database that runs on an Amazon EC2 instance. During a monthly sales event, database usage increases and causes database connection issues for the application. The traffic is unpredictable for subsequent monthly sales events, which impacts the sales forecast. The company needs to maintain performance when there is an unpredictable increase in traffic.

Which solution resolves this issue in the MOST cost-effective way?

- A. Migrate the PostgreSQL database to Amazon Aurora Serverless v2.
- B. Enable auto scaling for the PostgreSQL database on the EC2 instance to accommodate increased usage.
- C. Migrate the PostgreSQL database to Amazon RDS for PostgreSQL with a larger instance type.
- D. Migrate the PostgreSQL database to Amazon Redshift to accommodate increased usage.

Correct Answer: C

Community vote distribution

A (90%) 10%

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

Selected Answer: A

Answer is A.

Aurora Serverless v2 got autoscaling, highly available and cheaper when compared to the other options.

upvoted 5 times

✉  **TariqKipkemei**  1 day, 23 hours ago

Selected Answer: A

Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Aurora where the database automatically starts up, shuts down, and scales capacity up or down based on your application's needs. This is the least costly option for unpredictable traffic.

upvoted 1 times

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

A: "he traffic is unpredictable for subsequent monthly sales events" --> serverless

upvoted 2 times

✉  **Wayne23Fang** 2 months, 3 weeks ago

Selected Answer: C

A is probably more expensive than C. Aurora is serverless and fast. But nevertheless it needs DB migration service. Not sure DMS may not be free.

upvoted 1 times

✉  **danielmakita** 1 month ago

C is more expensive if you think the scenario where the traffic is low. You are paying for a larger hardware but not using it. That's why I think A is correct.

upvoted 1 times

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

Selected Answer: A

A to autoscaling

upvoted 2 times

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

Answer is A.

Aurora Serverless v2 got autoscaling, highly available and cheaper when compared to the other options.

upvoted 1 times

✉  **anikety123** 2 months, 4 weeks ago

Selected Answer: A

The correct answer is A

upvoted 1 times

A company hosts an internal serverless application on AWS by using Amazon API Gateway and AWS Lambda. The company's employees report issues with high latency when they begin using the application each day. The company wants to reduce latency.

Which solution will meet these requirements?

- A. Increase the API Gateway throttling limit.
- B. Set up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day.
- C. Create an Amazon CloudWatch alarm to initiate a Lambda function as a target for the alarm at the beginning of each day.
- D. Increase the Lambda function memory.

Correct Answer: B

Community vote distribution

B (100%)

✉  **TariqKipkemei** 1 day, 23 hours ago

Selected Answer: B

Provisioned concurrency pre-initializes execution environments for your functions. These execution environments are prepared to respond immediately to incoming function requests at start of day.

upvoted 1 times

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: B

A is wrong

API Gateway throttling limit is for better throughput, not for latency

upvoted 1 times

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

Selected Answer: B

Set up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day.

upvoted 3 times

✉  **MII1975** 2 months, 3 weeks ago

Selected Answer: B

Provisioned Concurrency incurs additional costs, so it is cost-efficient to use it only when necessary. For example, early in the morning when activity starts, or to handle recurring peak usage.

upvoted 2 times

✉  **Eminenza22** 2 months, 4 weeks ago

Selected Answer: B

B option setting up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day. This solution is cost-effective and requires minimal development effort.

upvoted 1 times

✉  **oayoade** 3 months ago

Selected Answer: B

<https://aws.amazon.com/blogs/compute/scheduling-aws-lambda-provisioned-concurrency-for-recurring-peak-usage/>

upvoted 3 times

A research company uses on-premises devices to generate data for analysis. The company wants to use the AWS Cloud to analyze the data. The devices generate .csv files and support writing the data to an SMB file share. Company analysts must be able to use SQL commands to query the data. The analysts will run queries periodically throughout the day.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

- A. Deploy an AWS Storage Gateway on premises in Amazon S3 File Gateway mode.
- B. Deploy an AWS Storage Gateway on premises in Amazon FSx File Gateway mode.
- C. Set up an AWS Glue crawler to create a table based on the data that is in Amazon S3.
- D. Set up an Amazon EMR cluster with EMR File System (EMRFS) to query the data that is in Amazon S3. Provide access to analysts.
- E. Set up an Amazon Redshift cluster to query the data that is in Amazon S3. Provide access to analysts.
- F. Setup Amazon Athena to query the data that is in Amazon S3. Provide access to analysts.

Correct Answer: CEF

Community vote distribution

ACF (93%) 7%

✉️  **TariqKipkemei** 1 day, 23 hours ago

Selected Answer: ACF

SMB + use SQL commands to query the data = Amazon S3 File Gateway mode + Amazon Athena
upvoted 1 times

✉️  **wsdasdasdqwdaw** 1 month ago

<https://aws.amazon.com/storagegateway/file/s3/#:~:text=Amazon%20S3%20File%20Gateway%20provides,Amazon%20S3%20with%20local%20caching>.

"Amazon S3 File Gateway provides a seamless way to connect to the cloud in order to store application data files and backup images as durable objects in Amazon S3 cloud storage. Amazon S3 File Gateway offers SMB or NFS-based access to data in Amazon S3 with local caching"

=> SMB and NFS is supported in Amazon S3 File Gateway => ACF
upvoted 2 times

✉️  **iwannabeawsgod** 1 month, 1 week ago

Selected Answer: ACF

ACF 100% sure
upvoted 3 times

✉️  **Ramdi1** 2 months ago

Selected Answer: ACF

I thought the correct answer was BCF however I have changed my mind to BCF
FSx does support SMB protocol. However so does s3 file gateway which is version 2 and 3 of the SMB protocol. Hence using it with athena ACF should be correct
upvoted 4 times

✉️  **RDM10** 2 months, 1 week ago

SMB file share- is B incorrect?
upvoted 1 times

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

Selected Answer: BCE

BCF is the correct
upvoted 1 times

✉️  **Eminenza22** 2 months, 4 weeks ago

Selected Answer: ACF

<https://docs.aws.amazon.com/glue/latest/dg/aws-glue-programming-etl-format-csv-home.html>
<https://aws.amazon.com/blogs/aws/amazon-athena-interactive-sql-queries-for-data-in-amazon-s3/>
<https://aws.amazon.com/storagegateway/faqs/>
upvoted 2 times

✉️  **anikety123** 2 months, 4 weeks ago

Selected Answer: ACF

It should be ACF
upvoted 2 times

 **ralfj** 2 months, 4 weeks ago

Selected Answer: ACF

ACF use S3 File Gateway, Use Glue and Use Athena
upvoted 2 times

A company wants to use Amazon Elastic Container Service (Amazon ECS) clusters and Amazon RDS DB instances to build and run a payment processing application. The company will run the application in its on-premises data center for compliance purposes.

A solutions architect wants to use AWS Outposts as part of the solution. The solutions architect is working with the company's operational team to build the application.

Which activities are the responsibility of the company's operational team? (Choose three.)

- A. Providing resilient power and network connectivity to the Outposts racks
- B. Managing the virtualization hypervisor, storage systems, and the AWS services that run on Outposts
- C. Physical security and access controls of the data center environment
- D. Availability of the Outposts infrastructure including the power supplies, servers, and networking equipment within the Outposts racks
- E. Physical maintenance of Outposts components
- F. Providing extra capacity for Amazon ECS clusters to mitigate server failures and maintenance events

Correct Answer: ACE

Community vote distribution

ACF (36%) ACD (31%) ACE (29%) 2%

  **taustin2** Highly Voted 1 month, 2 weeks ago

Selected Answer: ACF

From <https://docs.aws.amazon.com/whitepapers/latest/aws-outposts-high-availability-design/aws-outposts-high-availability-design.html>

With Outposts, you are responsible for providing resilient power and network connectivity to the Outpost racks to meet your availability requirements for workloads running on Outposts. You are responsible for the physical security and access controls of the data center environment. You must provide sufficient power, space, and cooling to keep the Outpost operational and network connections to connect the Outpost back to the Region. Since Outpost capacity is finite and determined by the size and number of racks AWS installs at your site, you must decide how much EC2, EBS, and S3 on Outposts capacity you need to run your initial workloads, accommodate future growth, and to provide extra capacity to mitigate server failures and maintenance events.

upvoted 9 times

  **ibu007** Highly Voted 2 months, 3 weeks ago

Selected Answer: ACE

My exam is tomorrow. thank you all for the answers and links.

upvoted 8 times

  **1rob** Most Recent 1 day, 17 hours ago

Selected Answer: ACF

From <<https://aws.amazon.com/outposts/rack/faqs/>> : Your site must support the basic power, networking and space requirements to host an Outpost ==> A

From <<https://docs.aws.amazon.com/whitepapers/latest/applying-security-practices-to-network-workload-for-cspsthe-shared-responsibility-model.html>> : In AWS Outposts, the customer takes the responsibility of securing the physical infrastructure to host the AWS Outposts equipment in their own data centers. ==> C

upvoted 1 times

  **1rob** 1 day, 17 hours ago

and From <<https://docs.aws.amazon.com/whitepapers/latest/aws-outposts-high-availability-design/aws-outposts-high-availability-design.html>> : Since Outpost capacity is finite and determined by the size and number of racks AWS installs at your site, you must decide how much EC2, EBS, and S3 on Outposts capacity you need to run your initial workloads, accommodate future growth, and to provide extra capacity to mitigate server failures and maintenance events. ==> F

upvoted 1 times

  **1rob** 1 day, 17 hours ago

From <<https://docs.aws.amazon.com/whitepapers/latest/aws-outposts-high-availability-design/aws-outposts-high-availability-design.html>> : AWS is responsible for the availability of the Outposts infrastructure including the power supplies, servers, and networking equipment within the AWS Outposts racks. AWS also manages the virtualization hypervisor, storage systems, and the AWS services that run on Outposts. So The customer isn't so not D.

upvoted 1 times

  **TariqKipkemei** 1 day, 23 hours ago

Selected Answer: AC

Only A and C are correct.

AWS is responsible for the hardware and software that run on AWS Outposts. This is a fully managed infrastructure service. AWS manages security patches, updates firmware, and maintains the Outpost equipment. AWS also monitors the performance, health, and metrics for your Outpost and determines whether any maintenance is required.

<https://docs.aws.amazon.com/outposts/latest/userguide/outpost-maintenance.html>

upvoted 1 times

✉ **devyoo** 1 week, 6 days ago

Selected Answer: ACE

The role that physical companies will play is ACE.

upvoted 1 times

✉ **potomac** 3 weeks, 1 day ago

Selected Answer: ACD

E is wrong

If there is a need to perform physical maintenance, AWS will reach out to schedule a time to visit your site.

<https://aws.amazon.com/outposts/rack/faqs/#:~:text=As%20AWS%20Outposts%20rack%20runs,the%20Outpost%20for%20compliance%20certification.>

upvoted 1 times

✉ **beast2091** 3 weeks, 3 days ago

ACE

AWS is responsible for the availability of the Outposts infrastructure including the power supplies, servers, and networking equipment within the AWS Outposts racks. AWS also manages the virtualization hypervisor, storage systems, and the AWS services that run on Outposts.

<https://d1.awsstatic.com/whitepapers/aws-outposts-high-availability-design-and-architecture-considerations.pdf>

upvoted 1 times

✉ **dilaaziz** 3 weeks, 5 days ago

Selected Answer: ACF

<https://docs.aws.amazon.com/whitepapers/latest/aws-outposts-high-availability-design/aws-outposts-high-availability-design.html>

upvoted 1 times

✉ **canonlycontainletters1** 4 weeks ago

Selected Answer: ACD

I choose ACD

upvoted 1 times

✉ **danielmakita** 1 month ago

Selected Answer: ACD

I think ACD is correct

upvoted 1 times

✉ **chris0975** 1 month ago

Selected Answer: ACF

You get to choose the capacity. F

upvoted 1 times

✉ **thanhnv142** 1 month, 1 week ago

A, C and D

upvoted 1 times

✉ **aleksand41** 1 month, 2 weeks ago

ACD <https://docs.aws.amazon.com/outposts/latest/userguide/outpost-maintenance.html>

upvoted 1 times

✉ **Ramdi1** 2 months ago

Selected Answer: ACD

I think because of the shared responsibility model it is ACD

upvoted 3 times

✉ **taustin2** 2 months ago

Selected Answer: ACF

A and C are obviously right. D is wrong because "within the Outpost racks". Between E and F, E is wrong because (<https://aws.amazon.com/outposts/rack/faqs/>) says "If there is a need to perform physical maintenance, AWS will reach out to schedule a time to visit your site. AWS may replace a given module as appropriate but will not perform any host or network switch servicing on customer premises." So, choosing F.

upvoted 1 times

✉ **RDM10** 2 months, 1 week ago

Why am I not able to access the rest of the question bank?

upvoted 1 times

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

ACD

<https://aws.amazon.com/outposts/rack/faqs/>

As part of the shared responsibility model, customers are responsible for attesting to physical security and access controls around the Outpost, as well as environmental requirements for facility, networking, and power.

upvoted 1 times

Question #600

Topic 1

A company is planning to migrate a TCP-based application into the company's VPC. The application is publicly accessible on a nonstandard TCP port through a hardware appliance in the company's data center. This public endpoint can process up to 3 million requests per second with low latency. The company requires the same level of performance for the new public endpoint in AWS.

What should a solutions architect recommend to meet this requirement?

- A. Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.
- B. Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.
- C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.
- D. Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.

Correct Answer: A

Community vote distribution

A (100%)

✉  **Sugarbear_01** Highly Voted  2 months ago

Selected Answer: A

Since the company requires the same level of performance for the new public endpoint in AWS.

A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule. It attempts to open a TCP connection to the selected target on the port specified in the listener configuration.

Link;

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>

upvoted 6 times

✉  **TariqKipkemei** Most Recent  1 day, 23 hours ago

Selected Answer: A

TCP = NLB

upvoted 1 times

✉  **taustin2** 2 months, 1 week ago

Selected Answer: A

NLBs handle millions of requests per second. NLBs can handle general TCP traffic.

upvoted 2 times

A company runs its critical database on an Amazon RDS for PostgreSQL DB instance. The company wants to migrate to Amazon Aurora PostgreSQL with minimal downtime and data loss.

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

- A. Create a DB snapshot of the RDS for PostgreSQL DB instance to populate a new Aurora PostgreSQL DB cluster.
- B. Create an Aurora read replica of the RDS for PostgreSQL DB instance. Promote the Aurora read replicate to a new Aurora PostgreSQL DB cluster.
- C. Use data import from Amazon S3 to migrate the database to an Aurora PostgreSQL DB cluster.
- D. Use the pg_dump utility to back up the RDS for PostgreSQL database. Restore the backup to a new Aurora PostgreSQL DB cluster.

Correct Answer: B

Community vote distribution

B (78%) A (22%)

✉  **TariqKipkemei** 1 day, 23 hours ago

Selected Answer: B

LEAST operational overhead = read replica
upvoted 1 times

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: B

A,B,C are all valid option.
But B: The Aurora read replica option minimizes downtime during a migration.
upvoted 1 times

✉  **thanhnv142** 1 month, 1 week ago

B is correct guys. Lets see what we got here:
C and D is not correct of course. We have to consider A and B.
A: migration using a snapshot: this would, of course, introduce heavy data loss and down time
B: migration using read replica: nearly no dataloss and downtime.
upvoted 3 times

✉  **RRya** 1 month, 1 week ago

Selected Answer: A

RDS PostgreSQL to Aurora PostgreSQL:

- Option 1: DB Snapshots from RDS PostgreSQL restored as PostgreSQL Aurora DB
- Option 2: Create an Aurora Read Replica from your RDS PostgreSQL, and when the replication lag is 0, promote it as its own DB cluster (can take time and cost \$)

upvoted 1 times

✉  **Jay2k23** 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Migrating.html>
upvoted 1 times

✉  **Sugarbear_01** 2 months ago

Answer [B]

There are five options for migrating data from your existing Amazon RDS for PostgreSQL database to an Amazon Aurora PostgreSQL-Compatible DB cluster.

- 1-Using a snapshot
- 2-Using an Aurora read replica
- 3-Using a pg_dump utility
- 4-Using logical replication
- 5-Using a data import from Amazon S3

(2-Using an Aurora read replica)

The Aurora read replica option minimizes downtime during a migration. Which is what the question demand so answer B; is the correct ;
<https://repost.aws/knowledge-center/aurora-postgresql-migrate-from-rds>

upvoted 3 times

✉  **Sugarbear_01** 2 months ago

Using (4 - using logical replication) RDS for PostgreSQL and Aurora PostgreSQL instance to migrate data off minimal downtime. But is not part of the option in the answer. Which makes answer B the best solution.

upvoted 1 times

 **Guru4Cloud** 2 months ago

Selected Answer: B

The key reasons are:

Aurora read replicas allow setting up replication from RDS PostgreSQL to Aurora PostgreSQL with minimal downtime.

Once replication is set up, the read replica can be promoted to a full standalone Aurora DB cluster with little to no downtime.

This approach leverages AWS's managed replication between the source RDS PostgreSQL instance and Aurora. It avoids having to manually create backups and restore data.

Using DB snapshots or pg_dump backups requires manually restoring data which increases downtime and operational overhead.

Data import from S3 would require exporting, uploading and then importing data which adds overhead.

upvoted 4 times

 **taustin2** 2 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Migrating.html>

upvoted 1 times

A company's infrastructure consists of hundreds of Amazon EC2 instances that use Amazon Elastic Block Store (Amazon EBS) storage. A solutions architect must ensure that every EC2 instance can be recovered after a disaster.

What should the solutions architect do to meet this requirement with the LEAST amount of effort?

- A. Take a snapshot of the EBS storage that is attached to each EC2 instance. Create an AWS CloudFormation template to launch new EC2 instances from the EBS storage.
- B. Take a snapshot of the EBS storage that is attached to each EC2 instance. Use AWS Elastic Beanstalk to set the environment based on the EC2 template and attach the EBS storage.
- C. Use AWS Backup to set up a backup plan for the entire group of EC2 instances. Use the AWS Backup API or the AWS CLI to speed up the restore process for multiple EC2 instances.
- D. Create an AWS Lambda function to take a snapshot of the EBS storage that is attached to each EC2 instance and copy the Amazon Machine Images (AMIs). Create another Lambda function to perform the restores with the copied AMIs and attach the EBS storage.

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud** Highly Voted 2 months ago

Selected Answer: C

The key reasons are:

AWS Backup automates backup of resources like EBS volumes. It allows defining backup policies for groups of resources. This removes the need to manually create backups for each resource.

The AWS Backup API and CLI allow programmatic control of backup plans and restores. This enables restoring hundreds of EC2 instances programmatically after a disaster instead of manually.

AWS Backup handles cleanup of old backups based on policies to minimize storage costs.

upvoted 6 times

 **TariqKipkemei** Most Recent 1 day, 23 hours ago

Selected Answer: C

LEAST amount of effort = AWS Backup

upvoted 1 times

 **Chiquitabandita** 1 week, 2 days ago

for the question, I would choose C as well, AWS Backup of the EC2, but design, why would anything of importance be on the Ec2 that would need to be restored? Shouldn't any critical or important data be on the EBS volumes in this example or similar location?

upvoted 1 times

 **taustin2** 2 months, 1 week ago

Selected Answer: C

Going with Backup. Can restore programmatically using Backup API.

upvoted 2 times

A company recently migrated to the AWS Cloud. The company wants a serverless solution for large-scale parallel on-demand processing of a semistructured dataset. The data consists of logs, media files, sales transactions, and IoT sensor data that is stored in Amazon S3. The company wants the solution to process thousands of items in the dataset in parallel.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Use the AWS Step Functions Map state in Inline mode to process the data in parallel.
- B. Use the AWS Step Functions Map state in Distributed mode to process the data in parallel.
- C. Use AWS Glue to process the data in parallel.
- D. Use several AWS Lambda functions to process the data in parallel.

Correct Answer: B

Community vote distribution

B (100%)

✉  **Guru4Cloud**  2 months ago

Selected Answer: B

AWS Step Functions allows you to orchestrate and scale distributed processing using the Map state. The Map state can process items in a large dataset in parallel by distributing the work across multiple resources.

Using the Map state in Distributed mode will automatically handle the parallel processing and scaling. Step Functions will add more workers to process the data as needed.

Step Functions is serverless so there are no servers to manage. It will scale up and down automatically based on demand.

upvoted 5 times

✉  **TariqKipkemei**  1 day, 22 hours ago

Selected Answer: B

The Distributed Map has been optimized for Amazon S3., helping you more easily iterate over objects in an S3 bucket. With the Distributed mode, you can run at concurrency of up to 10,000 parallel branches.

<https://aws.amazon.com/step-functions/faqs/#:~:text=A%20Map%20in%20Inline%20mode,up%20to%2010%2C000%20parallel%20branches>.
upvoted 1 times

✉  **Sugarbear_01** 2 months ago

Selected Answer: B

<https://docs.aws.amazon.com/step-functions/latest/dg/concepts-orchestrate-large-scale-parallel-workloads.html>

upvoted 1 times

✉  **taustin2** 2 months, 1 week ago

Selected Answer: B

With Step Functions, you can orchestrate large-scale parallel workloads to perform tasks, such as on-demand processing of semi-structured data. These parallel workloads let you concurrently process large-scale data sources stored in Amazon S3. <https://docs.aws.amazon.com/step-functions/latest/dg/concepts-orchestrate-large-scale-parallel-workloads.html>

upvoted 2 times

✉  **Sugarbear_01** 2 months ago

After going through the link I confirmed the answer is B

upvoted 1 times

✉  **[Removed]** 2 months, 1 week ago

Large Scale + Parallel = Distributed Step Function

<https://docs.aws.amazon.com/step-functions/latest/dg/concepts-inline-vs-distributed-map.html>
upvoted 1 times

A company will migrate 10 PB of data to Amazon S3 in 6 weeks. The current data center has a 500 Mbps uplink to the internet. Other on-premises applications share the uplink. The company can use 80% of the internet bandwidth for this one-time migration task.

Which solution will meet these requirements?

- A. Configure AWS DataSync to migrate the data to Amazon S3 and to automatically verify the data.
- B. Use rsync to transfer the data directly to Amazon S3.
- C. Use the AWS CLI and multiple copy processes to send the data directly to Amazon S3.
- D. Order multiple AWS Snowball devices. Copy the data to the devices. Send the devices to AWS to copy the data to Amazon S3.

Correct Answer: A

Community vote distribution

D (100%)

 **TariqKipkemei** 1 day, 22 hours ago

Selected Answer: D

PB = snowball
upvoted 1 times

 **wsdasdasdqwdaw** 1 month ago

D, but even if you do not know, all 3 option (A,B and C) have the same nature (transfer via bandwidth) and we know that there is only one correct answer => D.

upvoted 2 times

 **iwannabeawsgod** 1 month, 1 week ago

Selected Answer: D

snowball for sure
upvoted 2 times

 **joshik** 1 month, 3 weeks ago

Selected Answer: D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.
upvoted 1 times

 **Xin123** 2 months ago

D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.
upvoted 1 times

 **Sugarbear_01** 2 months ago

Selected Answer: D

D
1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.
upvoted 1 times

 **Devsin2000** 2 months ago

D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.
upvoted 1 times

 **Guru4Cloud** 2 months ago

Selected Answer: D

D. Order multiple AWS Snowball devices. Copy the data to the devices. Send the devices to AWS to copy the data to Amazon S3.
upvoted 1 times

 **taustin2** 2 months, 1 week ago

Selected Answer: D

10 PB = It's Snowballs.
upvoted 2 times

 **kambarami** 2 months, 1 week ago

Answer is DDDDD

A company has several on-premises Internet Small Computer Systems Interface (iSCSI) network storage servers. The company wants to reduce the number of these servers by moving to the AWS Cloud. A solutions architect must provide low-latency access to frequently used data and reduce the dependency on on-premises servers with a minimal number of infrastructure changes.

Which solution will meet these requirements?

- A. Deploy an Amazon S3 File Gateway.
- B. Deploy Amazon Elastic Block Store (Amazon EBS) storage with backups to Amazon S3.
- C. Deploy an AWS Storage Gateway volume gateway that is configured with stored volumes.
- D. Deploy an AWS Storage Gateway volume gateway that is configured with cached volumes.

Correct Answer: C

Community vote distribution

D (100%)

 **TariqKipkemei** 1 day, 22 hours ago

Selected Answer: D

low-latency access to frequently used data = cached volumes
upvoted 1 times

 **Sugarbear_01** 2 months ago

Answer D

Here is the link ;
<https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html>
upvoted 1 times

 **Guru4Cloud** 2 months ago

Selected Answer: D

The key reasons are:

The Storage Gateway volume gateway provides iSCSI block storage using cached volumes. This allows replacing the on-premises iSCSI servers with minimal changes.

Cached volumes store frequently accessed data locally for low latency access, while storing less frequently accessed data in S3.
This reduces the number of on-premises servers while still providing low latency access to hot data.

EBS does not provide iSCSI support to replace the existing servers.
S3 File Gateway is for file storage, not block storage.

Stored volumes would store all data on-premises, not in S3.

upvoted 4 times

 **taustin2** 2 months, 1 week ago

Selected Answer: D

iSCSI=Volume Gateway.
low-latency access to frequently used data = cached volumes
upvoted 2 times

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

"low-latency access to FREQUENTLY used data" = Cached AWS Storage Gateway volumes
upvoted 1 times

 **nnecode** 2 months, 1 week ago

Selected Answer: D

An AWS Storage Gateway volume gateway is a hybrid storage solution that connects your on-premises applications to your cloud storage. It provides low-latency access to frequently used data while storing your entire dataset in the cloud.

When you configure an AWS Storage Gateway volume gateway with cached volumes, the gateway stores a copy of frequently accessed data locally. This allows you to provide low-latency access to your frequently accessed data while reducing your dependency on on-premises servers.

upvoted 2 times

A solutions architect is designing an application that will allow business users to upload objects to Amazon S3. The solution needs to maximize object durability. Objects also must be readily available at any time and for any length of time. Users will access objects frequently within the first 30 days after the objects are uploaded, but users are much less likely to access objects that are older than 30 days.

Which solution meets these requirements MOST cost-effectively?

- A. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Glacier after 30 days.
- B. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- C. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D. Store all the objects in S3 Intelligent-Tiering with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

Correct Answer: B

Community vote distribution

B (100%)

 **TariqKipkemei** 1 day, 2 hours ago

Selected Answer: B

'Objects also must be readily available at any time and for any length of time'...definitely option B.
upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: B

B is correct
upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

B is correct
C is not correct because data must be durable. C is only for data that can be regenerated.
upvoted 2 times

 **Xin123** 2 months ago

Selected Answer: B

Durability. Available any time for any duration => B
upvoted 1 times

 **Sugarbear_01** 2 months ago

Selected Answer: B

Minimum Days for Transition to S3 Standard-IA or S3 One Zone-IA

Before you transition objects to S3 Standard-IA or S3 One Zone-IA, you must store them for at least 30 days in Amazon S3. For example, you cannot create a Lifecycle rule to transition objects to the S3 Standard-IA storage class one day after you create them. Amazon S3 doesn't support this transition within the first 30 days because newer objects are often accessed more frequently or deleted sooner than is suitable for S3 Standard-IA or S3 One Zone-IA storage.

Similarly, if you are transitioning noncurrent objects (in versioned buckets), you can transition only objects that are at least 30 days noncurrent to S3 Standard-IA or S3 One Zone-IA storage.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>
upvoted 2 times

 **Devsin2000** 2 months ago

A
S3 Glacier is most cost effective
upvoted 4 times

 **taustin2** 2 months, 1 week ago

Selected Answer: B

B meets the requirements. No need for intelligent Tiering because of 30 days.

upvoted 1 times

Question #607

Topic 1

A company has migrated a two-tier application from its on-premises data center to the AWS Cloud. The data tier is a Multi-AZ deployment of Amazon RDS for Oracle with 12 TB of General Purpose SSD Amazon Elastic Block Store (Amazon EBS) storage. The application is designed to process and store documents in the database as binary large objects (blobs) with an average document size of 6 MB.

The database size has grown over time, reducing the performance and increasing the cost of storage. The company must improve the database performance and needs a solution that is highly available and resilient.

Which solution will meet these requirements MOST cost-effectively?

- A. Reduce the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Magnetic.
- B. Increase the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Provisioned IOPS.
- C. Create an Amazon S3 bucket. Update the application to store documents in the S3 bucket. Store the object metadata in the existing database.
- D. Create an Amazon DynamoDB table. Update the application to use DynamoDB. Use AWS Database Migration Service (AWS DMS) to migrate data from the Oracle database to DynamoDB.

Correct Answer: C

Community vote distribution

C (100%)

✉️  **TariqKipkemei** 1 day, 2 hours ago

Selected Answer: C

MOST cost-effectively = store the objects in S3, and object metadata in the existing DB.

upvoted 1 times

✉️  **taustin2** 2 months ago

DynamoDB's limit on the size of each record is 400KB, so D is wrong.

upvoted 2 times

✉️  **Guru4Cloud** 2 months ago

Selected Answer: C

C. Create an Amazon S3 bucket. Update the application to store documents in the S3 bucket. Store the object metadata in the existing database.

upvoted 3 times

✉️  **taustin2** 2 months, 1 week ago

Selected Answer: C

Storing the blobs in the db is more expensive than s3 with references in the db.

upvoted 2 times

A company has an application that serves clients that are deployed in more than 20.000 retail storefront locations around the world. The application consists of backend web services that are exposed over HTTPS on port 443. The application is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The retail locations communicate with the web application over the public internet. The company allows each retail location to register the IP address that the retail location has been allocated by its local ISP.

The company's security team recommends to increase the security of the application endpoint by restricting access to only the IP addresses registered by the retail locations.

What should a solutions architect do to meet these requirements?

- A. Associate an AWS WAF web ACL with the ALB. Use IP rule sets on the ALB to filter traffic. Update the IP addresses in the rule to include the registered IP addresses.
- B. Deploy AWS Firewall Manager to manage the ALConfigure firewall rules to restrict traffic to the ALModify the firewall rules to include the registered IP addresses.
- C. Store the IP addresses in an Amazon DynamoDB table. Configure an AWS Lambda authorization function on the ALB to validate that incoming requests are from the registered IP addresses.
- D. Configure the network ACL on the subnet that contains the public interface of the ALB. Update the ingress rules on the network ACL with entries for each of the registered IP addresses.

Correct Answer: A

Community vote distribution

A (77%)

C (23%)

✉️  **TariqKipkemei** 1 day, 2 hours ago

Selected Answer: A

endpoint restriction by IP addresses = AWS WAF

upvoted 1 times

✉️  **Passeexam4sure_com** 1 month, 2 weeks ago

Selected Answer: A

Associate an AWS WAF web ACL with the ALB. Use IP rule sets on the ALB to filter traffic. Update the IP addresses in the rule to include the registered IP addresses.

upvoted 3 times

✉️  **Sugarbear_01** 2 months ago

Selected Answer: A

AWS WAF cannot be directly associated with a Web Application. But, can only be associated with Application Load Balancer, CloudFront and API Gateway.

upvoted 2 times

✉️  **taustin2** 2 months ago

Selected Answer: C

Changing answer to C because of "20000" IP addresses. Use Lambda with ALB.

upvoted 3 times

✉️  **potomac** 3 weeks, 1 day ago

10,000 IP addresses

For the latest version of AWS WAF, see AWS WAF. If you want to allow or block web requests based on the IP addresses that the requests originate from, create one or more IP match conditions. An IP match condition lists up to 10,000 IP addresses or IP address ranges that your requests originate from.

upvoted 1 times

✉️  **bsbs1234** 1 month, 2 weeks ago

I will choose this answer if it is API Gateway. But I cannot figure out how to do lambda authentication on ALB. I will go A

upvoted 1 times

✉️  **taustin2** 1 month, 2 weeks ago

You are right. I don't know of a way to use Lambda with ALB in this way. Answer is A.

upvoted 1 times

✉️  **potomac** 3 weeks, 1 day ago

ALB invokes Lambda function, sending the incoming data in JSON format. Lambda function performs task, returns HTTP response to ALB.
upvoted 1 times

 **potomac** 3 weeks, 1 day ago

WAF seems still better

upvoted 1 times

 **Guru4Cloud** 2 months ago

Selected Answer: A

A. Associate an AWS WAF web ACL with the ALB. Use IP rule sets on the ALB to filter traffic. Update the IP addresses in the rule to include the registered IP addresses.

upvoted 2 times

 **taustin2** 2 months, 1 week ago

Selected Answer: A

WAF meets the requirements.

upvoted 2 times

A company is building a data analysis platform on AWS by using AWS Lake Formation. The platform will ingest data from different sources such as Amazon S3 and Amazon RDS. The company needs a secure solution to prevent access to portions of the data that contain sensitive information.

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

- A. Create an IAM role that includes permissions to access Lake Formation tables.
- B. Create data filters to implement row-level security and cell-level security.
- C. Create an AWS Lambda function that removes sensitive information before Lake Formation ingests the data.
- D. Create an AWS Lambda function that periodically queries and removes sensitive information from Lake Formation tables.

Correct Answer: C

Community vote distribution

B (100%)

 **Guru4Cloud** Highly Voted 2 months ago

Selected Answer: B

The key reasons are:

Lake Formation data filters allow restricting access to rows or cells in data tables based on conditions. This allows preventing access to sensitive data.

Data filters are implemented within Lake Formation and do not require additional coding or Lambda functions.

Lambda functions to pre-process data or purge tables would require ongoing development and maintenance.

IAM roles only provide user-level permissions, not row or cell level security.

Data filters give granular access control over Lake Formation data with minimal configuration, avoiding complex custom code.

upvoted 6 times

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

Selected Answer: B

<https://docs.aws.amazon.com/lake-formation/latest/dg/data-filters-about.html>

upvoted 1 times

 **taustin2** 2 months, 1 week ago

Selected Answer: B

You can create data filters based on the values of columns in a Lake Formation table. Easy. Lowest operational overhead.

upvoted 1 times

 **nnecode** 2 months, 1 week ago

Selected Answer: B

The best solution to meet the requirements with the least operational overhead is to create data filters to implement row-level security and cell-level security.

Data filters are a feature of Lake Formation that allow you to restrict access to data based on row and column values. This can be used to implement row-level security and cell-level security.

To implement row-level security, you would create a data filter that only allows users to access rows where the values in certain columns meet certain criteria. For example, you could create a data filter that only allows users to access rows where the value in the customer_id column matches the user's own customer ID.

upvoted 2 times

A company deploys Amazon EC2 instances that run in a VPC. The EC2 instances load source data into Amazon S3 buckets so that the data can be processed in the future. According to compliance laws, the data must not be transmitted over the public internet. Servers in the company's on-premises data center will consume the output from an application that runs on the EC2 instances.

Which solution will meet these requirements?

- A. Deploy an interface VPC endpoint for Amazon EC2. Create an AWS Site-to-Site VPN connection between the company and the VPC.
- B. Deploy a gateway VPC endpoint for Amazon S3. Set up an AWS Direct Connect connection between the on-premises network and the VPC.
- C. Set up an AWS Transit Gateway connection from the VPC to the S3 buckets. Create an AWS Site-to-Site VPN connection between the company and the VPC.
- D. Set up proxy EC2 instances that have routes to NAT gateways. Configure the proxy EC2 instances to fetch S3 data and feed the application instances.

Correct Answer: B

Community vote distribution

B (100%)

 **taustin2** Highly Voted 2 months, 1 week ago

Selected Answer: B

Gateway VPC Endpoint = no internet to access S3. Direct Connect = secure access to VPC.
upvoted 6 times

 **TariqKipkemei** Most Recent 1 day, 2 hours ago

Selected Answer: B

data must not be transmitted over the public internet = gateway VPC endpoint for Amazon S3 and AWS Direct Connect connection between the on-premises network and the VPC.
upvoted 1 times

 **Guru4Cloud** 2 months ago

Selected Answer: B

Gateway VPC Endpoint = no internet to access S3. Direct Connect = secure access to VPC
I agree with you @taustin2- Happy Learning all
upvoted 4 times

A company has an application with a REST-based interface that allows data to be received in near-real time from a third-party vendor. Once received, the application processes and stores the data for further analysis. The application is running on Amazon EC2 instances.

The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application. When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.

Which design should a solutions architect recommend to provide a more scalable solution?

- A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.
- B. Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota limit for the third-party vendor.
- C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data. Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.
- D. Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud**  2 months ago

Selected Answer: A

The key reasons are:

Kinesis Data Streams provides an auto-scaling stream that can handle large amounts of streaming data ingestion and throughput. This removes the bottlenecks around receiving the data.

AWS Lambda can process and store the data in a scalable serverless manner, avoiding EC2 capacity limits.

API Gateway adds API management capabilities but does not improve the underlying scalability of the EC2 application.

SNS is for event publishing/notifications, not large scale data ingestion. ECS still relies on EC2 capacity.

upvoted 5 times

 **TariqKipkemei**  1 day, 2 hours ago

Selected Answer: A

more scalable solution? = serverless = Amazon Kinesis Data Streams and AWS Lambda functions

upvoted 1 times

 **wsdasdasdqwdaw** 1 month ago

Only A is pure serverless which means scale. A for sure.

upvoted 1 times

 **taustin2** 2 months, 1 week ago

Selected Answer: A

For near-real time data ingest and processing, Kinesis and Lambda are most scalable choice.

upvoted 4 times

A company has an application that runs on Amazon EC2 instances in a private subnet. The application needs to process sensitive information from an Amazon S3 bucket. The application must not use the internet to connect to the S3 bucket.

Which solution will meet these requirements?

- A. Configure an internet gateway. Update the S3 bucket policy to allow access from the internet gateway. Update the application to use the new internet gateway.
- B. Configure a VPN connection. Update the S3 bucket policy to allow access from the VPN connection. Update the application to use the new VPN connection.
- C. Configure a NAT gateway. Update the S3 bucket policy to allow access from the NAT gateway. Update the application to use the new NAT gateway.
- D. Configure a VPC endpoint. Update the S3 bucket policy to allow access from the VPC endpoint. Update the application to use the new VPC endpoint.

Correct Answer: A

Community vote distribution

D (100%)

 **TariqKipkemei** 1 day, 1 hour ago

Selected Answer: D

application must not use the internet to connect to the S3 bucket = VPC endpoint
upvoted 1 times

 **Guru4Cloud** 2 months ago

Selected Answer: D

The solution that will meet these requirements is to:

Configure a VPC endpoint for Amazon S3
Update the S3 bucket policy to allow access from the VPC endpoint
Update the application to use the new VPC endpoint
The key reasons are:

VPC endpoints allow private connectivity from VPCs to AWS services like S3 without using an internet gateway.
The application can connect to S3 through the VPC endpoint while remaining in the private subnet, without internet access.
upvoted 3 times

 **taustin2** 2 months, 1 week ago

Selected Answer: D

VPC Endpoint for S3.
upvoted 1 times

 **aleariva** 2 months, 1 week ago

D is the correct...<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/what-are-vpc-endpoints.html>
upvoted 1 times

 **awslearnerin2022** 2 months, 1 week ago

Selected Answer: D

VPC endpoint enables communication between VPC subnet and S3 bucket.
upvoted 1 times

 **nnecode** 2 months, 1 week ago

Selected Answer: D

A VPC endpoint is a managed endpoint in your VPC that is connected to a public AWS service. It provides a private connection between your VPC and the service, and it does not require an internet gateway or a NAT device.

Option A (internet gateway) would involve exposing the S3 bucket to the internet, which is not recommended for security reasons.

Option B (VPN connection) would require additional setup and would still involve traffic going over the internet.

Option C (NAT gateway) is used for outbound internet access from private subnets, not for accessing S3 without the internet.
upvoted 2 times

A company uses Amazon Elastic Kubernetes Service (Amazon EKS) to run a container application. The EKS cluster stores sensitive information in the Kubernetes secrets object. The company wants to ensure that the information is encrypted.

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

- A. Use the container application to encrypt the information by using AWS Key Management Service (AWS KMS).
- B. Enable secrets encryption in the EKS cluster by using AWS Key Management Service (AWS KMS).
- C. Implement an AWS Lambda function to encrypt the information by using AWS Key Management Service (AWS KMS).
- D. Use AWS Systems Manager Parameter Store to encrypt the information by using AWS Key Management Service (AWS KMS).

Correct Answer: B

Community vote distribution

B (100%)

✉  **Guru4Cloud**  2 months ago

Selected Answer: B

EKS supports encrypting Kubernetes secrets at the cluster level using AWS KMS keys. This provides an automated way to encrypt secrets. Enabling this feature requires minimal configuration changes to the EKS cluster and no code changes. Other options like using Lambda functions or modifying the application code to encrypt secrets require additional development effort and overhead. Systems Manager Parameter Store could store encrypted parameters but does not natively integrate with EKS to encrypt Kubernetes secrets. The EKS secrets encryption feature leverages AWS KMS without the need to directly call KMS APIs from the application.

upvoted 6 times

✉  **TariqKipkemei**  1 day, 1 hour ago

Selected Answer: B

LEAST operational overhead? = Enable secrets encryption in the EKS cluster

upvoted 1 times

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: B

<https://aws.amazon.com/about-aws/whats-new/2020/03/amazon-eks-adds-envelope-encryption-for-secrets-with-aws-kms/>

upvoted 1 times

✉  **dilaaziz** 4 weeks ago

Selected Answer: B

<https://aws.amazon.com/about-aws/whats-new/2020/03/amazon-eks-adds-envelope-encryption-for-secrets-with-aws-kms/>

upvoted 1 times

✉  **iwannabeawsgod** 1 month, 1 week ago

BBBBBBB

upvoted 1 times

✉  **taustin2** 2 months, 1 week ago

Selected Answer: B

Use KMS. Enable secrets encryption in KMS.

upvoted 2 times

✉  **nnecode** 2 months, 1 week ago

Selected Answer: B

Enabling secrets encryption in the EKS cluster by using AWS Key Management Service (AWS KMS) is the least operationally overhead way to encrypt the sensitive information in the Kubernetes secrets object.

When you enable secrets encryption in the EKS cluster, AWS KMS encrypts the secrets before they are stored in the EKS cluster. You do not need to make any changes to your container application or implement any additional Lambda functions.

upvoted 2 times

A company is designing a new multi-tier web application that consists of the following components:

- Web and application servers that run on Amazon EC2 instances as part of Auto Scaling groups
- An Amazon RDS DB instance for data storage

A solutions architect needs to limit access to the application servers so that only the web servers can access them.

Which solution will meet these requirements?

- A. Deploy AWS PrivateLink in front of the application servers. Configure the network ACL to allow only the web servers to access the application servers.
- B. Deploy a VPC endpoint in front of the application servers. Configure the security group to allow only the web servers to access the application servers.
- C. Deploy a Network Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the network ACL to allow only the web servers to access the application servers.
- D. Deploy an Application Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the security group to allow only the web servers to access the application servers.

Correct Answer: A

Community vote distribution

D (78%) B (22%)

 **Guru4Cloud**  2 months ago

Selected Answer: D

The key reasons are:

An Application Load Balancer (ALB) allows directing traffic to the application servers and provides access control via security groups. Security groups act as a firewall at the instance level and can control access to the application servers from the web servers. Network ACLs work at the subnet level and are less flexible for security groups for instance-level access control. VPC endpoints are used to provide private access to AWS services, not for access between EC2 instances. AWS PrivateLink provides private connectivity between VPCs, which is not required in this single VPC scenario.

upvoted 8 times

 **TariqKipkemei**  1 day, 1 hour ago

Selected Answer: D

Deploy an Application Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the security group to allow only the web servers to access the application servers

upvoted 1 times

 **Tekk97** 1 week, 6 days ago

Selected Answer: D

I think B also working. but A company has Auto Scaling groups. D has strategy for Auto Scaling. D is correct

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: D

D is correct

upvoted 1 times

 **iwannabeawsgod** 1 month, 1 week ago

Selected Answer: D

Scaling group to Scaling group.

upvoted 1 times

 **Devsin2000** 2 months ago

C - ALB is for Web applications only. NLB can be internal / not public

upvoted 1 times

 **taustin2** 2 months, 1 week ago

Selected Answer: D

ALB with Security Group is simplest solution.

upvoted 2 times

 **nnecode** 2 months, 1 week ago

Selected Answer: B

A VPC endpoint is a managed endpoint in your VPC that is connected to a public AWS service. It provides a private connection between your VPC and the service, and it does not require an internet gateway or a NAT device.

The other options do not meet all of the requirements:

Option A: AWS PrivateLink is a service that allows you to connect your VPC to private services that are owned by AWS or by other AWS customers. It is not designed to be used to limit access to resources within the same VPC.

Option C: A Network Load Balancer can be used to distribute traffic across multiple application servers, but it does not provide a way to limit access to the application servers.

Option D: An Application Load Balancer can be used to distribute traffic across multiple application servers, but it does not provide a way to limit access to the application servers.

upvoted 4 times

A company runs a critical, customer-facing application on Amazon Elastic Kubernetes Service (Amazon EKS). The application has a microservices architecture. The company needs to implement a solution that collects, aggregates, and summarizes metrics and logs from the application in a centralized location.

Which solution meets these requirements?

- A. Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
- B. Run AWS App Mesh in the existing EKS cluster. View the metrics and logs in the App Mesh console.
- C. Configure AWS CloudTrail to capture data events. Query CloudTrail by using Amazon OpenSearch Service.
- D. Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console.

Correct Answer: C

Community vote distribution

D (78%)

A (22%)

 **TariqKipkemei** 1 day, 1 hour ago

Selected Answer: D

EKS monitoring = Amazon CloudWatch Container Insights
upvoted 1 times

 **Examanier1217** 2 weeks, 4 days ago

Selected Answer: A

I have worked on it. A is the right answer
upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: D

Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices. Container Insights is available for Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and Kubernetes platforms on Amazon EC2. Container Insights supports collecting metrics from clusters deployed on AWS Fargate for both Amazon ECS and Amazon EKS.

upvoted 1 times

 **dilaaziz** 4 weeks ago

Selected Answer: D

<https://aws.amazon.com/cloudwatch/features/>
upvoted 1 times

 **Guru4Cloud** 2 months ago

Selected Answer: D

The key reasons are:

CloudWatch Container Insights automatically collects metrics and logs from containers running in EKS clusters. This provides visibility into resource utilization, application performance, and microservice interactions.

The metrics and logs are stored in CloudWatch Logs and CloudWatch metrics for central access.

The CloudWatch console allows querying, filtering, and visualizing the metrics and logs in one centralized place.

upvoted 2 times

 **ErnShm** 2 months ago

D

Amazon CloudWatch Application Insights facilitates observability for your applications and underlying AWS resources. It helps you set up the best monitors for your application resources to continuously analyze data for signs of problems with your applications.

upvoted 2 times

 **taustin2** 2 months, 1 week ago

Selected Answer: D

What Cloudwatch Container Insights is for.

upvoted 1 times

 **kambarami** 2 months, 1 week ago

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/deploy-container-insights-EKS.html>

upvoted 1 times

 **awslearnerin2022** 2 months, 1 week ago

Selected Answer: A

Cloudwatch monitors applications and provides metrics. Cloudtrail is used for API activities in the account.

upvoted 1 times

 **nnecode** 2 months, 1 week ago

Selected Answer: D

Amazon CloudWatch Container Insights is a service that collects, aggregates, and summarizes metrics and logs from containerized applications. It is designed to work with Amazon EKS and Kubernetes.

upvoted 1 times

A company has deployed its newest product on AWS. The product runs in an Auto Scaling group behind a Network Load Balancer. The company stores the product's objects in an Amazon S3 bucket.

The company recently experienced malicious attacks against its systems. The company needs a solution that continuously monitors for malicious activity in the AWS account, workloads, and access patterns to the S3 bucket. The solution must also report suspicious activity and display the information on a dashboard.

Which solution will meet these requirements?

- A. Configure Amazon Macie to monitor and report findings to AWS Config.
- B. Configure Amazon Inspector to monitor and report findings to AWS CloudTrail.
- C. Configure Amazon GuardDuty to monitor and report findings to AWS Security Hub.
- D. Configure AWS Config to monitor and report findings to Amazon EventBridge.

Correct Answer: A

Community vote distribution

C (100%)

✉  **Guru4Cloud**  2 months ago

Selected Answer: C

The key reasons are:

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior. It analyzes AWS CloudTrail, VPC Flow Logs, and DNS logs.
GuardDuty can detect threats like instance or S3 bucket compromise, malicious IP addresses, or unusual API calls.
Findings can be sent to AWS Security Hub which provides a centralized security dashboard and alerts.
Amazon Macie and Amazon Inspector do not monitor the breadth of activity that GuardDuty does. They focus more on data security and application vulnerabilities respectively.
AWS Config monitors for resource configuration changes, not malicious activity.

upvoted 6 times

✉  **dilaaziz**  4 weeks ago

Selected Answer: C

Guardduty

upvoted 1 times

✉  **taustin2** 2 months, 1 week ago

Selected Answer: C

What Guard Duty is for.

upvoted 2 times

✉  **Guru4Cloud** 2 months ago

The key reasons are:

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior. It analyzes AWS CloudTrail, VPC Flow Logs, and DNS logs.
GuardDuty can detect threats like instance or S3 bucket compromise, malicious IP addresses, or unusual API calls.
Findings can be sent to AWS Security Hub which provides a centralized security dashboard and alerts.
Amazon Macie and Amazon Inspector do not monitor the breadth of activity that GuardDuty does. They focus more on data security and application vulnerabilities respectively.
AWS Config monitors for resource configuration changes, not malicious activity.

upvoted 2 times

✉  **kambarami** 2 months, 1 week ago

Answer is C.

upvoted 1 times

✉  **aleariva** 2 months, 1 week ago

C is the correct. <https://aws.amazon.com/guardduty/>

upvoted 1 times

✉  **brownie23** 2 months, 1 week ago

Answer is C Since Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, Amazon Elastic Compute Cloud (EC2) workloads, container applications, Amazon Aurora databases, and data stored in Amazon Simple Storage Service (S3).

upvoted 2 times

awslearnerin2022 2 months, 1 week ago

Selected Answer: C

Gaurd duty is a threat detection service for accounts and workloads.

upvoted 1 times

Question #617

Topic 1

A company wants to migrate an on-premises data center to AWS. The data center hosts a storage server that stores data in an NFS-based file system. The storage server holds 200 GB of data. The company needs to migrate the data without interruption to existing services. Multiple resources in AWS must be able to access the data by using the NFS protocol.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Create an Amazon FSx for Lustre file system.
- B. Create an Amazon Elastic File System (Amazon EFS) file system.
- C. Create an Amazon S3 bucket to receive the data.
- D. Manually use an operating system copy command to push the data into the AWS destination.
- E. Install an AWS DataSync agent in the on-premises data center. Use a DataSync task between the on-premises location and AWS.

Correct Answer: AB

Community vote distribution

BE (100%)

awslearnerin2022 2 months ago

Selected Answer: BE

Amazon EFS provides a scalable, high performance NFS file system that can be accessed from multiple resources in AWS. AWS DataSync can perform the migration from the on-prem NFS server to EFS without interruption to existing services. This avoids having to manually move the data which could cause downtime. DataSync incrementally syncs changed data. EFS and DataSync together provide a cost-optimized approach compared to using S3 or FSx, while still meeting the requirements. Manually copying 200 GB of data to AWS would be slow and risky compared to using DataSync.

upvoted 5 times

dilaaziz 4 weeks ago

Selected Answer: BE

<https://aws.amazon.com/compare/the-difference-between-nfs-smb/>

upvoted 1 times

taustin2 2 months, 1 week ago

Selected Answer: BE

NFS file system = EFS, Use DataSync for the migration with NFS support.

upvoted 2 times

awslearnerin2022 2 months, 1 week ago

Selected Answer: BE

EFS can be accessed by multiple AWS resources.

Datasync allows NFS migrations.

upvoted 3 times

A company wants to use Amazon FSx for Windows File Server for its Amazon EC2 instances that have an SMB file share mounted as a volume in the us-east-1 Region. The company has a recovery point objective (RPO) of 5 minutes for planned system maintenance or unplanned service disruptions. The company needs to replicate the file system to the us-west-2 Region. The replicated data must not be deleted by any user for 5 years.

Which solution will meet these requirements?

- A. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- B. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- C. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- D. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.

Correct Answer: C

Community vote distribution

C (100%)

 **taustin2** Highly Voted 2 months, 1 week ago

Selected Answer: C

Need to use Compliance Mode, so it's either A or C. RPO leads to Multi-AZ so C.
upvoted 6 times

 **dilaaziz** Most Recent 4 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html>
upvoted 1 times

 **thanhnv142** 1 month, 1 week ago

C is correct.
A and C is potential answer because they mention compliance mode. But single AZ is recommended for test and development only. For production workloads, we need multi AZ, which is C
upvoted 1 times

 **Xin123** 2 months ago

Selected Answer: C

Trust me bro
upvoted 2 times

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

- A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
- B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
- C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it to the developer accounts.
- D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the management account.

Correct Answer: C

Community vote distribution

C (100%)

 **Xin123**  2 months ago

Selected Answer: C

Organizations + Restricts = SCP
upvoted 5 times

 **taustin2**  2 months, 1 week ago

Selected Answer: C

For Organizations to restrict users in accounts, use an SCP.
upvoted 5 times

 **Ramdi1**  1 month, 4 weeks ago

Selected Answer: C

C - Use SCP best way
upvoted 3 times

A company is planning to deploy a business-critical application in the AWS Cloud. The application requires durable storage with consistent, low-latency performance.

Which type of storage should a solutions architect recommend to meet these requirements?

- A. Instance store volume
- B. Amazon ElastiCache for Memcached cluster
- C. Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume
- D. Throughput Optimized HDD Amazon Elastic Block Store (Amazon EBS) volume

Correct Answer: C

Community vote distribution

C (100%)

 **taustin2** Highly Voted 2 months, 1 week ago

Selected Answer: C

Durable storage excludes A and B. Low-latency excludes D. Choose C.

upvoted 9 times

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

Selected Answer: C

Provisioned IOPS SSD — Provides high performance for mission-critical, low-latency, or high-throughput workloads. Throughput Optimized HDD — A low-cost HDD designed for frequently accessed, throughput-intensive workloads.

upvoted 2 times

 **dilaaziz** 4 weeks ago

Selected Answer: C

<https://aws.amazon.com/ebs/volume-types/>

upvoted 1 times

An online photo-sharing company stores its photos in an Amazon S3 bucket that exists in the us-west-1 Region. The company needs to store a copy of all new photos in the us-east-1 Region.

Which solution will meet this requirement with the LEAST operational effort?

- A. Create a second S3 bucket in us-east-1. Use S3 Cross-Region Replication to copy photos from the existing S3 bucket to the second S3 bucket.
- B. Create a cross-origin resource sharing (CORS) configuration of the existing S3 bucket. Specify us-east-1 in the CORS rule's AllowedOrigin element.
- C. Create a second S3 bucket in us-east-1 across multiple Availability Zones. Create an S3 Lifecycle rule to save photos into the second S3 bucket.
- D. Create a second S3 bucket in us-east-1. Configure S3 event notifications on object creation and update events to invoke an AWS Lambda function to copy photos from the existing S3 bucket to the second S3 bucket.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** Highly Voted 2 months ago

Selected Answer: A

S3 Cross-Region Replication handles automatically copying new objects added to the source bucket to the destination bucket in a different region. It continuously replicates new photos without needing to manually copy files or set up Lambda triggers.

CORS only enables cross-origin access, it does not copy objects.

Using Lifecycle rules or Lambda functions requires custom code and logic to handle the copying.

S3 Cross-Region Replication provides automated replication that minimizes operational overhead.

upvoted 6 times

 **dilaaziz** Most Recent 4 weeks ago

Selected Answer: A

<https://aws.amazon.com/about-aws/whats-new/2015/03/amazon-s3-introduces-cross-region-replication/>

upvoted 2 times

 **taustin2** 2 months, 1 week ago

Selected Answer: A

S3 Cross-Region Replication is least operational overhead.

upvoted 2 times

A company is creating a new web application for its subscribers. The application will consist of a static single page and a persistent database layer. The application will have millions of users for 4 hours in the morning, but the application will have only a few thousand users during the rest of the day. The company's data architects have requested the ability to rapidly evolve their schema.

Which solutions will meet these requirements and provide the MOST scalability? (Choose two.)

- A. Deploy Amazon DynamoDB as the database solution. Provision on-demand capacity.
- B. Deploy Amazon Aurora as the database solution. Choose the serverless DB engine mode.
- C. Deploy Amazon DynamoDB as the database solution. Ensure that DynamoDB auto scaling is enabled.
- D. Deploy the static content into an Amazon S3 bucket. Provision an Amazon CloudFront distribution with the S3 bucket as the origin.
- E. Deploy the web servers for static content across a fleet of Amazon EC2 instances in Auto Scaling groups. Configure the instances to periodically refresh the content from an Amazon Elastic File System (Amazon EFS) volume.

Correct Answer: CD

Community vote distribution

AD (50%)	CD (44%)	6%
----------	----------	----

✉  **t0nx** 6 days, 1 hour ago

Selected Answer: CD

CD as pattern is known
upvoted 1 times

✉  **bogobob** 1 week, 6 days ago

Selected Answer: CD

For those answering A over C, the question asks about scalability, but the text says the traffic patterns are known and don't state they will change. Both auto-scaling and on-demand can "scale", but auto-scaling is for known, on-demand is better for unknown traffic patterns. Its likely the "scalability" is more to do with the file hosting (EC2 wouldn't scale well at all vs S3)
upvoted 2 times

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: AD

B is valid, but not good as A
upvoted 1 times

✉  **dilaaziz** 4 weeks ago

Selected Answer: CD

It is a known traffic
<https://aws.amazon.com/dynamodb/pricing/>
upvoted 1 times

✉  **wsdasdasdqwdaw** 1 month ago

Okay, it is clear AD vs CD. The question is about providing the MOST scalability solution"
A is providing much more scalability compared to C. I would go for AD.
upvoted 1 times

✉  **potomac** 1 month ago

AD

For tables using on-demand mode, DynamoDB instantly accommodates customers' workloads as they ramp up or down to any previously observed traffic level. If the level of traffic hits a new peak, DynamoDB adapts rapidly to accommodate the workload.

<https://aws.amazon.com/blogs/aws/amazon-dynamodb-on-demand-no-capacity-planning-and-pay-per-request-pricing/>
upvoted 1 times

✉  **Wayne23Fang** 1 month ago

Selected Answer: C

Quoted from DynamoDB On-Demand Scaling vs Provisioned with Auto-Scaling [The Ultimate Comparison] Charlie Fish Published on October 25th, 2021:
This means Auto-Scaling is best for situations where traffic will scale gradually and not incur sudden spikes of traffic. For most applications this is fine, traffic normally spikes during the middle of the day, and tapers off overnight. But it is important to understand that Auto-Scaling and changes to provisioned capacity is not instantaneous. Also He mentioned AWS allows multiple capacity decrease through a day with provisioned mode. But agree it is tough call to compare. User bsbs1234's comment is valid. But it is arguable that the traffic pattern is considered consistent.
upvoted 1 times

 **bsbs1234** 1 month, 2 weeks ago

CD:

Was think AD, but after read comments. I think it should be CD. Because the traffic pattern is known. On-Demand is more suitable when traffic pattern is not clear. Provision with auto-scaling should be more cost efficient.

upvoted 1 times

 **Xin123** 2 months ago

Selected Answer: AD

Remember for Provisioned with Auto-Scaling you are basically paying for throughput 24/7. Whereas for On-Demand Scaling you pay per request. This means for applications still in development or low traffic applications, it might be more economical to use On-Demand Scaling and not worry about provisioning throughput. However, at scale, this can quickly shift once you have a more consistent usage pattern.

<https://dynobase.dev/dynamodb-on-demand-vs-provisioned-scaling/>

upvoted 3 times

 **taustin2** 2 months ago

Selected Answer: AD

Changing answer to A,D. DynamoDB on-demand is more scalable than DynamoDB auto-scaling.

upvoted 4 times

 **Jay2k23** 2 months ago

Selected Answer: AD

A: DynamoDB on-demand mode make automatically scale up and down with your workload.

D: S3 for static web site

upvoted 2 times

 **Guru4Cloud** 2 months ago

Selected Answer: CD

The key reasons are:

DynamoDB auto scaling allows the database to scale up and down dynamically based on traffic patterns. This handles the large spike in traffic in the mornings and lower traffic later in the day.

S3 combined with CloudFront provides a highly scalable infrastructure for the static content. CloudFront caching improves performance.

Aurora serverless could be an option but may not scale as seamlessly as DynamoDB to the very high spike in users.

EC2 Auto Scaling groups add complexity compared to S3/CloudFront for static content hosting.

upvoted 1 times

 **taustin2** 2 months, 1 week ago

Selected Answer: CD

Static content = S3 + CloudFront. Radidly scale and rapidly evolve schema = DynamoDB with auto-scaling enabled (which it is by default).

upvoted 2 times

A company uses Amazon API Gateway to manage its REST APIs that third-party service providers access. The company must protect the REST APIs from SQL injection and cross-site scripting attacks.

What is the MOST operationally efficient solution that meets these requirements?

- A. Configure AWS Shield.
- B. Configure AWS WAF.
- C. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS Shield in CloudFront.
- D. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS WAF in CloudFront.

Correct Answer: A

Community vote distribution

B (100%)

✉  **taustin2** Highly Voted 2 months, 1 week ago

Selected Answer: B

SQL Injection and Cross-Site Scripting = WAF so Either B or D. Both B and D are valid options but the question doesn't indicate a real need for CloudFront, so just use WAF with the API Gateway. Answer is B.

upvoted 7 times

✉  **awslearnerin2022** Highly Voted 2 months, 1 week ago

Selected Answer: B

WAF helps with layer 7 attacks like SQL injection and XSS. Shield is helpful for DDOS attacks.

upvoted 6 times

✉  **potomac** Most Recent 3 weeks, 1 day ago

Selected Answer: B

B or D

But no need for CloudFront

upvoted 1 times

✉  **Sugarbear_01** 1 month ago

Selected Answer: B

AWS WAF protect agains :

Presence of SQL code that is likely to be malicious (known as SQL injection).

Presence of a script that is likely to be malicious (known as cross-site scripting).

AWS Shield provides protection against distributed denial of service (DDoS) attacks for AWS resources, at the network and transport layers (layer 3 and 4) and the application layer (layer 7).

<https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

upvoted 1 times

✉  **thanhnv142** 1 month, 1 week ago

Finally, I am here at the end. Thank you guys for your support!

upvoted 4 times

✉  **Guru4Cloud** 2 months ago

Selected Answer: B

B. Configure AWS WAF.

upvoted 4 times

✉  **aleariva** 2 months, 1 week ago

B is the correct. <https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html>

upvoted 3 times

A company wants to provide users with access to AWS resources. The company has 1,500 users and manages their access to on-premises resources through Active Directory user groups on the corporate network. However, the company does not want users to have to maintain another identity to access the resources. A solutions architect must manage user access to the AWS resources while preserving access to the on-premises resources.

What should the solutions architect do to meet these requirements?

- A. Create an IAM user for each user in the company. Attach the appropriate policies to each user.
- B. Use Amazon Cognito with an Active Directory user pool. Create roles with the appropriate policies attached.
- C. Define cross-account roles with the appropriate policies attached. Map the roles to the Active Directory groups.
- D. Configure Security Assertion Markup Language (SAML) 2.0-based federation. Create roles with the appropriate policies attached. Map the roles to the Active Directory groups.

Correct Answer: D

Community vote distribution

D (75%)

B (25%)

 **NickGordon** 2 weeks, 5 days ago

Selected Answer: D

D.

An Amazon Cognito user pool is a user directory for WEB and MOBILE app authentication and authorization. So it is not a best option for corporate users.

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: D

I think it is D

upvoted 1 times

 **ahlofan** 3 weeks, 3 days ago

Selected Answer: B

Access to Aws resource -> cognito, then use iam role
SAML or AD -> identity pool

upvoted 1 times

 **dilaaziz** 3 weeks, 4 days ago

Selected Answer: D

<https://aws.amazon.com/identity/saml/>

upvoted 1 times

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF
- C. Configure Amazon Route 53 with a geolocation policy
- D. Configure Amazon Route 53 with a geoproximity routing policy

Correct Answer: A

Community vote distribution

C (100%)

 **LemonGremlin** 2 weeks ago

It is C

upvoted 1 times

 **shihabnoori** 3 weeks, 1 day ago

C. Configure Amazon Route 53 with a geolocation policy

upvoted 2 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

Geolocation routing policy — Use when you want to route traffic based on the location of users.

Geo-proximity routing policy — Use when you want to route traffic based on the location of your resources and optionally switch resource traffic at one location to resources elsewhere.

upvoted 3 times

 **dilaaziz** 3 weeks, 4 days ago

Selected Answer: C

<https://aws.amazon.com/about-aws/whats-new/2014/07/31/amazon-route-53-announces-domain-name-registration-geo-routing-and-lower-pricing/>

upvoted 1 times

A company stores its data on premises. The amount of data is growing beyond the company's available capacity.

The company wants to migrate its data from the on-premises location to an Amazon S3 bucket. The company needs a solution that will automatically validate the integrity of the data after the transfer.

Which solution will meet these requirements?

- A. Order an AWS Snowball Edge device. Configure the Snowball Edge device to perform the online data transfer to an S3 bucket
- B. Deploy an AWS DataSync agent on premises. Configure the DataSync agent to perform the online data transfer to an S3 bucket.
- C. Create an Amazon S3 File Gateway on premises. Configure the S3 File Gateway to perform the online data transfer to an S3 bucket
- D. Configure an accelerator in Amazon S3 Transfer Acceleration on premises. Configure the accelerator to perform the online data transfer to an S3 bucket.

Correct Answer: B

Community vote distribution

B (100%)

 **potomac** 3 weeks, 1 day ago

Selected Answer: B

During a transfer, AWS DataSync always checks the integrity of your data, but you can specify how and when this verification happens with the following options: Verify only the data transferred (recommended) – DataSync calculates the checksum of transferred files and metadata at the source location.

<https://docs.aws.amazon.com/datasync/latest/userguide/configure-data-verification-options.html>

upvoted 2 times

 **dilaaziz** 3 weeks, 4 days ago

Selected Answer: B

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

upvoted 1 times

A company wants to migrate two DNS servers to AWS. The servers host a total of approximately 200 zones and receive 1 million requests each day on average. The company wants to maximize availability while minimizing the operational overhead that is related to the management of the two servers.

What should a solutions architect recommend to meet these requirements?

- A. Create 200 new hosted zones in the Amazon Route 53 console Import zone files.
- B. Launch a single large Amazon EC2 instance Import zone files. Configure Amazon CloudWatch alarms and notifications to alert the company about any downtime.
- C. Migrate the servers to AWS by using AWS Server Migration Service (AWS SMS). Configure Amazon CloudWatch alarms and notifications to alert the company about any downtime.
- D. Launch an Amazon EC2 instance in an Auto Scaling group across two Availability Zones. Import zone files. Set the desired capacity to 1 and the maximum capacity to 3 for the Auto Scaling group. Configure scaling alarms to scale based on CPU utilization.

Correct Answer: A

Community vote distribution

A (75%) D (25%)

 **EdenWang** 1 week, 3 days ago

Selected Answer: A

Only A makes sense
upvoted 1 times

 **NickGordon** 2 weeks, 5 days ago

Selected Answer: A

Should be A

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/migrate-dns-domain-in-use.html>
upvoted 2 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: D

D makes more sense to me
upvoted 1 times

A global company runs its applications in multiple AWS accounts in AWS Organizations. The company's applications use multipart uploads to upload data to multiple Amazon S3 buckets across AWS Regions. The company wants to report on incomplete multipart uploads for cost compliance purposes.

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

- A. Configure AWS Config with a rule to report the incomplete multipart upload object count.
- B. Create a service control policy (SCP) to report the incomplete multipart upload object count.
- C. Configure S3 Storage Lens to report the incomplete multipart upload object count.
- D. Create an S3 Multi-Region Access Point to report the incomplete multipart upload object count.

Correct Answer: C

Community vote distribution

C (100%)

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

C for sure

upvoted 1 times

 **warp** 3 weeks, 2 days ago

Selected Answer: C

S3 storage lenses can be used to find incomplete multipart uploads: <https://aws.amazon.com/blogs/aws-cloud-financial-management/discovering-and-deleting-incomplete-multipart-uploads-to-lower-amazon-s3-costs/>

upvoted 4 times

A company runs a production database on Amazon RDS for MySQL. The company wants to upgrade the database version for security compliance reasons. Because the database contains critical data, the company wants a quick solution to upgrade and test functionality without losing any data.

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

- A. Create an RDS manual snapshot. Upgrade to the new version of Amazon RDS for MySQL.
- B. Use native backup and restore. Restore the data to the upgraded new version of Amazon RDS for MySQL.
- C. Use AWS Database Migration Service (AWS DMS) to replicate the data to the upgraded new version of Amazon RDS for MySQL.
- D. Use Amazon RDS Blue/Green Deployments to deploy and test production changes.

Correct Answer: D

Community vote distribution

D (100%)

 **potomac** 3 weeks, 1 day ago

Selected Answer: D

D is the answer
upvoted 1 times

 **warp** 3 weeks, 2 days ago

Selected Answer: D

You can make changes to the RDS DB instances in the green environment without affecting production workloads. For example, you can upgrade the major or minor DB engine version, upgrade the underlying file system configuration, or change database parameters in the staging environment. You can thoroughly test changes in the green environment.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/blue-green-deployments-overview.html>

upvoted 3 times

A solutions architect is creating a data processing job that runs once daily and can take up to 2 hours to complete. If the job is interrupted, it has to restart from the beginning.

How should the solutions architect address this issue in the MOST cost-effective manner?

- A. Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.
- B. Create an AWS Lambda function triggered by an Amazon EventBridge scheduled event.
- C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge scheduled event.
- D. Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge scheduled event.

Correct Answer: C

Community vote distribution

C (67%) B (33%)

✉️  **Alex1atd** 1 week, 1 day ago

Selected Answer: C

Lambda function have a limit timeout about 15 minutes, so cannot be B.

Answer is C

upvoted 1 times

✉️  **hungta** 2 weeks, 1 day ago

Selected Answer: C

Lamda function have a limit timeout about 15 minutes

upvoted 1 times

✉️  **cciesam** 2 weeks, 4 days ago

Selected Answer: B

I think it should be B. Considering the Cost.

upvoted 2 times

✉️  **zhdetn** 2 weeks, 1 day ago

Lambda Maximum execution time: 900 seconds (15 minutes)

upvoted 3 times

✉️  **potomac** 3 weeks, 1 day ago

Selected Answer: C

I guess it is C

upvoted 2 times

A social media company wants to store its database of user profiles, relationships, and interactions in the AWS Cloud. The company needs an application to monitor any changes in the database. The application needs to analyze the relationships between the data entities and to provide recommendations to users.

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

- A. Use Amazon Neptune to store the information. Use Amazon Kinesis Data Streams to process changes in the database.
- B. Use Amazon Neptune to store the information. Use Neptune Streams to process changes in the database.
- C. Use Amazon Quantum Ledger Database (Amazon QLDB) to store the information. Use Amazon Kinesis Data Streams to process changes in the database.
- D. Use Amazon Quantum Ledger Database (Amazon QLDB) to store the information. Use Neptune Streams to process changes in the database.

Correct Answer: B

Community vote distribution

B (80%)

C (20%)

 **NickGordon** 2 weeks, 5 days ago

Selected Answer: B

B

Social network -> Graph Structure -> Neptune
upvoted 1 times

 **ekisako** 2 weeks, 6 days ago

Selected Answer: B

Keyword: analyze the relationships
With Amazon Neptune, you can create sophisticated, interactive graph applications that can query billions of relationships in milliseconds.

<https://aws.amazon.com/neptune/features/>
upvoted 2 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

Amazon Neptune is primarily used for managing highly connected graph data, making it well-suited for graph-based applications.

In contrast, Amazon QLDB is designed for applications that require an immutable and auditable transaction history to ensure data integrity.
upvoted 1 times

 **warp** 3 weeks, 2 days ago

Selected Answer: B

Neptune is a graph type database and Neptune streams provides view on changes into the database:

<https://docs.aws.amazon.com/neptune/latest/userguide/streams.html>

upvoted 1 times

 **AF_1221** 3 weeks, 6 days ago

C is the correct answer
provides a well-suited, managed, and scalable solution for storing and monitoring the database with the least operational overhead, meeting the requirements of the social media company.
upvoted 2 times

A company is creating a new application that will store a large amount of data. The data will be analyzed hourly and will be modified by several Amazon EC2 Linux instances that are deployed across multiple Availability Zones. The needed amount of storage space will continue to grow for the next 6 months.

Which storage solution should a solutions architect recommend to meet these requirements?

- A. Store the data in Amazon S3 Glacier. Update the S3 Glacier vault policy to allow access to the application instances.
- B. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the application instances.
- C. Store the data in an Amazon Elastic File System (Amazon EFS) file system. Mount the file system on the application instances.
- D. Store the data in an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS volume shared between the application instances.

Correct Answer: C

Community vote distribution

C (100%)

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

C is correct

upvoted 1 times

 **AF_1221** 3 weeks, 6 days ago

C is correct

Shared File System: Amazon EFS allows multiple Amazon EC2 instances to mount the same file system simultaneously, making it easy for multiple instances to access and modify the data concurrently.

upvoted 3 times

A company manages an application that stores data on an Amazon RDS for PostgreSQL Multi-AZ DB instance. Increases in traffic are causing performance problems. The company determines that database queries are the primary reason for the slow performance.

What should a solutions architect do to improve the application's performance?

- A. Serve read traffic from the Multi-AZ standby replica.
- B. Configure the DB instance to use Transfer Acceleration.
- C. Create a read replica from the source DB instance. Serve read traffic from the read replica.
- D. Use Amazon Kinesis Data Firehose between the application and Amazon RDS to increase the concurrency of database requests.

Correct Answer: C

Community vote distribution

C (100%)

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

you can't read from the standby DB instance. If applications require more read capacity, you should create or add additional read replicas.
upvoted 1 times

 **warp** 3 weeks, 1 day ago

Selected Answer: C

After you create a read replica from a source DB instance, the source becomes the primary DB instance. When you make updates to the primary DB instance, Amazon RDS copies them asynchronously to the read replica.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html
upvoted 1 times

A company collects 10 GB of telemetry data daily from various machines. The company stores the data in an Amazon S3 bucket in a source data account.

The company has hired several consulting agencies to use this data for analysis. Each agency needs read access to the data for its analysts. The company must share the data from the source data account by choosing a solution that maximizes security and operational efficiency.

Which solution will meet these requirements?

- A. Configure S3 global tables to replicate data for each agency.
- B. Make the S3 bucket public for a limited time. Inform only the agencies.
- C. Configure cross-account access for the S3 bucket to the accounts that the agencies own.
- D. Set up an IAM user for each analyst in the source data account. Grant each user access to the S3 bucket.

Correct Answer: C

Community vote distribution

C (67%) D (33%)

✉  **NickGordon** 2 weeks, 5 days ago

Selected Answer: C

C is the best answer
upvoted 1 times

✉  **cciesam** 2 weeks, 5 days ago

Selected Answer: D

C may not correct as it's doesn't say if the analyst are using AWS services
upvoted 1 times

✉  **NickGordon** 2 weeks, 5 days ago

in that case, an analyst user group should be created and the access should be assigned to the group. So C is better
upvoted 1 times

✉  **potomac** 3 weeks, 1 day ago

Selected Answer: C

I think it is C
upvoted 1 times

A company uses Amazon FSx for NetApp ONTAP in its primary AWS Region for CIFS and NFS file shares. Applications that run on Amazon EC2 instances access the file shares. The company needs a storage disaster recovery (DR) solution in a secondary Region. The data that is replicated in the secondary Region needs to be accessed by using the same protocols as the primary Region.

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

- A. Create an AWS Lambda function to copy the data to an Amazon S3 bucket. Replicate the S3 bucket to the secondary Region.
- B. Create a backup of the FSx for ONTAP volumes by using AWS Backup. Copy the volumes to the secondary Region. Create a new FSx for ONTAP instance from the backup.
- C. Create an FSx for ONTAP instance in the secondary Region. Use NetApp SnapMirror to replicate data from the primary Region to the secondary Region.
- D. Create an Amazon Elastic File System (Amazon EFS) volume. Migrate the current data to the volume. Replicate the volume to the secondary Region.

Correct Answer: C

Community vote distribution

C (100%)

 **Oblako** 1 week ago

Selected Answer: C

SnapMirror enables you to configure replication with an RPO of as low as five minutes, and an RTO in single digit minutes. It is the recommended solution for DR when using FSx for ONTAP: <https://aws.amazon.com/blogs/storage/cross-region-disaster-recovery-with-amazon-fsx-for-netapp-ontap/>

upvoted 1 times

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

You can use NetApp SnapMirror to schedule periodic replication of your FSx for ONTAP file system to or from a second file system. This capability is available for both in-Region and cross-Region deployments.

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/scheduled-replication.html>

upvoted 2 times

A development team is creating an event-based application that uses AWS Lambda functions. Events will be generated when files are added to an Amazon S3 bucket. The development team currently has Amazon Simple Notification Service (Amazon SNS) configured as the event target from Amazon S3.

What should a solutions architect do to process the events from Amazon S3 in a scalable way?

- A. Create an SNS subscription that processes the event in Amazon Elastic Container Service (Amazon ECS) before the event runs in Lambda.
- B. Create an SNS subscription that processes the event in Amazon Elastic Kubernetes Service (Amazon EKS) before the event runs in Lambda
- C. Create an SNS subscription that sends the event to Amazon Simple Queue Service (Amazon SQS). Configure the SQS queue to trigger a Lambda function.
- D. Create an SNS subscription that sends the event to AWS Server Migration Service (AWS SMS). Configure the Lambda function to poll from the SMS event.

Correct Answer: C

Community vote distribution

C (100%)

 **potomac** 3 weeks, 1 day ago

Selected Answer: C

Amazon SQS is designed for event-driven and scalable message processing. It can handle large volumes of messages and automatically scales based on the incoming workload. This allows for better load distribution and scaling as compared to direct Lambda invocation.

upvoted 3 times

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Choose two.)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Correct Answer: BC

Community vote distribution

BC (100%)

 **potomac** Highly Voted  3 weeks, 1 day ago

Selected Answer: BC

B and C

upvoted 7 times

A company collects and shares research data with the company's employees all over the world. The company wants to collect and store the data in an Amazon S3 bucket and process the data in the AWS Cloud. The company will share the data with the company's employees. The company needs a secure solution in the AWS Cloud that minimizes operational overhead.

Which solution will meet these requirements?

- A. Use an AWS Lambda function to create an S3 presigned URL. Instruct employees to use the URL.
- B. Create an IAM user for each employee. Create an IAM policy for each employee to allow S3 access. Instruct employees to use the AWS Management Console.
- C. Create an S3 File Gateway. Create a share for uploading and a share for downloading. Allow employees to mount shares on their local computers to use S3 File Gateway.
- D. Configure AWS Transfer Family SFTP endpoints. Select the custom identity provider options. Use AWS Secrets Manager to manage the user credentials. Instruct employees to use Transfer Family.

Correct Answer: D

Community vote distribution

A (56%)	D (33%)	11%
---------	---------	-----

 **AwsZora** 4 days, 21 hours ago

Selected Answer: A

A is simple
upvoted 1 times

 **t0nx** 6 days, 1 hour ago

Selected Answer: D

AWS Transfer Family (Option D)

By configuring AWS Transfer Family SFTP endpoints, you can provide a secure and convenient way for employees to access and transfer data to and from the S3 bucket.

Using custom identity provider options allows you to integrate with existing identity systems, and AWS Secrets Manager can be used to manage user credentials securely.

A suggests using an AWS Lambda function to create an S3 presigned URL. While this can work, it involves manual generation of URLs and sharing them, which may not be as scalable or user-friendly.

B suggests creating an IAM user for each employee with IAM policies for S3 access. This involves more operational overhead, as managing IAM users for each employee can be cumbersome and less scalable.

C suggests using an S3 File Gateway. While this can work, it introduces additional components and may not be as straightforward or as efficient as using AWS Transfer Family for SFTP access.

upvoted 3 times

 **Oblako** 1 week ago

Selected Answer: B

C and D are incorrect as the data will be processed in AWS, no need to download, transfer.

A, I believe is also incorrect. As it is not operationally efficient to use a lambda function to generate Presigned URLs when using the data within AWS. Let's say an employee of that company wants to process millions of those files in SageMaker for a study. This would mean they'd have to invoke this lambda function millions of times to generate pre-signed URLs for all of these files. Not really efficient.

Nothing is really wrong with answer B. As it is the employees will process the data in the AWS Cloud, they need an IAM user anyway. It seems a bit odd that the answer states: "Create an IAM policy for each employee to allow S3 access". As this should be done using a group. But still I am going with B.

upvoted 1 times

 **potomac** 3 weeks ago

Selected Answer: A

D is not for minimizing operational overhead

upvoted 4 times

A company is building a new furniture inventory application. The company has deployed the application on a fleet of Amazon EC2 instances across multiple Availability Zones. The EC2 instances run behind an Application Load Balancer (ALB) in their VPC.

A solutions architect has observed that incoming traffic seems to favor one EC2 instance, resulting in latency for some requests.

What should the solutions architect do to resolve this issue?

- A. Disable session affinity (sticky sessions) on the ALB
- B. Replace the ALB with a Network Load Balancer
- C. Increase the number of EC2 instances in each Availability Zone
- D. Adjust the frequency of the health checks on the ALB's target group

Correct Answer: A

Community vote distribution

A (100%)

 **NickGordon** 2 weeks, 5 days ago

Selected Answer: A

A

<https://repost.aws/knowledge-center/elb-fix-unequal-traffic-routing>
upvoted 1 times

 **potomac** 3 weeks ago

Selected Answer: A

A makes more sense than others
upvoted 2 times

A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS Key Management Service (AWS KMS) keys. A solutions architect needs to design a solution that will ensure the required permissions are set correctly.

Which combination of actions accomplish this? (Choose two.)

- A. Attach the kms:decrypt permission to the Lambda function's resource policy
- B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy
- C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
- D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.
- E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

Correct Answer: BE

Community vote distribution

BE (71%) 14% 14%

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

Selected Answer: BE

BE is right.

The key policy has to be modified to give lambda execution role access. You can't set another resource policy as principle. So C is not right
upvoted 5 times

✉  **louisaok**  2 weeks, 6 days ago

Selected Answer: CE

CE is right

upvoted 1 times

✉  **potomac** 3 weeks ago

Selected Answer: DE

DE?

Create an IAM role for the Lambda function that also grants decryption permission to the S3 bucket.
Configure the IAM role as the Lambda functions execution role.

To use an IAM policy to control access to a KMS key, the key policy for the KMS key must give the account permission to use IAM policies.

<https://repost.aws/knowledge-center/lambda-execution-role-s3-bucket>
<https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html>

upvoted 1 times

✉  **potomac** 3 weeks ago

change to CE

C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.

E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

<https://docs.aws.amazon.com/lambda/latest/dg/access-control-resource-based.html>
<https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html>

upvoted 2 times

A company wants to monitor its AWS costs for financial review. The cloud operations team is designing an architecture in the AWS Organizations management account to query AWS Cost and Usage Reports for all member accounts. The team must run this query once a month and provide a detailed analysis of the bill.

Which solution is the MOST scalable and cost-effective way to meet these requirements?

- A. Enable Cost and Usage Reports in the management account. Deliver reports to Amazon Kinesis. Use Amazon EMR for analysis.
- B. Enable Cost and Usage Reports in the management account. Deliver the reports to Amazon S3 Use Amazon Athena for analysis.
- C. Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon S3 Use Amazon Redshift for analysis.
- D. Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon Kinesis. Use Amazon QuickSight for analysis.

Correct Answer: B*Community vote distribution*

B (100%)

 **NickGordon** 2 weeks, 5 days ago

Selected Answer: B

B

<https://aws.amazon.com/blogs/big-data/analyze-amazon-s3-storage-costs-using-aws-cost-and-usage-reports-amazon-s3-inventory-and-amazon-athena/>

upvoted 2 times

 **potomac** 3 weeks ago

Selected Answer: B

B

once a month

upvoted 2 times

A company wants to run a gaming application on Amazon EC2 instances that are part of an Auto Scaling group in the AWS Cloud. The application will transmit data by using UDP packets. The company wants to ensure that the application can scale out and in as traffic increases and decreases.

What should a solutions architect do to meet these requirements?

- A. Attach a Network Load Balancer to the Auto Scaling group.
- B. Attach an Application Load Balancer to the Auto Scaling group.
- C. Deploy an Amazon Route 53 record set with a weighted policy to route traffic appropriately.
- D. Deploy a NAT instance that is configured with port forwarding to the EC2 instances in the Auto Scaling group.

Correct Answer: A*Community vote distribution*

A (100%)

 **Sugarbear_01**  3 weeks, 5 days ago

Selected Answer: A

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>

upvoted 7 times

A company runs several websites on AWS for its different brands. Each website generates tens of gigabytes of web traffic logs each day. A solutions architect needs to design a scalable solution to give the company's developers the ability to analyze traffic patterns across all the company's websites. This analysis by the developers will occur on demand once a week over the course of several months. The solution must support queries with standard SQL.

Which solution will meet these requirements MOST cost-effectively?

- A. Store the logs in Amazon S3. Use Amazon Athena for analysis.
- B. Store the logs in Amazon RDS. Use a database client for analysis.
- C. Store the logs in Amazon OpenSearch Service. Use OpenSearch Service for analysis.
- D. Store the logs in an Amazon EMR cluster. Use a supported open-source framework for SQL-based analysis.

Correct Answer: A

Community vote distribution

A (100%)

 **NickGordon** 2 weeks, 5 days ago

Selected Answer: A

A, most cost effective
upvoted 1 times

 **potomac** 3 weeks ago

Selected Answer: A

option D (using Amazon EMR with an open-source framework) may be overkill for the relatively simple SQL-based analysis.
upvoted 1 times

An international company has a subdomain for each country that the company operates in. The subdomains are formatted as example.com, country1.example.com, and country2.example.com. The company's workloads are behind an Application Load Balancer. The company wants to encrypt the website data that is in transit.

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

- A. Use the AWS Certificate Manager (ACM) console to request a public certificate for the apex top domain example.com and a wildcard certificate for *.example.com.
- B. Use the AWS Certificate Manager (ACM) console to request a private certificate for the apex top domain example.com and a wildcard certificate for *.example.com.
- C. Use the AWS Certificate Manager (ACM) console to request a public and private certificate for the apex top domain example.com.
- D. Validate domain ownership by email address. Switch to DNS validation by adding the required DNS records to the DNS provider.
- E. Validate domain ownership for the domain by adding the required DNS records to the DNS provider.

Correct Answer: AE

Community vote distribution

AE (100%)

 **cciesam** 3 weeks ago

Selected Answer: AE

AE correct

upvoted 1 times

 **potomac** 3 weeks ago

Selected Answer: AE

BCD are wrong

upvoted 2 times

 **t0nx** 6 days, 22 hours ago

Why E and not D ?

upvoted 1 times

A company is required to use cryptographic keys in its on-premises key manager. The key manager is outside of the AWS Cloud because of regulatory and compliance requirements. The company wants to manage encryption and decryption by using cryptographic keys that are retained outside of the AWS Cloud and that support a variety of external key managers from different vendors.

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

- A. Use AWS CloudHSM key store backed by a CloudHSM cluster.
- B. Use an AWS Key Management Service (AWS KMS) external key store backed by an external key manager.
- C. Use the default AWS Key Management Service (AWS KMS) managed key store.
- D. Use a custom key store backed by an AWS CloudHSM cluster.

Correct Answer: B

Community vote distribution

B (100%)

 **1rob** 1 week, 1 day ago

Selected Answer: B

Answer A does not comply because aws cloudHSM is within aws

Answer B is the correct answer because the company is required to use its on-premises key manager. Following

<https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html> gives :An external key store is an AWS KMS custom key store backed by an external key manager outside of AWS that you own and control.(...)

Answer C and D are both solutions in the aws cloud so that does not fit.

upvoted 1 times

 **potomac** 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html>

upvoted 4 times

A solutions architect needs to host a high performance computing (HPC) workload in the AWS Cloud. The workload will run on hundreds of Amazon EC2 instances and will require parallel access to a shared file system to enable distributed processing of large datasets. Datasets will be accessed across multiple instances simultaneously. The workload requires access latency within 1 ms. After processing has completed, engineers will need access to the dataset for manual postprocessing.

Which solution will meet these requirements?

- A. Use Amazon Elastic File System (Amazon EFS) as a shared file system. Access the dataset from Amazon EFS.
- B. Mount an Amazon S3 bucket to serve as the shared file system. Perform postprocessing directly from the S3 bucket.
- C. Use Amazon FSx for Lustre as a shared file system. Link the file system to an Amazon S3 bucket for postprocessing.
- D. Configure AWS Resource Access Manager to share an Amazon S3 bucket so that it can be mounted to all instances for processing and postprocessing.

Correct Answer: C

Community vote distribution

C (100%)

 **potomac** 3 weeks ago

Selected Answer: C

Amazon FSx for Lustre is a fully managed, high-performance file system optimized for HPC workloads. It is designed to deliver sub-millisecond latencies and high throughput, making it ideal for applications that require parallel access to shared storage, such as simulations and data analytics.
upvoted 3 times

A gaming company is building an application with Voice over IP capabilities. The application will serve traffic to users across the world. The application needs to be highly available with an automated failover across AWS Regions. The company wants to minimize the latency of users without relying on IP address caching on user devices.

What should a solutions architect do to meet these requirements?

- A. Use AWS Global Accelerator with health checks.
- B. Use Amazon Route 53 with a geolocation routing policy.
- C. Create an Amazon CloudFront distribution that includes multiple origins.
- D. Create an Application Load Balancer that uses path-based routing.

Correct Answer: A

Community vote distribution

A (89%)

11%

 **ekisako** 2 weeks, 6 days ago

Selected Answer: A

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html>

upvoted 2 times

 **cciesam** 2 weeks, 6 days ago

Selected Answer: A

Global Accelerator is the answer as it can handle both TCP and UDP

upvoted 2 times

 **potomac** 3 weeks ago

Selected Answer: A

Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

upvoted 4 times

 **Sugarbear_01** 3 weeks, 5 days ago

Selected Answer: C

This answer should be C

upvoted 1 times

A weather forecasting company needs to process hundreds of gigabytes of data with sub-millisecond latency. The company has a high performance computing (HPC) environment in its data center and wants to expand its forecasting capabilities.

A solutions architect must identify a highly available cloud storage solution that can handle large amounts of sustained throughput. Files that are stored in the solution should be accessible to thousands of compute instances that will simultaneously access and process the entire dataset.

What should the solutions architect do to meet these requirements?

- A. Use Amazon FSx for Lustre scratch file systems.
- B. Use Amazon FSx for Lustre persistent file systems.
- C. Use Amazon Elastic File System (Amazon EFS) with Bursting Throughput mode.
- D. Use Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.

Correct Answer: B

Community vote distribution

B (100%)

 **potomac** 3 weeks ago

Selected Answer: B

Option A (Amazon FSx for Lustre scratch file systems) is designed for temporary data storage and does not provide the data persistence required for this scenario.

upvoted 3 times

An ecommerce company runs a PostgreSQL database on premises. The database stores data by using high IOPS Amazon Elastic Block Store (Amazon EBS) block storage. The daily peak I/O transactions per second do not exceed 15,000 IOPS. The company wants to migrate the database to Amazon RDS for PostgreSQL and provision disk IOPS performance independent of disk storage capacity.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure the General Purpose SSD (gp2) EBS volume storage type and provision 15,000 IOPS.
- B. Configure the Provisioned IOPS SSD (io1) EBS volume storage type and provision 15,000 IOPS.
- C. Configure the General Purpose SSD (gp3) EBS volume storage type and provision 15,000 IOPS.
- D. Configure the EBS magnetic volume type to achieve maximum IOPS.

Correct Answer: C

Community vote distribution

C (100%)

 **Oblako** 1 week ago

Selected Answer: C

Both gp2 and gp3 can provision up to 16,000 IOPS. gp3 is cheaper than gp2.

upvoted 1 times

 **lagorb** 2 weeks, 2 days ago

gp2 and gp3 can provision up to 16,000 IOPS, and gp3 is cheaper than gp2

upvoted 2 times

 **potomac** 3 weeks ago

Selected Answer: C

GP3 is better and cheaper than GP2

upvoted 2 times

A company wants to migrate its on-premises Microsoft SQL Server Enterprise edition database to AWS. The company's online application uses the database to process transactions. The data analysis team uses the same production database to run reports for analytical processing. The company wants to reduce operational overhead by moving to managed services wherever possible.

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

- A. Migrate to Amazon RDS for Microsoft SQL Server. Use read replicas for reporting purposes
- B. Migrate to Microsoft SQL Server on Amazon EC2. Use Always On read replicas for reporting purposes
- C. Migrate to Amazon DynamoDB. Use DynamoDB on-demand replicas for reporting purposes
- D. Migrate to Amazon Aurora MySQL. Use Aurora read replicas for reporting purposes

Correct Answer: A

Community vote distribution

A (100%)

 **potomac** 3 weeks ago

Selected Answer: A

A is the only choice

upvoted 3 times

A company stores a large volume of image files in an Amazon S3 bucket. The images need to be readily available for the first 180 days. The images are infrequently accessed for the next 180 days. After 360 days, the images need to be archived but must be available instantly upon request. After 5 years, only auditors can access the images. The auditors must be able to retrieve the images within 12 hours. The images cannot be lost during this process.

A developer will use S3 Standard storage for the first 180 days. The developer needs to configure an S3 Lifecycle rule.

Which solution will meet these requirements MOST cost-effectively?

- A. Transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 180 days. S3 Glacier Instant Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.
- B. Transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 180 days. S3 Glacier Flexible Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.
- C. Transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days, S3 Glacier Instant Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.
- D. Transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days, S3 Glacier Flexible Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.

Correct Answer: C

Community vote distribution

C (64%)

A (36%)

 **Alex1atd** 1 week ago

Selected Answer: C

The images cannot be lost during this process.

upvoted 2 times

 **1rob** 1 week, 1 day ago

Selected Answer: C

"The images cannot be lost during this process" , imho this rules out S3 One zone infrequent access. S3 Glacier Instant Retrieval gives immediate access. S3 Glacier Flexible Retrieval does not give immediate access. so C.

upvoted 2 times

 **EdenWang** 1 week, 3 days ago

Selected Answer: A

high availability is not mentioned, thus I go for A

upvoted 1 times

 **cciesam** 3 weeks ago

Selected Answer: A

I'll go for A as it doesn't talk about High availability. Considering cost. I'll go for A

upvoted 3 times

 **ekisako** 2 weeks, 6 days ago

"The images cannot be lost during this process."

upvoted 2 times

 **dilaaziz** 3 weeks, 5 days ago

Selected Answer: C

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

upvoted 3 times

A company has a large data workload that runs for 6 hours each day. The company cannot lose any data while the process is running. A solutions architect is designing an Amazon EMR cluster configuration to support this critical data workload.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure a long-running cluster that runs the primary node and core nodes on On-Demand Instances and the task nodes on Spot Instances.
- B. Configure a transient cluster that runs the primary node and core nodes on On-Demand Instances and the task nodes on Spot Instances.
- C. Configure a transient cluster that runs the primary node on an On-Demand Instance and the core nodes and task nodes on Spot Instances.
- D. Configure a long-running cluster that runs the primary node on an On-Demand Instance, the core nodes on Spot Instances, and the task nodes on Spot Instances.

Correct Answer: B

Community vote distribution

B (100%)

 **potomac**  3 weeks ago

Selected Answer: B

A transient cluster provides cost savings because it runs only during the computation time, and it provides scalability and flexibility in a cloud environment.

Option C (transient cluster with On-Demand primary node and Spot core and task nodes) exposes the core nodes to Spot Instance interruptions, which may not be acceptable for a workload that cannot lose any data.

upvoted 7 times

 **louisaok**  2 weeks, 6 days ago

Relax man. take a break since you have made this far so far.

upvoted 6 times

 **MFKang**  1 week, 5 days ago

Get up Stand up

upvoted 1 times

A company maintains an Amazon RDS database that maps users to cost centers. The company has accounts in an organization in AWS Organizations. The company needs a solution that will tag all resources that are created in a specific AWS account in the organization. The solution must tag each resource with the cost center ID of the user who created the resource.

Which solution will meet these requirements?

- A. Move the specific AWS account to a new organizational unit (OU) in Organizations from the management account. Create a service control policy (SCP) that requires all existing resources to have the correct cost center tag before the resources are created. Apply the SCP to the new OU.
- B. Create an AWS Lambda function to tag the resources after the Lambda function looks up the appropriate cost center from the RDS database. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function.
- C. Create an AWS CloudFormation stack to deploy an AWS Lambda function. Configure the Lambda function to look up the appropriate cost center from the RDS database and to tag resources. Create an Amazon EventBridge scheduled rule to invoke the CloudFormation stack.
- D. Create an AWS Lambda function to tag the resources with a default value. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function when a resource is missing the cost center tag.

Correct Answer: B

Community vote distribution

B (100%)

 **t0nx** 6 days, 23 hours ago

Selected Answer: B

This solution utilizes AWS Lambda and Amazon EventBridge to automate the tagging process based on information from the RDS database and CloudTrail events.

AWS Lambda Function: Create a Lambda function that can look up the cost center information from the RDS database and tag resources accordingly.

Amazon EventBridge Rule: Set up an EventBridge rule to react to AWS CloudTrail events. The rule triggers the Lambda function whenever a resource is created, allowing dynamic tagging based on the cost center associated with the user in the RDS database.

This solution provides automation, ensuring that resources are tagged appropriately with the cost center ID of the user who created the resource. It also allows for flexibility in updating cost center information without modifying the infrastructure.

upvoted 3 times

A company recently migrated its web application to the AWS Cloud. The company uses an Amazon EC2 instance to run multiple processes to host the application. The processes include an Apache web server that serves static content. The Apache web server makes requests to a PHP application that uses a local Redis server for user sessions.

The company wants to redesign the architecture to be highly available and to use AWS managed solutions.

Which solution will meet these requirements?

- A. Use AWS Elastic Beanstalk to host the static content and the PHP application. Configure Elastic Beanstalk to deploy its EC2 instance into a public subnet. Assign a public IP address.
- B. Use AWS Lambda to host the static content and the PHP application. Use an Amazon API Gateway REST API to proxy requests to the Lambda function. Set the API Gateway CORS configuration to respond to the domain name. Configure Amazon ElastiCache for Redis to handle session information.
- C. Keep the backend code on the EC2 instance. Create an Amazon ElastiCache for Redis cluster that has Multi-AZ enabled. Configure the ElastiCache for Redis cluster in cluster mode. Copy the frontend resources to Amazon S3. Configure the backend code to reference the EC2 instance.
- D. Configure an Amazon CloudFront distribution with an Amazon S3 endpoint to an S3 bucket that is configured to host the static content. Configure an Application Load Balancer that targets an Amazon Elastic Container Service (Amazon ECS) service that runs AWS Fargate tasks for the PHP application. Configure the PHP application to use an Amazon ElastiCache for Redis cluster that runs in multiple Availability Zones.

Correct Answer: D

A company runs a web application on Amazon EC2 instances in an Auto Scaling group that has a target group. The company designed the application to work with session affinity (sticky sessions) for a better user experience.

The application must be available publicly over the internet as an endpoint. A WAF must be applied to the endpoint for additional security. Session affinity (sticky sessions) must be configured on the endpoint.

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

- A. Create a public Network Load Balancer. Specify the application target group.
- B. Create a Gateway Load Balancer. Specify the application target group.
- C. Create a public Application Load Balancer. Specify the application target group.
- D. Create a second target group. Add Elastic IP addresses to the EC2 instances.
- E. Create a web ACL in AWS WAF. Associate the web ACL with the endpoint

Correct Answer: CE

A company runs a website that stores images of historical events. Website users need the ability to search and view images based on the year that the event in the image occurred. On average, users request each image only once or twice a year. The company wants a highly available solution to store and deliver the images to users.

Which solution will meet these requirements MOST cost-effectively?

- A. Store images in Amazon Elastic Block Store (Amazon EBS). Use a web server that runs on Amazon EC2.
- B. Store images in Amazon Elastic File System (Amazon EFS). Use a web server that runs on Amazon EC2.
- C. Store images in Amazon S3 Standard. Use S3 Standard to directly deliver images by using a static website.
- D. Store images in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Use S3 Standard-IA to directly deliver images by using a static website.

Correct Answer: C

 **aragornfsm** 2 days, 20 hours ago

I believe the correct answer is option D, but ChatGPT mentioned option C. I didn't understand. I'm curious about the actual correct answer.
upvoted 1 times

 **chikuvan** 4 days, 4 hours ago

Selected Answer: D

users request each image only once or twice a year
So the answer is D

upvoted 2 times

A company has multiple AWS accounts in an organization in AWS Organizations that different business units use. The company has multiple offices around the world. The company needs to update security group rules to allow new office CIDR ranges or to remove old CIDR ranges across the organization. The company wants to centralize the management of security group rules to minimize the administrative overhead that updating CIDR ranges requires.

Which solution will meet these requirements MOST cost-effectively?

- A. Create VPC security groups in the organization's management account. Update the security groups when a CIDR range update is necessary.
- B. Create a VPC customer managed prefix list that contains the list of CIDRs. Use AWS Resource Access Manager (AWS RAM) to share the prefix list across the organization. Use the prefix list in the security groups across the organization.
- C. Create an AWS managed prefix list. Use an AWS Security Hub policy to enforce the security group update across the organization. Use an AWS Lambda function to update the prefix list automatically when the CIDR ranges change.
- D. Create security groups in a central administrative AWS account. Create an AWS Firewall Manager common security group policy for the whole organization. Select the previously created security groups as primary groups in the policy.

Correct Answer: B

A company uses an on-premises network-attached storage (NAS) system to provide file shares to its high performance computing (HPC) workloads. The company wants to migrate its latency-sensitive HPC workloads and its storage to the AWS Cloud. The company must be able to provide NFS and SMB multi-protocol access from the file system.

Which solution will meet these requirements with the LEAST latency? (Choose two.)

- A. Deploy compute optimized EC2 instances into a cluster placement group.
- B. Deploy compute optimized EC2 instances into a partition placement group.
- C. Attach the EC2 instances to an Amazon FSx for Lustre file system.
- D. Attach the EC2 instances to an Amazon FSx for OpenZFS file system.
- E. Attach the EC2 instances to an Amazon FSx for NetApp ONTAP file system.

Correct Answer: AE

✉  **chikuvan** 4 days, 4 hours ago

Selected Answer: AE

<https://aws.amazon.com/jp/fsx/lustre/features/>

upvoted 1 times

✉  **reika1914** 4 days, 8 hours ago

Selected Answer: AC

To meet the requirements of migrating latency-sensitive HPC workloads with multi-protocol access (NFS and SMB) to AWS with minimal latency, the following solutions would be the most appropriate:

- A. Deploy compute optimized EC2 instances into a cluster placement group.
 - C. Attach the EC2 instances to an Amazon FSx for Lustre file system.
- upvoted 1 times

✉  **Chiquitabandita** 6 days, 8 hours ago

Selected Answer: AE

[https://aws.amazon.com/fsx/netapp-ontap/features/#:~:text=Amazon%20FSx%20for%20NetApp%20ONTAP%20provides%20access%20to%20shared%20file,access\)%20to%20the%20same%20data.](https://aws.amazon.com/fsx/netapp-ontap/features/#:~:text=Amazon%20FSx%20for%20NetApp%20ONTAP%20provides%20access%20to%20shared%20file,access)%20to%20the%20same%20data.) "Amazon FSx for NetApp ONTAP provides access to shared file storage over all versions of the Network File System (NFS) and Server Message Block (SMB) protocols, and also supports multi-protocol access (i.e. concurrent NFS and SMB access) to the same data."

upvoted 2 times

✉  **LemonGremlin** 1 week ago

Selected Answer: AC

Option A: A cluster placement group provides low-latency and high-bandwidth connectivity between instances. This is particularly beneficial for high-performance computing workloads that are latency-sensitive. Instances within a cluster placement group are placed in close proximity to each other within the same Availability Zone.

Option C: Amazon FSx for Lustre is a high-performance file system optimized for fast access to data. It is well-suited for high-performance computing workloads. It provides low-latency access to data and supports the NFS protocol.

upvoted 3 times

✉  **t0nx** 6 days, 2 hours ago

Thank you

upvoted 1 times

A company is relocating its data center and wants to securely transfer 50 TB of data to AWS within 2 weeks. The existing data center has a Site-to-Site VPN connection to AWS that is 90% utilized.

Which AWS service should a solutions architect use to meet these requirements?

- A. AWS DataSync with a VPC endpoint
- B. AWS Direct Connect
- C. AWS Snowball Edge Storage Optimized
- D. AWS Storage Gateway

Correct Answer: C

A company hosts an application on Amazon EC2 On-Demand Instances in an Auto Scaling group. Application peak hours occur at the same time each day. Application users report slow application performance at the start of peak hours. The application performs normally 2-3 hours after peak hours begin. The company wants to ensure that the application works properly at the start of peak hours.

Which solution will meet these requirements?

- A. Configure an Application Load Balancer to distribute traffic properly to the instances.
- B. Configure a dynamic scaling policy for the Auto Scaling group to launch new instances based on memory utilization.
- C. Configure a dynamic scaling policy for the Auto Scaling group to launch new instances based on CPU utilization.
- D. Configure a scheduled scaling policy for the Auto Scaling group to launch new instances before peak hours.

Correct Answer: D

 **Arnaud92** 6 days ago

D. The application performs normally 2-3 hours after peak hours begin is a key! (schedule policy)
upvoted 3 times

A company runs applications on AWS that connect to the company's Amazon RDS database. The applications scale on weekends and at peak times of the year. The company wants to scale the database more effectively for its applications that connect to the database.

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

- A. Use Amazon DynamoDB with connection pooling with a target group configuration for the database. Change the applications to use the DynamoDB endpoint.
- B. Use Amazon RDS Proxy with a target group for the database. Change the applications to use the RDS Proxy endpoint.
- C. Use a custom proxy that runs on Amazon EC2 as an intermediary to the database. Change the applications to use the custom proxy endpoint.
- D. Use an AWS Lambda function to provide connection pooling with a target group configuration for the database. Change the applications to use the Lambda function.

Correct Answer: B

A company uses AWS Cost Explorer to monitor its AWS costs. The company notices that Amazon Elastic Block Store (Amazon EBS) storage and snapshot costs increase every month. However, the company does not purchase additional EBS storage every month. The company wants to optimize monthly costs for its current storage usage.

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

- A. Use logs in Amazon CloudWatch Logs to monitor the storage utilization of Amazon EBS. Use Amazon EBS Elastic Volumes to reduce the size of the EBS volumes.
- B. Use a custom script to monitor space usage. Use Amazon EBS Elastic Volumes to reduce the size of the EBS volumes.
- C. Delete all expired and unused snapshots to reduce snapshot costs.
- D. Delete all nonessential snapshots. Use Amazon Data Lifecycle Manager to create and manage the snapshots according to the company's snapshot policy requirements.

Correct Answer: D

 **t0nx** 1 week ago

Selected Answer: D

This option involves managing snapshots efficiently to optimize costs with minimal operational overhead.

Delete all nonessential snapshots: This reduces costs by eliminating unnecessary snapshot storage.

Use Amazon Data Lifecycle Manager (DLM): DLM can automate the creation and deletion of snapshots based on defined policies. This reduces operational overhead by automating snapshot management according to the company's snapshot policy requirements.

upvoted 2 times

A company is developing a new application on AWS. The application consists of an Amazon Elastic Container Service (Amazon ECS) cluster, an Amazon S3 bucket that contains assets for the application, and an Amazon RDS for MySQL database that contains the dataset for the application. The dataset contains sensitive information. The company wants to ensure that only the ECS cluster can access the data in the RDS for MySQL database and the data in the S3 bucket.

Which solution will meet these requirements?

- A. Create a new AWS Key Management Service (AWS KMS) customer managed key to encrypt both the S3 bucket and the RDS for MySQL database. Ensure that the KMS key policy includes encrypt and decrypt permissions for the ECS task execution role.
- B. Create an AWS Key Management Service (AWS KMS) AWS managed key to encrypt both the S3 bucket and the RDS for MySQL database. Ensure that the S3 bucket policy specifies the ECS task execution role as a user.
- C. Create an S3 bucket policy that restricts bucket access to the ECS task execution role. Create a VPC endpoint for Amazon RDS for MySQL. Update the RDS for MySQL security group to allow access from only the subnets that the ECS cluster will generate tasks in.
- D. Create a VPC endpoint for Amazon RDS for MySQL. Update the RDS for MySQL security group to allow access from only the subnets that the ECS cluster will generate tasks in. Create a VPC endpoint for Amazon S3. Update the S3 bucket policy to allow access from only the S3 VPC endpoint.

Correct Answer: A

 **t0nx** 1 week ago

Selected Answer: D

Option D is the most comprehensive solution as it leverages VPC endpoints for both Amazon RDS and Amazon S3, along with proper network-level controls to restrict access to only the necessary resources from the ECS cluster.

upvoted 4 times

 **LemonGremlin** 1 week ago

Selected Answer: D

Create a VPC endpoint for Amazon RDS for MySQL: This ensures that the ECS cluster can access the RDS database directly within the same Virtual Private Cloud (VPC), without having to go over the internet. By updating the security group to allow access only from the specific subnets that the ECS cluster will generate tasks in, you limit access to only the authorized entities.

Create a VPC endpoint for Amazon S3: This allows the ECS cluster to access the S3 bucket directly within the same VPC. By updating the S3 bucket policy to allow access only from the S3 VPC endpoint, you restrict access to the designated VPC, ensuring that only authorized resources can access the S3 bucket.

upvoted 2 times

A company has a web application that runs on premises. The application experiences latency issues during peak hours. The latency issues occur twice each month. At the start of a latency issue, the application's CPU utilization immediately increases to 10 times its normal amount.

The company wants to migrate the application to AWS to improve latency. The company also wants to scale the application automatically when application demand increases. The company will use AWS Elastic Beanstalk for application deployment.

Which solution will meet these requirements?

- A. Configure an Elastic Beanstalk environment to use burstable performance instances in unlimited mode. Configure the environment to scale based on requests.
- B. Configure an Elastic Beanstalk environment to use compute optimized instances. Configure the environment to scale based on requests.
- C. Configure an Elastic Beanstalk environment to use compute optimized instances. Configure the environment to scale on a schedule.
- D. Configure an Elastic Beanstalk environment to use burstable performance instances in unlimited mode. Configure the environment to scale on predictive metrics.

Correct Answer: B

✉  reika1914 4 days, 8 hours ago

Selected Answer: D

Given the scenario described, the best solution among the provided options to meet the requirements of migrating the application to AWS, improving latency, and scaling the application automatically during increased demand would be:

D. Configure an Elastic Beanstalk environment to use burstable performance instances in unlimited mode. Configure the environment to scale on predictive metrics.

upvoted 1 times

✉  t0nx 1 week ago

Selected Answer: D

In this scenario, the application experiences latency issues during peak hours with a sudden increase in CPU utilization. Using burstable performance instances in unlimited mode allows the application to burst beyond the baseline performance when needed. Configuring the environment to scale on predictive metrics enables proactive scaling based on anticipated increases in demand.

upvoted 3 times

✉  LemonGremlin 1 week ago

Selected Answer: D

Burstable Performance Instances (T3 or T3a): These instances are designed for burstable workloads and provide a baseline level of CPU performance with the ability to burst above that baseline when needed. Bursting is particularly beneficial for handling sudden spikes in CPU utilization, such as those described in the scenario.

Unlimited Mode: Enabling "unlimited" mode allows instances to burst beyond their baseline performance without accumulating CPU credits. This is important for handling sudden and sustained increases in CPU utilization during peak hours.

Scale on Predictive Metrics: Configuring the environment to scale on predictive metrics allows AWS Elastic Beanstalk to proactively adjust the number of instances based on anticipated demand. This can help ensure that the environment is scaled up before the latency issues occur, addressing them in advance.

upvoted 4 times

A company has customers located across the world. The company wants to use automation to secure its systems and network infrastructure. The company's security team must be able to track and audit all incremental changes to the infrastructure.

Which solution will meet these requirements?

- A. Use AWS Organizations to set up the infrastructure. Use AWS Config to track changes.
- B. Use AWS CloudFormation to set up the infrastructure. Use AWS Config to track changes.
- C. Use AWS Organizations to set up the infrastructure. Use AWS Service Catalog to track changes.
- D. Use AWS CloudFormation to set up the infrastructure. Use AWS Service Catalog to track changes.

Correct Answer: B

A startup company is hosting a website for its customers on an Amazon EC2 instance. The website consists of a stateless Python application and a MySQL database. The website serves only a small amount of traffic. The company is concerned about the reliability of the instance and needs to migrate to a highly available architecture. The company cannot modify the application code.

Which combination of actions should a solutions architect take to achieve high availability for the website? (Choose two.)

- A. Provision an internet gateway in each Availability Zone in use.
- B. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB instance.
- C. Migrate the database to Amazon DynamoDB, and enable DynamoDB auto scaling.
- D. Use AWS DataSync to synchronize the database data across multiple EC2 instances.
- E. Create an Application Load Balancer to distribute traffic to an Auto Scaling group of EC2 instances that are distributed across two Availability Zones.

Correct Answer: BE

A company is moving its data and applications to AWS during a multiyear migration project. The company wants to securely access data on Amazon S3 from the company's AWS Region and from the company's on-premises location. The data must not traverse the internet. The company has established an AWS Direct Connect connection between its Region and its on-premises location.

Which solution will meet these requirements?

- A. Create gateway endpoints for Amazon S3. Use the gateway endpoints to securely access the data from the Region and the on-premises location.
- B. Create a gateway in AWS Transit Gateway to access Amazon S3 securely from the Region and the on-premises location.
- C. Create interface endpoints for Amazon S3. Use the interface endpoints to securely access the data from the Region and the on-premises location.
- D. Use an AWS Key Management Service (AWS KMS) key to access the data securely from the Region and the on-premises location.

Correct Answer: A

 t0nx 6 days, 2 hours ago

Selected Answer: C

CCCCCC

upvoted 1 times

 LemonGremlin 1 week ago

Selected Answer: C

Amazon VPC interface endpoints enable you to privately connect your VPC to supported AWS services without requiring an internet gateway, NAT device, VPN, or Direct Connect connection.

By creating interface endpoints for Amazon S3 in both the AWS Region and the on-premises location, you can securely access data without traversing the internet.

Direct Connect Connection:

With an AWS Direct Connect connection established between the AWS Region and the on-premises location, the data can flow over the dedicated, private connection rather than going over the public internet.

upvoted 4 times

A company created a new organization in AWS Organizations. The organization has multiple accounts for the company's development teams. The development team members use AWS IAM Identity Center (AWS Single Sign-On) to access the accounts. For each of the company's applications, the development teams must use a predefined application name to tag resources that are created.

A solutions architect needs to design a solution that gives the development team the ability to create resources only if the application name tag has an approved value.

Which solution will meet these requirements?

- A. Create an IAM group that has a conditional Allow policy that requires the application name tag to be specified for resources to be created.
- B. Create a cross-account role that has a Deny policy for any resource that has the application name tag.
- C. Create a resource group in AWS Resource Groups to validate that the tags are applied to all resources in all accounts.
- D. Create a tag policy in Organizations that has a list of allowed application names.

Correct Answer: D

A company runs its databases on Amazon RDS for PostgreSQL. The company wants a secure solution to manage the master user password by rotating the password every 30 days.

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

- A. Use Amazon EventBridge to schedule a custom AWS Lambda function to rotate the password every 30 days.
- B. Use the modify-db-instance command in the AWS CLI to change the password.
- C. Integrate AWS Secrets Manager with Amazon RDS for PostgreSQL to automate password rotation.
- D. Integrate AWS Systems Manager Parameter Store with Amazon RDS for PostgreSQL to automate password rotation.

Correct Answer: C